U.S. Department of Justice
Office of Community Oriented Policing Services

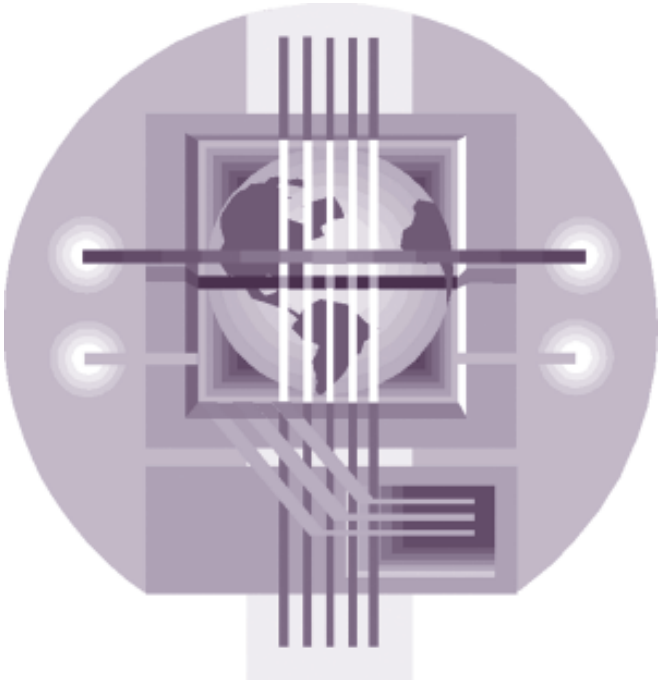
COPS
COMMUNITY ORIENTED POLICING SERVICES
U.S. DEPARTMENT OF JUSTICE

LAW ENFORCEMENT TECH GUIDE FOR

Information Technology Security

How to Assess Risk and Establish Effective Policies

A Guide for Executives, Managers, and Technologists



Copyright © 2006 SEARCH Group, Incorporated. The U.S. Department of Justice reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use, and to authorize others to use, this book for Federal Government purposes. This document may be freely distributed and used for noncommercial and educational purposes. No part of this book may be reproduced in any form, by any means (including electronic, photocopying, recording, or otherwise) for commercial purposes without the prior permission of the U.S. Department of Justice or the authors.

U.S. Department of Justice
Office of Community Oriented Policing Services

LAW ENFORCEMENT TECH GUIDE FOR

Information Technology Security

How to Assess Risk and Establish Effective Policies

A Guide for Executives, Managers, and Technologists

By Kelly J. Harris and Todd G. Shipley, CFE, CFCE

This publication was supported by cooperative agreement #2003CKWXK054 awarded by the U.S. Department of Justice Office of Community Oriented Policing Services to SEARCH Group, Incorporated, 7311 Greenhaven Drive, Suite 145, Sacramento, CA 95831. The opinions or recommendations contained herein are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice. References to specific organizations, products, or services should not be considered an endorsement of the product by the author(s) or the U.S. Department of Justice. Rather, the references are illustrations to supplement discussion of the issues.

U.S. Department of Justice

Office of Community Oriented Policing Services

Office of The Director
1100 Vermont Avenue, NW
Washington, D.C. 20005

Dear Colleague,

Technology systems have contributed significantly to the operational effectiveness and efficiency of law enforcement agencies of all types. As the ability to collect, share, and use information continues to gain momentum in modern policing, technology tools that offer agencies the chance to develop this ability are ever more omnipresent. Yet, as much as we rely on technology for some of our most sensitive and necessary activities, securing that technology is often an afterthought to system deployment rather than being an integrated part of the strategic implementation process.

The *Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies* is intended to provide the law enforcement community with strategies, best practices, recommendations, and ideas for developing and implementing information technology security policies. It will help you identify and assess information technology security risks within your agency and provide ideas for mitigating them. Moreover, it will encourage readers to view security policies and practices as an ongoing process of assessment, modification, and measurement.

This guide is one of the many resources that the Office of Community Oriented Policing Services (COPS) offers to law enforcement. It can be used as a stand-alone resource or used in conjunction with the original *Law Enforcement Tech Guide (how to plan, purchase and manage technology (successfully!)* published by the COPS Office in 2002. That guide and many of our other knowledge-based resources can be downloaded from **www.cops.usdoj.gov**, or they can be ordered free of charge by calling the COPS Office Response Center at 800.421.6770 or via e-mail at **askCOPSRC@usdoj.gov**.

I hope that you find this guide to be both informative and helpful.

Carl R. Peed
Director

Contents

Acknowledgments x
About the Authors xi

About the Guide

About the Guide 3
Assumptions About You 5
How this Guide Is Organized 6
NIST—A Logical Framework for IT Security Policy Development 7
Definitions of Icons 8
A Roadmap to the Guide 10
IT Security Policy Development—A Cyclical Process 12

Chapter 1
Information Systems Security: Understanding Your Responsibility, Security Policies, and Risk 17
A Responsibility to Secure Your Systems 18
What Is a Security Policy? 20
What Are the Risk Factors to an IT System? 22
Evaluating Risk Is Key to Developing Security Policies 25
How Security Policies Control Risk 25

Chapter 2
Organize and Charge the Security Policy Development Team 29
Step 1: Get Senior Leadership to the Table 30
Step 2: Identify Stakeholders 31
Step 3: Assign a Project Manager 32
Step 4: Create a Governance Structure with Roles and Responsibilities 33
Step 5: Review Your Agency Mission and Objectives 35
Step 6: Allocate Resources 36
Step 7: Adopt a Methodology and Plan of Action 36
Sample Security Policy Development and Implementation Scenario 38

Chapter 3
Phase I–Conduct a Security Self-Assessment 45
The Self-Assessment Process 46
Step 1: Identify the Systems, Single System, or System Part for Which You Will Develop Security Policies..... 47
Step 2: Assemble the Appropriate Participants for the Process and Hold a Kickoff Meeting 47
Step 3: Gather Organizational Data 48
Step 4: Conduct the Self-Assessment 57
The SEARCH IT Security Self- and Risk-Assessment Tool: Easy to Use, Visible Results 61

Chapter 4
Phase II–Assess Security Risks..... 71
Why Is the Risk-Assessment Process Important? 72
Conduct a Risk Assessment 73
Step 1: Identify the Risk and Write a Description of It..... 73
Step 2: Categorize and Quantify the Identified Risks..... 74
Step 3: Determine Your Tolerance for Levels of Risk..... 76
Make Your Risk Assessment Easier by Using the SEARCH Assessment Tool..... 78
What's Next? 80

Chapter 5
Phase III–Develop a Risk-Mitigation Strategy 83
Prioritize Your Agency's Risks 84
What Are Security Controls? 84
Build Your Agency's Controls in Six Steps 89
Document the Controls 94
Select Which Controls to Implement and Assign Responsibility 94
Develop an Implementation Plan..... 95

Chapter 6
Phase IV–Measure Your Security Controls 99
What Are Security Measures? 100
Develop and Select Measurement Methods 100
Build Your Agency's Measures in Seven Steps 103

Chapter 7
Formalize Your IT Security Policies 111
Write an Information Security Policy in Six Steps 113

Conclusion 118

Appendixes

A. Assessment Worksheets and Questions from the SEARCH IT Security Self- and Risk-Assessment Tool 121
B. SEARCH IT Security Worksheets: Control Development, Measurement Development, Policy Development 181
C. Glossary of Security Terms 189
D. Security Resources..... 195

Acknowledgments

This publication was prepared by SEARCH, The National Consortium for Justice Information and Statistics, Mr. Francis X. Aumand III, chair, and Ronald P. Hawley, executive director. The project director was Kelly J. Harris, deputy executive director. Ms. Harris and Todd G. Shipley, CFE, CFCE, director of training services, wrote this publication. James E. Jolley, CISSP, computer training specialist, was a contributor. Twyla R. Putt, corporate communications manager, edited this publication. Jane L. Bassett, publishing specialist, provided layout and design. Chris Roebuck, webmaster, provided web site coordination. The federal project manager was Debra Cohen, Ph.D., of the U.S. Department of Justice Office of Community Oriented Policing Services (COPS). The authors would like to thank the Hawaii Attorney General's Office IT Group for its advice in the development of the early drafts of the self- and risk-assessment tool.

Suggested Citation
Harris, Kelly J. and Todd G. Shipley, *Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies*, Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2006.

About Us

SEARCH, The National Consortium for Justice Information and Statistics, is dedicated to improving the quality of justice and public safety through the use, management, and exchange of information; application of new technologies; and responsible law and policy, while safeguarding security and privacy.

We assist local, tribal, county, regional, and state agencies and organizations—including law enforcement and public safety; first responders; prosecution; defense; adjudication; detention; corrections and probation; and other disciplines, such as transportation, drivers' licensing, vehicle registration, public health, and social services—through a broad array of activities, resources, and products. Our focus is on criminal history systems, integrated justice information systems, information technology (planning, purchasing, managing), communications interoperability, and cybercrime investigation. Our services include in-house and on-site technical assistance and training, resource development (web sites, publications, white papers, conferences, workshops), public policy assistance, and model development (model legislation, standards and procedures, best practices) in these focus areas. SEARCH online resources provide information on law enforcement information technology (IT), integrated justice, justice software solutions, and IT acquisition at **www.search.org**.

About the Authors

Author **Kelly J. Harris** is deputy executive director for SEARCH, where she oversees the development, implementation, and management of all SEARCH programs and related projects. SEARCH programs focus on IT and its successful application to justice and public safety decision-making. In each program, Ms. Harris directs a broad array of activities, resources, and products provided to local, regional, tribal, and state justice and public safety agencies nationwide. These include technical assistance, training, resource development (publications, web sites, model development), national-scope policy research, and national workshops, symposia, and conferences. Ms. Harris oversees programs funded by grants, cooperative agreements, and contracts from the U.S. Departments of Justice (DOJ) and Homeland Security (DHS), and from state and local agencies.

The key focus areas of SEARCH programs overseen by Ms. Harris are:

- Law and policy issues associated with information and identification technologies
- Planning for and implementing information-sharing technology
- Interoperable communications technologies
- High-technology crime investigation.

Program activities and resources address such issues as justice information-sharing system integration; how to plan for, develop, improve, acquire, and manage automated systems; homeland security; and combating cybercrime. Specific projects involve Internet crimes against children, national criminal history repository improvements, justice information exchange modeling, and community oriented policing services.

Ms. Harris has developed, organized, and presented at numerous national symposia on justice information sharing and technology, and technical assistance workshops and conferences on justice and public safety IT planning and implementation issues. These programs have trained thousands of practitioners and state and local policymakers. She has written numerous articles, technical bulletins, and reports on justice system automation and integration for SEARCH and for publication by the U.S. DOJ. She has also provided technical assistance on issues relating to justice and public safety information sharing, interoperability, and integration.

Ms. Harris is a member of various advisory committees, including the Law Enforcement Information Technology Standards Council and the Global Justice Information Sharing Initiative's Intelligence Working Group. Ms. Harris joined SEARCH in 1991. She received a bachelor's degree in political science and communications from the University of California, Davis.

Author **Todd G. Shipley** is director of training services for SEARCH, where he oversees a national program that provides expert technical assistance and training to local, state, and federal justice agencies on successfully conducting high-technology computer crimes investigations.

Mr. Shipley instructs and oversees a variety of SEARCH technology crimes courses offered at its National Criminal Justice Computer Laboratory and Training Center in Sacramento, California, and at other sites nationwide. SEARCH assistance and training services—provided by an experienced team of certified computer crimes investigators and information systems security professionals—focus on systems security, computer forensics, and investigations involving the Internet, local area networks, and online child exploitation.

Mr. Shipley has 25 years of experience in law enforcement, all with the Reno (Nevada) Police Department, where he developed subject-matter expertise in computer forensics, online investigations, and information technology security. Prior to joining SEARCH in 2004, he was a senior detective sergeant managing the department's Financial and Computer Crimes Unit, where he investigated serious fraud- and financial-related offenses using basic investigative, technical, and covert surveillance techniques. He was responsible for developing cybercrime and technology crime investigative policy; serving as a liaison to other law enforcement, intelligence, and government agencies and industry bodies; providing department/regional training; and serving as an expert witness.

His previous positions with the Department included 4 years as a detective and detective sergeant assigned to the U.S. Attorney's Office Organized Crime Drug Enforcement Task Force, 5 years as a detective investigating major property and person crimes, and 8 years as a patrol officer. Mr. Shipley formed Nevada's First Computer Crime Investigations Unit. He is a Certified Fraud Examiner (CFE) through the Association of Certified Fraud Examiners and a Certified Forensics Computer Examiner (CFCE) through the International Association of Computer Investigative Specialists. He is a member of the High Technology Crime Investigation Association (HTCIA), and has written and spoken extensively on computer forensics and technology crime topics.

Contributor **James E. Jolley** is a computer training specialist for SEARCH, where he performs a variety of tasks related to the provision of training to local, state, and federal agencies on computer technology issues with criminal justice applications. He also researches techniques for online investigations, assists in preparing material for the computer training courses, assists with computer forensic examinations, and maintains the computer network and equipment of SEARCH's National Criminal Justice Computer Laboratory and Training Center in Sacramento, California.

Before joining SEARCH in 2002, Mr. Jolley worked primarily in the computer security industry. He has served as a network security analyst for SBC, a senior security analyst for Chevron/Texaco, and a security consultant for CHG, LLC. In these capacities, he has configured and managed firewalls, installed and monitored intrusion detection systems, performed network scans for customer sites, provided on-site technical assistance for users, and worked in security policy development.

Mr. Jolley holds a bachelor's degree in computer science from the University of San Francisco, and has completed graduate course work in quantitative business methods at California State University, Hayward. He is a member of both the Information System Security Association and the HTCIA. He has several certifications, credentials, and licenses, including Certified Information Systems Security Professional (CISSP), Certified Wireless Network Administrator (CWNA), Microsoft Certified Professional (MCP), Cisco Certified Network Associate (CCNA), Cisco Certified Design Associate (CCDA), and CheckPoint Certified System Engineer (CCSE). He has also received extensive training on computer crime investigation, forensic computer science, Microsoft, Cisco, and CheckPoint.

IT Security Tech Guide Review Committee

SEARCH extends its deepest thanks and appreciation to the members of the IT Security Tech Guide Review Committee, who participated in an advisory capacity during the preparation of this Guide. These individuals have direct experience in law enforcement IT planning, procurement, implementation, and management and generously contributed their time and expertise over a period of many months, providing critical review and comments on early drafts of the Guide. Their contributions to the successful completion of this Guide cannot be overstated.

William Spernow
Security Mentors, LLC
Security Consultant

Liane M. Moriyama
Hawaii Criminal Justice Data Center

Dr. Ron Glensor
Reno (Nevada) Police Department

Steve Correll
Nlets—The International Justice & Public Safety Information Sharing Network

Susan Ballou
Office of Law Enforcement Standards
Steering Committee Representative for State/Local Law Enforcement
National Institute of Standards and Technology

Mark Wilson, CISSP
IT Specialist (Information Security)
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Special Thanks

In addition to the peer reviewers mentioned above, SEARCH extends special thanks to the following organizations that provided additional critical review of this document:

- U.S. Department of Justice Office of Community Oriented Policing Services
- The Bureau of Justice Assistance and U.S. Department of Justice's Global Justice Information Sharing Initiative
- Security Committee, Integrated Justice Information Systems Institute
- Security and Access Ad Hoc Subcommittee, FBI Criminal Justice Information Services Advisory Policy Board
- Microsoft Corporation.

About the Guide

A Library of Tech Guide Resources

This Tech Guide on information technology security is intended to serve as a companion guide to *Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!)*. The original Tech Guide was published in 2002 by the U.S. Department of Justice Office of Community Oriented Policing Services (COPS) and was developed as a step-by-step guide to help law enforcement agencies as they implement new technologies.

This Information Technology Security Tech Guide is intended to complement and be used along with the original Tech Guide. As such, this Guide makes frequent references to content in the original Tech Guide. It may help to keep the original Tech Guide close at hand so you can refer to particular pages and sections as needed.

This Tech Guide is one of a series of four topic-specific Tech Guides funded by the COPS Office. The four companion Tech Guides that will form a comprehensive library of technology resources, along with the original Tech Guide, are:

- *Law Enforcement Tech Guide for Small and Rural Police Agencies: A Guide for Executives, Managers, and Technologists*
- *Law Enforcement Tech Guide for Creating Performance Measures that Work: A Guide for Executives and Managers*
- *Law Enforcement Tech Guide for Communications Interoperability: A Guide for Interagency Communications Projects*
- *Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies*

See page 5 for details on how to download or order your copy of the original *Law Enforcement Tech Guide*.

About the Guide

Technology continues to proliferate throughout law enforcement. Indeed, information systems are indispensable tools for effective, expedient, and well-informed policing.

Technology also poses an enormous security risk. Law enforcement agencies that operate mission-critical information technology (IT) systems without adequate security controls in place put the public, themselves, and our government at extreme risk. Data contained within these systems are extraordinarily sensitive and mission-critical. Sensitive case reports, confidential investigative data, agency intelligence, suspect and personal data, and personnel information are just a few examples of data that may be subject to compromise via a malicious hack, an untrustworthy insider, an accidental misuse of the system, and/or a natural disaster.

Creating security policies and instituting a security process has traditionally been—at best—an afterthought in many IT implementations. Too often, only marginal consideration is given to the security of a system (such as requiring passwords) when it is being developed or implemented. What is missing is the adoption of an IT security policy development *process,* a conscious decision by senior management to establish a formal procedure to investigate and analyze the very real security risks to the agency's IT systems, and to develop mechanisms and policies designed to mitigate those risks. Securing an information system is much more involved than merely requiring a password, applying a digital signature, or using encryption. **It is an organizational strategy that must be driven by the highest levels of the organization**.

Having effective information technology security policies is essential to protecting the information assets of an agency from accidental or malicious compromise. **This Guide offers an approach to help law enforcement agencies through the often complex process of developing and implementing effective information security policies**. It also provides a framework to establish an ongoing process to gauge the performance and effectiveness of these policies.

Controlling risk is key to having a secure information system.

Therefore, identifying what those risks are is an important first step to developing effective IT security policies.

Understanding your security risks is central to building an effective IT security program. Unless you can figure out *what* your agency's exposures are, you will probably not be successful in reducing your overall risk. **Controlling risk is key to having a secure information system**. Controlling risk allows you to avoid exposures that, if unidentified, could be exploited and result in damage to your system, your data, and your agency's reputation.

HOW TO USE THIS GUIDE

This *Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies* is intended to provide strategies, best practices, recommendations, and ideas for developing and implementing IT security policies. This Guide should not be construed as specific legal advice for any specific factual situation. This publication is meant to serve as a guideline for situations generally encountered in law enforcement IT security policy environments. It does not replace or supersede any policies, procedures, rules, and ordinances applicable to your jurisdiction's IT security situation. This Guide is not legal counsel and should not be interpreted as a legal service.

This Guide walks you through the essential components of *risk management*, which include undertaking a detailed *self-assessment* of your IT system, which will ultimately enable your agency to identify its security risks, and then to *mitigate* these risks through the development of effective security policies.

This document can be used independently or along with *Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!)*, which SEARCH created in 2002 under a cooperative agreement with the U.S. Department of Justice Office of Community Oriented Policing Services (COPS).[1] That publication provided law enforcement technology practitioners with a useful, hands-on guide for implementing various types of technology. Although this IT Security Tech Guide is a great resource on its own, we suggest keeping the "original" *Law Enforcement Tech Guide* close at hand. The two guides are complementary and, used together, make a comprehensive toolset.

How can you get your own copy of the original *Law Enforcement Tech Guide*? See page 5.

If you don't have a copy of the original *Law Enforcement Tech Guide*, download or order one. Since this Guide on IT security policies is intended the complement the original, at times we will refer to it rather than repeat advice.

[1] Harris, Kelly J. and William H. Romesburg, *Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!), A Guide for Executives, Managers and Technologists*, Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2002.

SOURCES OF THE ORIGINAL "LAW ENFORCEMENT TECH GUIDE"

The COPS Office published the *Law Enforcement Tech Guide* in 2002. It is available electronically from the COPS Office web site at **www.cops.usdoj.gov/default.asp?Item=512**. There it is broken down into its separate parts as Portable Document Format (PDF) files so you can download or read one at a time.

If you're anxious to download the entire document at once—all 14 megabytes—the complete version can be found on SEARCH's web site: **www.search.org/files/pdf/TECHGUIDE.pdf**.

Hard copy versions are distributed by the COPS Office. To request one, contact the COPS Office Response Center at 800.421.6770 or via e-mail at **askCOPSRC@usdoj.gov**.

Assumptions About You

To prepare this Guide, we had to make some assumptions about you, the reader. You may be the first person in your agency to get this Guide and read it; or, you may be part of a security team that has been formed to develop and implement security policies. Perhaps you are the chief or sheriff who will lead this effort. Regardless of your position in the agency, your personal knowledge of the agency's operations is integral to this project's success. Understanding the movement of and need for information within your agency to accomplish its daily business needs is valuable. You may be the person in your agency responsible for technical support (and that does not exclude you from also being one of the other types of readers as well!). If so, you may be called upon to research the technical aspects of this project as they affect and change the operations of your agency's systems.

Finally, you might be a project manager who possesses useful project management skills, yet who has little experience with law enforcement. Or, you may not have any project management skills, but you have been assigned to manage this task nonetheless. Either way, your role of project manager is pivotal to this effort. You are the "go-to" person for project information and coordination. In most law enforcement agencies, both sworn and civilian personnel must wear many different hats; very few agencies have the resources to fully staff an IT support department or to hire a dedicated project manager. We assume many of our readers will fall into one or more of the categories above. If so, this IT Security Guide is designed to help each of you.

How this Guide Is Organized

The purpose of this "how-to" Guide is to provide you with a series of general steps through which you can: 1) understand and identify your security "exposures," 2) develop and implement controls to mitigate these identified security risks, 3) create and implement a program to measure the effectiveness of these controls, and 4) using the work done in the previous steps, develop and implement security policies for your agency. The processes will involve many different persons and skill sets. Only when you have a set of security policies and their associated security controls (procedures) in place, and you have implemented a process to monitor their effectiveness, can you effectively maintain the security and integrity of your IT systems.

What will you learn from this Guide?

- An overview of security risk management; the importance of implementing an information security policy; and the critical leadership role of managers in policy initiatives.
- Who to involve in your project and how to develop your Security Policy Development Team.
- The four key phases of the IT security development and implementation process.
  - Learn how to conduct a self-assessment, which provides a status report of your current system (see Phase I).
  - Through a risk assessment, determine what security exposures exist in your IT systems, using findings from the self-assessment (see Phase II).
  - Learn how to properly develop and implement security controls to mitigate the identified risks (see Phase III).
  - Learn how to develop and implement an ongoing measurement process to ensure that the controls are effectively mitigating the risks (see Phase IV).
- The hands-on process of how to write information security policies.

The NIST Security Manuals are:

–Not copyrighted.

–Developed by a recognized and competent organization.

–Focused on government information security operations, not corporate operations.

They are available online at **http://www.nist.gov** and through the Computer Security Resource Center at **http://csrc.nist.gov/**.

See Appendix D for a list and description of key NIST security documents.

NIST—A Logical Framework for IT Security Policy Development

The National Institute of Standards and Technology (NIST) was tasked, after the E-Government Act (Public Law 107-347) was signed into law by the President in December 2002, to formulate and publish standards for all federal agencies to follow when developing information security policy and procedures. As such, NIST has produced and maintained numerous security manuals that create a standardized process for IT security policy development, particularly focused on government operations. We believe the NIST framework provides the most robust, consistent, and widely used methodology for government agencies on which to base their security policies.

The NIST manuals are complex and voluminous, comprising more than 7,000 pages of free reference works. This Guide borrows some of the key NIST principles to develop a framework for state and local law enforcement security policy development, and tailors their application to the unique issues and challenges that law enforcement agencies face when developing security policies and procedures. We will reference NIST documents throughout this Guide where appropriate for additional reading and research.

The key for an agency wishing to follow a national and standardized methodology, such as the NIST guidelines, is to develop security policies consistent with the federal agencies with which your state and your agency may share data (for example, the FBI's Criminal Justice Information Services program).

Global Document a Key Companion to Security Policy Development Efforts

Another "must-have" document is *Applying Security Practices to Information Sharing Systems*. This excellent resource document, developed by the Global Justice Information Sharing Initiative Security Working Group, is designed to educate justice executives and managers in basic, foundational security practices that they can deploy within their enterprise and between multiple enterprises. This document and its companion CD contain background information, overviews of best practices, and guidelines for secure information sharing. The document (in PDF) and CD (a browser-style, graphical overview of the document) are available at **http://it.ojp.gov/global**.

The Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee, advising the U.S. Attorney General on justice information sharing and integration initiatives. Global was created to support the broad-scale exchange of pertinent justice and public safety information. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment.

We believe that using this Guide, along with the NIST and Global documents, provides a comprehensive resource for your agency's security policy development initiative.

Definition of Icons

Throughout this Guide, icons are used to draw your attention to important concepts, ideas, reference material, and, in some cases, warnings. Below are the icons and what they represent:

Original Tech Guide Reference

The parent Tech Guide contains useful tools, charts, and instructions for conducting various tasks. When you see this icon, you will be directed to a specific page, or range of pages, in the original *Law Enforcement Tech Guide*.

Chief/Sheriff/Executive

This icon alerts chiefs/sheriffs and executive managers to the activities, issues, and concepts they need to be aware of.

Project Manager

This icon alerts project managers to activities, issues, and concepts they must be aware of.

Stop Sign

When you see a stop sign icon, pay particular attention, as it indicates where others have encountered trouble in their projects. This icon indicates pitfalls to avoid.

Tips

If we have heard or know of shortcuts or have useful ideas on how to tackle a particular task, we will use this icon to let you know.

NIST

We will use this icon when we refer to content that originated in a NIST publication.

The IT Security Self- and Risk-Assessment Tool

We will use this icon when we refer to the **SEARCH IT Security Self- and Risk-Assessment Tool**, a Microsoft Excel spreadsheet that guides you through a detailed assessment of your agency's IT system in three categories: Management, Organizational, and Technical. (For a description of this Assessment Tool, see page 61.)

A Roadmap to the Guide

Organize and Charge the Security Policy Development Team

a. Obtain leadership and involvement of senior management.
b. Identify and recruit internal and external stakeholders and obtain their input and support.
c. Assign a project manager to guide and oversee the initiative.
d. Create a governance structure with defined roles and responsibilities.
e. Review your business mission and IT strategic plan as guidance to your security initiative.
f. Allocate time and human/financial resources.
g. Adopt a methodology and action plan to developing/implementing your security policies.

Phase I–Conduct a Security Self-Assessment

a. Determine which system(s) or system part you want to develop security policies for.
b. Assemble appropriate stakeholders and hold a kickoff meeting to discuss process.
c. Gather relevant organizational data about the system(s) to be assessed.
d. Use the SEARCH IT Security Self- and Risk-Assessment Tool to conduct the self-assessment.
e. Compile the results.

Phase II–Assess Security Risks

a. For each assessment question your team answered during the self-assessment, identify the risk and write a description of it (use the Assessment Tool for this and the remaining risk-assessment tasks).
b. Categorize and quantify each identified risk (likelihood: remote, possible, or likely; severity: high, medium, or low; and area of impact: human, financial, liability, etc.).
c. Determine your tolerance level for each identified risk (avoid, assume, mitigate, or transfer).
d. Determine a numeric priority for action for each identified risk (1 being highest priority, 3 being lowest).

Phase III–Develop a Risk-Mitigation Strategy

a. Prioritize risks, using the results of the risk assessment.
b. Build security controls to mitigate risks (a six-step process).
c. Document the controls.
d. Select which controls to implement and manage, and assign responsibility for these.
e. Develop an implementation plan that articulates how each control is implemented.

Phase IV–Measure Your Security Controls

a. Develop and select measurement methods for the controls you will implement.
b. Identify existing measures.
c. Identify all other possible measures.
d. Identify implications of measures.
e. Recommend measures for adoption by management.

Formalize and Write your Security Policy

a. Identify existing policy that addresses the identified risks.
b. Write proposed security policy that addresses these risks.
c. Recommend security policy for adoption by management.

IT Security Policy Development — A Cyclical Process

Developing policies to manage your IT systems must be a first priority for executives and managers. Policies lead to procedures for implementing security, the controls that prevent security breaches, and solid metrics to measure your effectiveness. **In short, it is a cyclical *process* that never ends—not a project that contains defined beginning and end points (Figure 1).**

Figure 1: Normal IT Security System Development Lifecycle

Normally, *policy* drives procedures and measures of effectiveness. However, what should you do when policy does not exist? In producing a Tech Guide to help you build effective IT security policies, we obviously had to take a linear, step-by-step approach and one that assumed that the reader probably did not have comprehensive security policies in place. We realize you will probably not be starting from scratch; indeed, you may already have several security policies in place that you must adhere to. Some policies are "known" but not well documented, others came from legislative and organizational mandates, others may have been developed in response to a specific concern, while still others have yet to be developed.

SDLC is a cyclical process regarding IT and, in particular, policy development. It means you are never really "finished" with an effort, but instead, it involves continuous review, revision, enhancement, and implementation of new and existing policies and procedures.

In a perfect world, we would have followed a proper System Development Lifecycle (SDLC). We would have developed our policy first on how our systems should run and interact. Let's fast-forward to the real world. Many state and local law enforcement agencies rarely have the good fortune or time and money to develop and complete an SDLC for their existing networked systems. Most agencies have already developed systems that have grown over time. Some security policy may already exist, as well as procedures, controls, and measurements. In most agencies, however, thoroughly documented security policies are lacking.

Our goal is to help you take the policies that already exist (whether or not they are written down), build upon them and create a single, comprehensive, documented, security policy for your IT assets. To properly develop security policy using the model described in this Tech Guide requires a *complete understanding* of your existing system. To achieve this understanding, we recommend that your security policy team complete a self-assessment and risk assessment *first*. These exercises, which will provide you with a complete identification of your agency's assets and the potential risks to them, are instrumental in helping you determine what controls you need to mitigate those risks—and the methods you need in place to measure the effectiveness of those controls.

Once completed, these tasks—**self-assessment, risk identification, risk mitigation** through controls, and control **measurement**—all inform what your policy should be. As we walk you through the policy development process, you will see how this all comes together. So, although it is at the end of this Guide that you will craft your formal policy statement (which may seem contrary to standard convention at first blush), stay with us and follow the creation of policy from beginning to end.

Have you read the
"IT Security Policy Development —
A Cyclical Process" section yet?
(It's on pages 12 and 13.)
If not, it is important that you read it
before you continue any further.

CHAPTER 1
INFORMATION SYSTEMS SECURITY: UNDERSTANDING YOUR RESPONSIBILITY, SECURITY POLICIES, AND RISK

"Like any risk management process, information security must be fully integrated into all relevant organizational policies, which can occur only when security consciousness exists at all levels."

From "Information Security Governance,"
in *ITAUDIT*, vol. 4, February 15, 2001,
The Institute of Internal Auditors

Chapter 1:
Information Systems Security:
Understanding Your Responsibility, Security Policies, and Risk

What You must clearly understand your responsibility for securing information technology (IT), the security risks inherent in IT systems, and how security policies help you mitigate them.

Why Security policy development is complex and is an activity that has most often been an afterthought to information system implementation. Developing IT security policies should become integral to effective IT systems planning, procurement, and implementation.

Who Everyone in the organization must understand the IT system vulnerabilities and how they can occur. Management is responsible for initiating and maintaining effective security policies, but ultimately many individuals at varying levels in the organization will be involved, including system and information owners, legal counsel, IT support staff, and users.

When Ideally, from the beginning of a technology project, but policies can (and should!) be developed for IT systems at any time.

> *"Our increasing dependence on computers and computer networks exposes us to the risks of cyber attacks, viruses and hacking that have the potential to rob us of our personal identity, disrupt our economy, and undermine our national security."*
>
> **—Rep. Lamar Smith (R-Texas)**
> **Floor statement**
> **U.S. House of Representatives**
> **October 17, 2005**

A Responsibility to Secure Your Systems

What do you accomplish with a security policy?
— Confidentiality
— Integrity
— Availability

Effective law enforcement in the world we live in today is nearly impossible without the use of computer systems and computer networks. With the advent of mobile computing, officers can conduct business from the patrol car, accessing information from computer-aided dispatch systems; querying numerous state, local, and federal databases (i.e., regional law enforcement information systems, the National Crime Information Center [NCIC], National Law Enforcement Telecommunications System [Nlets], and terrorism watch lists); filing incident and other reports directly from the field; and communicating directly in real time with supervisors, peers, and other first responders. Moreover, agency internal IT systems such as records management systems (RMS) capture, maintain, and analyze all police agency and incident-related event information, which allows the tracking and managing of criminal and noncriminal events, investigations, and personnel information.

As the original *Law Enforcement Tech Guide* noted, "Indeed, records management systems of the 21st century have become a key asset to effective policing, offering robust analytical tools, the ability to seamlessly share information, develop complex linkages between myriad data and information and assist in effective management strategies. The police RMS is a key component to informed and intelligent decision-making and the basis for sound integrated justice information systems."

Jacqueline Wagner, chair, Institute of Internal Auditors International, and General Motors' general auditor: "Effective information security must be pervasive. A security or controls group no longer owns the task. Security is everyone's job—it must be broad and touch every cubicle and office."

Clearly, to be so robust, police systems contain sensitive records, documents, data, information, and files related to persons (victims, witnesses, suspects), vehicles, incidents, arrests, warrants, accidents, citations, field interviews, civil process paper service, gun registration investigations, property, and evidence, to name a few. This information can be captured and stored in a variety of forms, including data, voice, and images. Information stored in law enforcement information systems is, obviously, sensitive and often confidential and may be subject to many laws, policies, and regulations regarding its collection, use, storage, disposal, and sharing.

Law enforcement systems, like many other organizational IT systems, are among the most valuable assets of any agency. At the federal level, the U.S. Office of Management and Budget (OMB) has promulgated a policy that requires each federal agency to implement and maintain a program to adequately secure its information assets.[2] In addition, each agency must have programs that:

- Assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability.

---

[2] *Federal Information Technology Security Assessment Framework*, November 2000, included as part of NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.

According to ***Report to the President, Cyber Security: A Crisis of Prioritization***, **President's Information Technology Advisory Committee, Executive Office of the President of the United States (pp. 10-11, February 2005)**: "The Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University reports that 3,780 new electronic vulnerabilities were published in 2004, more than a 20-fold increase from 1995."

- Protect system data commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification of those data.

These security goals are valid not only for agencies within the Federal Government, but any state or local government entity. Law enforcement executives have a fiduciary responsibility to ensure that their automated information systems and networks are protected. They must also ensure that appropriate persons are assigned responsibility for securing those systems and that they exercise due care in the performance of their duties. Thus, a commitment to staff training on security issues and your organization's security policies is key. Training will give staff the background they need to make informed decisions about system security to successfully avoid risks and/or mitigate those risks to acceptable levels. Ultimately, senior management, as the owners of the system, bear the responsibility for all the risks inherent in the operation of your agency's IT systems.

What can happen when reasonable and effective security practices are not mandated by senior management and followed through by an agency? Let's look at a couple of examples of what can happen.

Example 1: *Audit identifies major security vulnerability for a state agency web site; site closed for business*. In one state, the Department of Motor Vehicles developed and implemented a web-based vehicle registration renewal system in 2000. The system gave citizens the ability to renew their motor vehicle license tabs and plates over the Internet. According to the report, citizens could pay their registration renewal taxes from their home. The state web site was a great success: Revenue related to the registration renewals and use of the web-based system increased from $6.6 million in FY2001 to $30.5 million in FY2004. However, an audit conducted in 2005 found major security vulnerabilities and ultimately concluded that failure by the agency to carefully plan for and prevent tampering with the data offered by the web site meant that it would have to be shut down. Indeed, the audit report contents read:

Key Conclusion
Serious security weaknesses have exposed the web-based Vehicle Registration Renewal System and citizens' private data to an unacceptable risk of tampering, disruption, and misuse. Until significant security enhancements are made, the system should not be used to conduct business.

Findings

- The department did not implement an effective security program.
- Computer programs developed by the Driver and Vehicle Services Division contained security flaws.

Why aren't there more published "horror stories" on security? The answer is simple. Most organizations or agencies do not want their name up in lights when they have failed to protect systems or data, for obvious reasons. The organizations usually want to clean up the mess quickly, get the problem fixed, and move on. The sooner the problem gets off the radar screen, the better everyone feels.

- Poorly configured wireless access devices provided a way to bypass the department's firewall.
- Sensitive customer data and critical system components were not properly protected.
- The department did not promptly perform important system maintenance procedures.
- The department did not adequately monitor its systems.

Example 2: *Employee error causes a security failure at a large state university*. The incident involved open Internet access to about 20 documents that contained student names and social security numbers. When the university finally looked into the matter, they determined that a university staff member had backed up these files on the university web server. While the staff member had legitimate access to these documents, they were unknowingly saved to the web server. Because the university did not enforce a periodic review of its IT systems, this problem went undetected for about 2 years.

What Is a Security Policy?

A security policy is a document—or an electronic file—that spells out specific rules and adds structure to the organization's procedures. It gives your agency staff guidance regarding how they should act and respond to given events or situations.

Some general facts about information security policy development you should know *before* you start: Policies ultimately must be:

Security Policy: A written statement that directs the behavior of one or more individuals and is designed to reduce or eliminate a specific risk, or set of risks, incurred by the operation of an IT system.

1. **Implementable** by your agency. Writing a thorough and concise policy that no one can hope to put into practice is of no use to you or your agency. Analyzing the chosen controls, as well as their implementation and management, should clearly indicate whether the resulting policy will be reasonable.
2. **Enforceable**. Any written policy must have mechanisms that will control its enforcement, whether that is a management mechanism such as review and oversight or an automated function of a particular system.
3. **Responsible**. The policy must clearly define who is responsible for the implementation of the policy and must consistently ensure that the responsibility is aptly handled.
4. **Documented**. The policy must be formally documented, distributed, and understood by all affected personnel within the agency.

Security policies and their development make for interesting discussion, but unless you have gone through the process, few know what actually goes into creating a policy and, more important, why they are useful. Many believe that if they could just

adopt an existing policy, they could solve their security needs. The problem with this approach is that security is actually a *process*, and security policies are specific to an organization, derived from many factors, and used for many different reasons.

Effective IT security: the state where recognized IT security risks have been reduced, by means of security procedures, to a level that is acceptable to management and monitored on an ongoing basis.

Developing effective information security policies for a law enforcement agency is the product of a comprehensive **risk-management** effort, which includes **assessing** the risk to the organization with respect to its technology implementation, developing ways to **mitigate** that risk, and **evaluating** whether policies and procedures put in place to reduce the risk are effective.

A security policy represents the distillation of many activities, including:

- A detailed understanding of the current IT environment and any existing security policies and procedures
- An assessment of risk and system vulnerabilities associated with that environment
- Priorities based on identified risks
- Mitigation strategies adopted by management
- Implementation of the mitigation strategies
- Ongoing evaluation of the effectiveness of the strategies
- Creating the written security policy
- Revising the strategies and rewriting the policies when needed.

Simply put, security policies are developed as a part of a comprehensive risk management process. If you do not have policies in place, you need to start with both a *self-assessment and a risk assessment.* After fully understanding your system and its risks, you can then successfully craft policies to manage those risks. Once the policies are in place, they become the basis for the actual control mechanisms that will reduce or mitigate your IT system risk.

Just because a security policy looks simple does not mean that time or effort to develop the policy was either easy or quick. The real issue is if the policy accomplishes management's goal of reducing risk to an acceptable level.

Now, there are some exceptions to the notion that you must know the risk before you can develop a policy. You will be required to adhere to some federal, state, and local laws, rules, and ordinances regardless of your assessment of risk. For example:

- States accessing NCIC must adhere to the *CJIS Security Policy* issued by the FBI's Criminal Justice Information Services (CJIS) Division. (In addition, agencies accessing any criminal justice information system governed by the *CJIS Security Policy* must be in compliance with Federal Information Processing Standards [FIPS] for all procurements after September 30, 2005.)

This Tech Guide does not specifically deal with state or local compliance issues that may affect your agency. You will need to know your responsibility in complying with any or all the laws or regulations that govern your agency.

- Federal regulations governing the Health Insurance Portability and Accountability Act (HIPAA)[3] may apply to certain records maintained by state and local government agencies.
- Federal regulations regarding Child Protective Services may apply to state and local agencies.

Ultimately, your security policies will allow your agency to:

- Control and reduce its exposure to risks, vulnerabilities, and compromise of your IT systems and their data to levels you deem acceptable, or that are mandated by some overarching law or policy.
- Define what outcomes need to be measured so that you can continuously assess the effectiveness and appropriateness of your security policies.

Let's take a quick look at the common risk factors in a law enforcement IT system and how security policies mitigate these risks.

What Are the Risk Factors to an IT System?

Risk may come from a variety of sources both internal and external. Generally threats to systems and data security come from these sources:

- **The system itself**

  Computer systems, because of their design, may have a variety of inherent vulnerabilities. For example, a system may use an unencrypted database and have a default password length that is inappropriate (i.e., too short or uncomplicated and therefore easier for a hacker or some other malicious attacker to crack) for the kind of data being protected. We have all experienced security breaches inherent in mainstream products and operating systems that require us to regularly download system "fixes" or "patches" from the Internet when a vulnerability is exposed (think of the viruses that are rapidly spread over the Internet via e-mail).

A security policy is essentially a distillation of any number of risk factors and the strategy for their resolution.

- **How the system is used**

  Until you investigate *how* a system is used, you will not know what additional exposures may be present. Often, the system itself may be secure, but methods of using the system create vulnerabilities. For example, if an IT department backs up an RMS before it is encrypted, then anyone who can access the back-up tape could access any data on the tape. This exposure would be completely outside of the normal operation of the system.

[3] Public Law 104-191.

"Some information security experts believe as much as 80% of security problems stem from lack of understanding or carelessness, not direct attack. Examples like the I Love You *virus (which infected only those who opened both an unexpected message and its attachment), sloppy administration and use—even sharing—of passwords, and leaving computers logged on and unattended are dangerous, yet common examples of the need for greater security awareness."*

— Charles Le Grand, "Information Security Governance," in *ITAUDIT* (vol. 4, Feb. 15, 2001)[4]

"Effectively mitigating the insider threat requires policies, practices, and continued training." —***The National Strategy to Secure Cyberspace*, p. 40, February 2003, President's Critical Infrastructure Protection Board**

- **People—intentionally and unintentionally**

  People are often the weakest link in the security chain, whether they mean to be or not. Clearly you must assess your vulnerability to attack by malicious hackers, criminals, and/or disgruntled individuals or employees. That scenario certainly presents specific types of risks.

  People also pose a great risk when they *inadvertently* misuse a system or they are not educated on proper system usage. People often compromise security simply because of human nature. If you have adopted a password policy that requires long and complicated passwords, for example, do not be surprised if users write them on a sticky note and put it under their keyboard. If you require burdensome paperwork to move backup tapes around, people may simply stop using the system because they just want to get their job done and move on to what they consider to be more important tasks. Or, as in the earlier example at the university, the staff member inadvertently backed up sensitive data onto a web server that allowed public access to the documents via the World Wide Web. It is not that there is malicious intent, necessarily, in these scenarios, but rather the failure of individuals to understand that their actions and/or use of the system could compromise the system and/or its confidential data.

- **Natural disasters**

  Certainly your system—like any other agency assets—could be damaged, entirely lost, or compromised during a flood, fire, earthquake, or other natural disaster.

[4] Available at **http://www.theiia.org/itaudit/index.cfm?act=ITAudit.archive&fid=132**.

- **Not knowing and/or not meeting your mandated responsibilities**

  You could jeopardize your system and expose your agency to liability if you are not aware of or have not complied with existing legislation, laws, policies, and other regulations relating to the secure operation of your system and/or those that interact with it.

  Any number of laws, such as the Computer Security Act of 1987 (Public Law 100-235) or the Federal Information Security Management Act of 2002 (FISMA), may affect how you protect your data because these laws create minimum acceptable security practices. The Computer Security Act of 1987 provided for the establishment of standards for improving security and privacy of information on federal systems. It also assigned to NIST (then the National Bureau of Standards) the responsibility to establish standards and guidelines for federal computer systems. FISMA updates much of the 1987 act and in part states: "... provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities... ."[5]

  Your state, county, or city may have additional legislation and/or policies that may affect you. In addition, users of the FBI's CJIS will need to adhere to the latest CJIS security policy. Failure to adhere to these existing laws, regulations, and policies could leave your systems at significant risk and you and your agency in a position of liability.

- **Limited capacity to address IT security risks**

  Let's face it, many organizations are limited in their ability to adequately address security risks that may face them. In addition, sometimes managers must decide that they can only mitigate a risk to a certain extent, which may stop short of the highest possible levels of security. Perhaps implementing higher security levels are just too costly or the agency lacks the expertise to properly implement and manage the activities to secure a system at that level. That means that the agency assumes a level of risk, simply by knowing that the likelihood exists that something could occur based on that decision.

[5] 44 USC 3541.

Evaluating Risk Is Key to Developing Security Policies

Assessing risk under these broad categories will provide management the information it needs to determine the extent of potential threats to and risks associated with a specific IT system. Understanding, analyzing, assessing, prioritizing, and mitigating risk becomes the foundation for developing an agency's security policies. The rest of this guide, you will find, focuses heavily on activities surrounding this analysis of risk. Once an agency evaluates the information developed during the risk-assessment process and prioritizes the identified risks in order of their importance, it can then develop specific procedures to address the risk. At the end of this process, the agency will balance the most appropriate procedures for implementation that will reduce (or mitigate) risks to an acceptable level for the agency.

A key component of a robust security program is implementing a *continuous* process to evaluate the effectiveness of the security policy. For IT systems, the only constant in the system is that it will change. Consequently, as changes are made to the system, new risks will be discovered and old risks may go away. The agency must continually evaluate and assess the effectiveness of the security procedures to ensure the level of risk is still within the acceptable range by management.

How Security Policies Control Risk

It is impossible or impractical to completely eliminate all risk; therefore, developing risk mitigation strategies, and the resulting policy, seeks to find the security procedures that do the following:

- Minimize the total costs for the agency
- Are the most appropriate to reduce agency risks to an acceptable level
- Create the least adverse impact on the agency.

If security policies are well-thought-out, implemented properly, and monitored for effectiveness, then management will have successfully contemplated:

- The goals of the organization, how technology supports them, and how security ensures their safety
- The security exposures to the agency and how established procedures reduce risk levels
- Requirements of existing legislation, agreements, or other policies that dictate the level of security required for the system
- That deviations from the expected risk levels will be detected
- That the cost of the security is within bounds established by management.

Given what is involved in assessing risk, making decisions about acceptable levels of risk, and instituting organizational policies to address the risk, it should be clear that law enforcement managers play a key role in developing, implementing, and maintaining IT security policies. So let's get started!

The question is no longer can we afford security, but can we afford to do business without it?

—University of Georgia,
Office of the Chief Information Security Officer[6]

[6] Source: **www.infosec.uga.edu/ciso/quotes.php**.

CHAPTER 2
ORGANIZE AND CHARGE THE SECURITY POLICY DEVELOPMENT TEAM

"A successful security program starts with the senior management of the institution empowering a Security Officer and flows down through the security team members…."

—University of Georgia,
Office of the Chief Information Security Officer

Chapter 2: Organize and Charge the Security Policy Development Team

What An inclusive and representative team that will be responsible for all aspects of security policy development, implementation, and evaluation.

Why To ensure that the right people are involved to perform systems analysis, identify risk, and make security decisions.

Who The policy development team consists of a variety of stakeholders within the organization from the chief/sheriff to managers, to users and line staff.

When Now! Establishing the security policy development team must be the initial task taken on by executive managers involved in the project.

"Projects, like police organizations, require structure and disciplined rules if they are to be successful. The decision-making structure (in this case, the Security Policy Development Team) defines the 'chain of command,' documenting the roles and responsibilities of the various people responsible for project actions."

It is important to include representatives of the various stakeholder groups within the agency not only for buy-in to the initiative, but also because each representative will bring his or her knowledge and expertise of some specific aspect of the information technology (IT) systems that will be critical in developing the security policies.

A security policy development initiative begins like all other IT efforts. It requires a sound decision-making structure, an effective leader, and the development of a solid plan.

Standards of Due Care

"Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. Management must also assess and incorporate the results of the risk-assessment activity into their decision making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management."

— NIST Special Publication 800-30,
Risk Management Guide for Information Technology Systems

Step 1

Get Senior Leadership to the Table

Creating effective information security policies requires the leadership and involvement of the agency's senior management. Managers are responsible for the following:

- Providing the leadership and accountability for your agency's security policy development
- Understanding the information security process and how it relates to your agency
- Allocating resources to security policy development (human and financial)
- Establishing acceptable risk levels for your organization based on analysis conducted
- Creating the security policies
- Reviewing, approving, and instituting a program to ensure that the security policies remain effective.

Management support in the security process is critical to its success for the reasons noted above because most IT systems cross organizational boundaries. It is only with management's overarching support that rational security policies can be adopted and implemented for the entire organization. Management involvement will also help resolve any intra- and/or interagency issues that may develop.

Step 2

Identify Stakeholders

Access to the National Crime Information Center (NCIC) and criminal justice information systems are examples of intangible assets for a law enforcement organization. Maintenance of these rights necessitates conformance to a certain set of policies set by the FBI. Failure to meet and maintain these standards may result in revoking access rights to NCIC and CJIS.

Identifying stakeholders and obtaining their input and support during your agency's efforts to develop and implement effective IT security policies is also critical to the success of your initiative. Stakeholders are individuals who use, access, manage, and/or are responsible in some way for the security of your networks and information systems. **Remember that some stakeholders can be external to your organization.** Each stakeholder will have different needs and points of view depending on the security interests of his or her role and position within the agency.

When you begin this effort, a list of obvious stakeholders will come to mind. This initial group usually consists of people from your own agency who will be affected by the undertaking: senior management, system owners, administrators, and user groups. There can also be other persons or groups who should be involved because they process or access data from the IT systems. These stakeholders could be other agencies, persons, or positions that are in some way linked to the system or its data by virtue of its operation, legislation, regulations, and/or policies. Your project manager needs to identify and help create this stakeholder team. The success of the security initiative can often rest on having the right people selected for this team!

A good way to identify some less-than-obvious stakeholders is to start by asking a series of abstract questions. Some of the questions you may want to ask are:

- Who are the unrepresented constituencies?
- Who are the representatives of those likely to be affected by any changes implemented?
- Who can make the effort more effective through his or her participation?
- Who can make it less effective by his or her ***non***participation?
- Who might outright oppose the project? (This could include individuals within or outside the organization who may mobilize against the project.)
- Who can contribute financial and technical resources?
- Whose behavior has to change for the effort to succeed?

NOTE

Remember, governance and decision-making structures can change as you dive deeper into your project. Along the way, you will likely discover other parties who have access to your systems and/or data or are in some way affected by these systems. As you identify these parties during the process, you need to analyze whether they may need to become part of your Security Policy Development Team.

Anyone within your agency is potentially an information system security stakeholder. Some positions, however, have a greater stake in IT security than others, such as:

1. Agency executive.
2. Head of major agency divisions, such as Investigations, Field Services, Records, and Dispatch.
3. Internal IT staff.
4. External IT staff.
5. City/county/state IT manager.
6. External user group.
7. Information-sharing partners, such as the courts, prosecutor, and probation.

Because of the potential effect the stakeholders have on the initiative, it is essential to establish a *representative* stakeholder team. It is only when you achieve stakeholder buy-in that your project can create effective security controls and have a reasonable expectation that they will be completely implemented.

Determining an appropriate group to serve in this capacity is also a balance. You need enough participants to achieve solid and comprehensive representation, but not so many that the group becomes unwieldy. We often suggest that working groups consist of eight or fewer individuals. Otherwise, scheduling meetings, having successful working sessions, and other project activities become just too difficult to orchestrate. Keep in mind that you can always solicit broader input from more individuals through a variety of methods, such as surveys, forming ad hoc groups to focus on an issue, or holding informal meetings.

Step 3

Assign a Project Manager

Not sure of the qualifications of a good project manager? See Chapter 2 of the original *Law Enforcement Tech Guide* for guidance on this important task.

Depending on the size, scope, and scale of your security policy initiative (are you developing policies for the entire agency's IT resources, or are you focusing on a specific, smaller system?) you may need to assign a full-time project manager. For the smaller undertaking, you most likely will be able to assign someone within the organization to take the lead and to be responsible for all aspects of project management: meeting deadlines, communicating with all affected groups, project documentation, Steering Committee liaison, etc. (chief or sheriff: make sure you give them the time they need to do this!)

For a more comprehensive discussion of outsourcing project staff support and how to determine if it's right for you, consult the original *Law Enforcement Tech Guide*.

In the case of a more expansive initiative, a single individual ought to be dedicated full-time until the security policies and evaluation measures are developed and finalized. A project manager can come from within the organization, or you may want to outsource the responsibility for leading the security policy development effort.

A project manager for a security initiative should have a solid combination of security and technical skills and project management experience. This is necessary because of the wide range of issues that arise in an effort of this type. The project manager also needs to have access to the Steering Committee and chief/sheriff on a regular basis to keep them informed about progress, status, challenges, and obstacles.

Step 4

Create a Governance Structure with Roles and Responsibilities

The stakeholders that you have identified have differing roles and responsibilities. There are many ways to configure a governance structure, but here is a model we recommend that seems to work for most agencies, regardless of their size (Figure 2):

Too much governance? You may be looking at this governance structure and thinking, "Wow, this looks just like the structure we already have in place for broad IT planning and implementation." If so, then good for you, and we suggest that you incorporate this structure within that governing body. Indeed, it would be best if the IT Security Policy Development Team was always a core part of overall IT governance within a jurisdiction or organization.

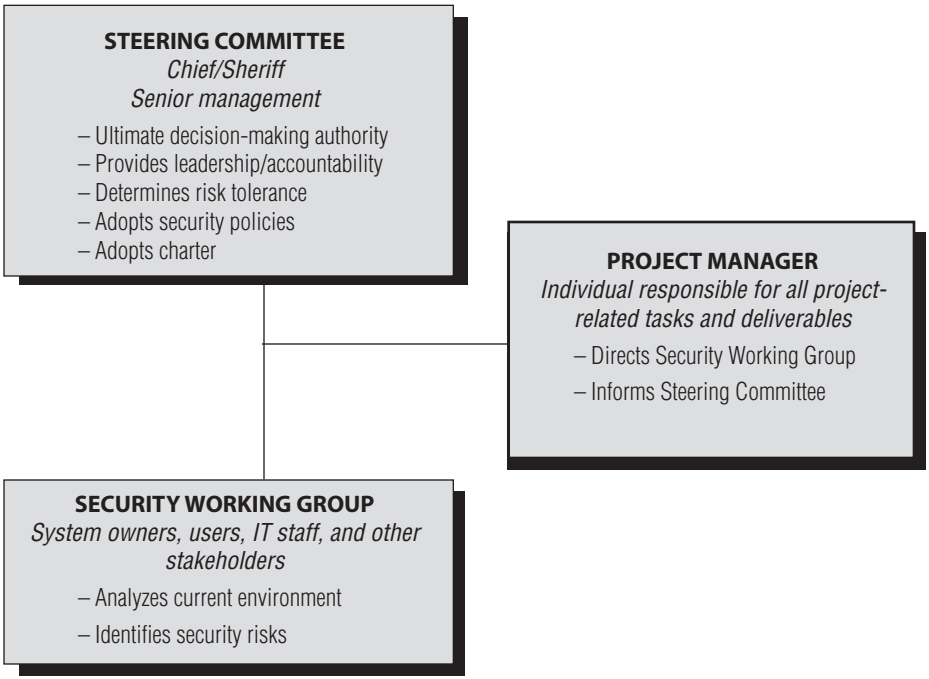


Figure 2: Security Policy Development Team

Your initial attack on this effort will be very active with the Steering Committee and the Security Working Group. Be aware that the Steering Committee should never cease to exist. Its continued presence helps to ensure that you maintain the security development process. Having strong security policies is a long-term project. Once you move from the active state of assessing and improving your security, you enter a long-term maintenance mode.

Steering Committee

The Steering Committee needs to include the chief or sheriff, and any other members of senior management within the organization. These folks will assign and commit staff within the department to participate in this initiative. Their most important role will be to constantly and consistently provide guidance and oversight to the effort. Ultimately, they will have the critical task of reviewing the Security Working Group's project deliverables, making determinations about how the organization will deal with risks and vulnerabilities to its IT assets, and settling on the policies to help protect them. When they make these decisions, they will be making them in a fashion that supports the organization's business mission and objectives, and that considers the agency's budget and resources.

Project Manager

This is the individual who serves as the ringleader for the entire security effort and is the "go-to" individual for all related information. At the direction of the Steering Committee and working in conjunction with the Security Working Group, the project manager makes sure that project management best practices are followed for security policy development. This individual will make sure that the effort is properly scoped; deadlines and milestones plotted and met; deliverables remain on schedule; all activities are documented, organized, and archived; and constantly communicates with all members of the team and other interested parties concerning the status of the security effort.

The Steering Committee must empower the project manager and any other staff who are engaged in this effort with the resources, training, and guidance they need for its success.

Security Working Group

The Security Working Group is where all of the real action takes place. This group assists in all of the assessment and analysis activities regarding existing IT systems and their current security policies. The group identifies risks and vulnerabilities and potential procedures to control them that are then presented to the Steering Committee for resolution. This group will understand all aspects of the current IT security environment and make recommendations for how it can be improved. Its work directly influences the decisions made by the Steering Committee.

The Security Working Group consists of those who know the day-to-day operations of technology, who use it consistently, who are managing the agency's IT systems, or who otherwise are affected by the agency's IT.

Step 5

Review Your Agency Mission and Objectives

As asserted in the original *Law Enforcement Tech Guide*: "IT must support the strategic business mission, goals, and objectives of the law enforcement agency. Information technology can be an effective tool for any business to meet its overall strategic objectives. But first, those business objectives must be outlined in a strategic plan. Then, information systems can be designed to meet those business objectives."

As you begin your security policy development initiative, go back and read your organization's business mission. Then review the IT strategic plan. Those documents will be critical to guiding your approach to systems security.

Properly designed computer security enhances the ability of an organization to meet its objectives. In addition, it provides a basis to protect the valuable resources used by the organization.

The following is an example of how important IT security is in meeting an organization's mission:

> In 1999, the Metropolitan Police Department in Washington, D.C., wrote that "information technology...makes it easier for the MPDC to share information with the community quickly and effectively. As such, new information technology is a critical part of the MPDC's evolving strategy of community policing and crime prevention."
>
> —From *Information Technology and the MPDC: Moving Into the Next Century* (p. 1)

The department's focus on sharing information with the public means that MPDC plans to interact with and provide important information to the community so that it can be involved and make informed decisions. This statement clearly highlights the implications for securing confidential data (need to know, who is able to see what types of information), making sure the data are accurate (integrity), that the data are not compromised (secured), and that they are available to share. These considerations will drive many of the security policies adopted in such an organization.

Sharing information in an agency gets more complicated when you begin to delve deeper into numerous agency objectives that deal with the complex aspects of policing, intelligence information systems, and first response.

Step 6

Allocate Resources

You will need to allocate time and resources (both human and financial) to develop and implement a security policy process. The first step is to make sure your staff has the time it needs to participate in this effort. Most individuals participating on the working group, in particular, are also responsible for their full-time duties; therefore, you must carve out time for them to work on the security initiative.

Once new security policies are in place, implementing them may cost money, as will continually evaluating the effectiveness of those policies and developing new policies as they are needed.

Step 7

Adopt a Methodology and Plan of Action

You need to plot a course for how you will develop and implement your security policies. While there are many different methodologies to choose from, we suggest the following steps in IT security policy development that will form the basis for the rest of this guide.

Phase I: Conduct a Self-Assessment. The activity your Security Policy Development Team will undertake is a thorough self-assessment of your existing IT system(s). The purpose of this assessment is to identify and catalog all the information you have regarding the IT system and its operation. When the assessment is complete, you will know what you are doing today to secure the system and your legal and contractual obligations for secure system operations.

Phase II: Assess Security Risks. Next, you will examine the assessment information collected during Phase I, identify the security risks to the system and, together with management input, determine the agency's tolerance for each risk.

Phase III: Develop a Mitigation Strategy through Security Controls and Procedures. In this phase, the team develops the security controls and/or procedures necessary to mitigate the risks identified in Phase II. The controls require technical skills of staff who are familiar with the IT system, and managers and supervisors who are familiar with the system workflow. Once the security controls are developed, they are implemented.

Phase IV: Develop and Implement Measurements to Monitor the Effectiveness of the Security Controls. In this phase, the team develops and implements procedures to monitor the security controls to ensure they are effectively reducing IT security risks to the levels specified by management. This phase is your "insurance

policy" that risk levels are maintained at the appropriate values.

Once the work in Phases I through IV is complete, the Security Policy Development Team can now create the agency's IT security policies. Policies should be formulated based on an identified risk and the controls developed to mitigate that risk. When implemented, they can be assured of their success and properly measured. The developed policies following this formula will meet the risk levels that are acceptable to the agency's management.

All of these phases need to be accomplished in a logical manner, and using project management best practices. See Chapters 9 through 11 of the original *Law Enforcement Tech Guide* for details on how to create a project timeline, scope, budget, and general processes to be followed.

So, have we piqued your curiosity? Or have we scared you off? We hope the former! Let us give you a sneak preview of the entire security policy development process as applied to a probable scenario in a law enforcement agency. We will walk you through all the phases of security policy development here. Each phase is the basis for the rest of the detail in this Guide. Enjoy!

Sample Security Policy Development and Implementation Scenario

Let's take a look at a sample law enforcement IT system scenario to help us understand what security policies are, how they are developed, and how they are used. The following scenario, as illustrated in Figure 3, is very simplified, but it will help to explain the basic security concepts.

The Security Project

A police department in a medium-sized city decides to purchase a records management system (RMS) to automate and standardize record-keeping activities for criminal investigations. Additionally, the mayor and city council have mandated that all city departments must use the city's IT department for all server-based applications. Accordingly, the RMS was purchased and installed on a city server for the exclusive use of the police department. (For this scenario, we are calling it the Anytown Police Department.)

Phase I	***Conduct a Self-Assessment***
	Phase I in the security policy development process is to conduct a self-assessment of the existing system to gather and identify detailed information about the agency's current system security environment. The Anytown Police Department's security policy team does this, and the information collected is used to inform Phase II of the process.

Figure 3: Sample Security Policy Development/Implementation Scenario

Phase II	***Identify and Assess Risks*** Phase II involves using the data gathered in the self-assessment phase to identify security risks in the system, and then categorizing and quantifying these identified risks to determine the likelihood of the risk occurring, the severity of the risk, and the agency's tolerance for each risk (either to avoid the risk, assume it, mitigate it, or transfer it). During the risk assessment, the Anytown Police Department's security policy team identifies the following security issues: A. The database is not encrypted. B. The RMS is connected to the city network and there are no firewalls or other routing controls to limit connections to the case management server. C. The RMS requires passwords for access, but they can be any length of four characters or more. D. City employees are used as IT system support personnel. However, as a cost-cutting option, the city also has contracted with a temp agency for part-time support personnel. For any risks that your agency determines must be mitigated, the security policy team then designs a risk mitigation strategy through the use of controls and procedures (Phase III).
Phase III	***Develop Security Controls to Mitigate the Identified Risks*** Phase III involves developing security controls necessary to mitigate the risks identified in Phase II. The following controls were crafted by the Security Policy Development Team in response to the risks they identified: A. The department technical liaison officer should investigate the possibility of acquiring a software upgrade for the RMS that would encrypt the database. B. Limit access to the RMS server to department management and investigators. C. A password of at least eight characters in length will be required for access to the RMS. D. Because nondepartment personnel have potential access to criminal investigation data, all persons who have potential access must undergo an annual criminal background check. Most people would stop the security policy process at this point and declare the battle won. However, the only constant with IT systems is change. Thus, measurements must be put in place to ensure the controls are, and remain, effective (Phase IV).

Figure 3, continued

Phase IV	**Develop and Implement Security Measurements** Phase IV involves developing and implementing measures to monitor the effectiveness of the security controls. The Anytown Police Department's policy team creates the following ongoing methods for measuring security policy effectiveness: A. The department's technical liaison officer verifies annually that the RMS software database is encrypted. The officer may require assistance from the IT system staff for this activity. The first check is done 1 week after the software upgrade is installed and is done independently of the software installation. A report is submitted to the chief annually. B. The technical liaison officer reviews the network connections to the RMS annually. With the assistance of the IT systems staff, router and firewall configurations are reviewed to verify that only department users can access the case management server over the city network. C. The technical liaison officer is directed to request a file of the encrypted RMS passwords annually. A dictionary-cracking program is run against the passwords to determine if any can be cracked. The first test of the password file is to occur 1 month after the software has been modified to support the new password policy. A report of the number of cracked passwords is submitted to the chief. D. The department's personnel officer audits the IT system staff records annually to verify that all IT system personnel, both city employees and contractors, have undergone a criminal background check. The first audit is conducted 3 months after the city personnel policy is revised. A report of the results of this check is prepared and submitted to the chief.
	Write the Policies At this point, the agency leadership and Security Policy Development Team are ready to write the IT security policies, building on the work that has been accomplished in Phases I through IV. Anytown Police Department thus creates the following policies for each identified risk: A. All data related to criminal activity or investigations within the department must be encrypted. If encryption is not cost effective, the data must be under the direct control at all times of a sworn officer of the department. B. All network access to department servers containing confidential and/or criminal data shall be limited to authorized users. C. Access control to any department system containing classified and/or criminal data shall require a password of at least eight characters and shall contain at least one nonalphanumeric character. D. All nonsworn personnel having potential access to confidential or criminal data must undergo an annual criminal background check.

Figure 3, continued

Figure 4 illustrates the relationship among the identified risks, controls, measures, and policies in this scenario.

This identified risk…	…resulted in this control,	which is monitored by this measure.	The policy the agency created and implemented:
The database is not encrypted.	The department technical liaison officer should investigate the possibility of acquiring a software upgrade for the RMS that would encrypt the database.	The department's technical liaison officer verifies annually that the RMS software database is encrypted. The officer may require assistance from the IT system staff for this activity. The first check is done 1 week after the software upgrade is installed and is done independently of the software installation. A report is submitted to the chief annually.	All data related to criminal activity or investigations within the department must be encrypted. If encryption is not cost effective, the data must be under the direct control at all times of a sworn officer of the department.
The RMS is connected to the city network and there are no firewalls or other routing controls to limit connections to the case management server.	Limit access to the RMS server to department management and investigators.	The technical liaison officer reviews the network connections to the RMS annually. With the assistance of the IT systems staff, router and firewall configurations are reviewed to verify that only department users can access the case management server over the city network.	All network access to department servers containing confidential and/or criminal data shall be limited to authorized users.
The RMS requires passwords for access, but they can be any length of four characters or more.	A password of at least eight characters in length will be required for access to the RMS.	The technical liaison officer is directed to request a file of the encrypted RMS passwords annually. A dictionary-cracking program is run against the passwords to determine if any can be cracked. The first test of the password file is to occur 1 month after the software has been modified to support the new password policy. A report of the number of cracked passwords is submitted to the chief.	Access control to any department system containing classified and/or criminal data shall require a password of at least eight characters and shall contain at least one nonalphanumeric character.
City employees are used as IT system support personnel. However, as a cost-cutting option, the city also has a contracted with a temp agency for part-time support personnel.	Because non-department personnel have potential access to criminal investigation data, all persons who have potential access must undergo an annual criminal background check.	The department's personnel officer audits the IT system staff records annually to verify that all IT system personnel, both city employees and contractors, have undergone a criminal background check. The first audit is conducted 3 months after the revised city personnel policy is changed. A report of the results of this check is prepared and submitted to the chief.	All nonsworn personnel having potential access to confidential or criminal data must undergo an annual criminal background check.

Figure 4: Relationship Among Risks, Controls, Measures, and Policies

CHAPTER 3
PHASE I—
CONDUCT A SECURITY SELF-ASSESSMENT

"Security needs to be built in from the start—not slapped on after the fact."

—Gene Spafford, Professor of Computer Sciences,
Purdue University

Chapter 3: Phase I—Conduct a Security Self-Assessment

What Gather and identify detailed information about your agency's current (as-is) system(s) security environment in three categories: Management, Operational, and Technical.

Why Understanding the environment in which your system is currently operating, and the rules (or lack thereof) governing its operation, maintenance, access, and security, will help you identify where the system may be subject to vulnerabilities.

Who Senior management, project managers, administrators, and users may be called upon by the Security Policy Development Team to contribute to gathering and organizing the self-assessment inventory for your agency.

When The self-assessment inventory should be the first activity your security policy team undertakes and completes. Since this inventory process will take some time to accomplish properly, it is best if this phase of the security policy initiative is started promptly at the project's inception. (You need to hit the ground running.)

Security self-assessment is a method by which your agency can understand where it is today in terms of providing security for information technology (IT) systems. Think of the assessment as an "as-is" of the state of your organization's IT security. It is an exercise that will help you bring together any guidelines, rules, procedures, controls, and informal activities currently in place that impacts a specific IT system's security. In most state and local law enforcement agencies, there are many policies, procedures, and methods in place to secure IT, but generally they are not located in a single place, nor have they been rationally organized into a single document. Sometimes they are just things people in the organization "know" but that have never been written down. Conducting a self-assessment will help you bring together all those critical guidelines and methodologies to allow you to successfully explore your environment.

The completed self-assessment informs all future phases of the security policy development process, and, in particular, forms the basis for successful risk assessment and security policy development. You can conduct a self-assessment of one system, many systems, or part of a system, depending on the scope of your project.

Creating a comprehensive "inventory" of information about the *management, operational,* and *technical environment* of the system or systems is the crux of a self-assessment.[7] As you will see, it involves collecting detailed data and information about each of these areas, which individuals—both inside and outside your organization—are responsible for them, and any existing formal or informal rules, policies, and procedures governing each.

It is best if your agency accomplishes this inventory itself because your staff:

- Understand how your systems work
- Are the most aware of the intricacies of the system
- Are the most familiar with how the system is actually used
- Will learn even more by handling the self-assessment internally.

While there are a number of self-assessment guides or audit checklists available for a fee or free on the Internet, remember, these are just guides and no publication can provide your agency with an all-inclusive list of the security issues that you need to be aware of. ***It is management's responsibility to understand the current status of their IT systems and controls so they can make informed decisions to appropriately mitigate risks to an acceptable level.***

The Self-Assessment Process

This process is really quite straightforward—it just requires time, research, legwork, and organization! Here are the steps we suggest you follow to complete this process:

1. Identify which systems, single system, or part of a system for which you will be developing security policies.
2. Assemble the appropriate participants for the process and hold a kickoff meeting.
3. Gather relevant organizational data regarding the IT systems to be assessed that addresses management, operational, and technical system issues.
4. Conduct the self-assessment by ranking the level to which the agency has developed, implemented, and evaluated policies, procedures, and controls regarding the management, operational, and technical components of the subject systems (and yes, we have a questionnaire you can use to guide you through this).[8]
5. Compile the results of your self-assessment, which will become the basis for your agency's IT security risk assessment (detailed in Chapter 4).

---

[7] The key areas of the self-assessment—*Management, Operational*, and *Technical*—are taken from the NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems* and Revision 1 of NIST SP 800-26, *Guide for Information Security Program Assessments and System Reporting Form* and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems.*

[8] Refer to Appendix A for a description of this self-assessment questionnaire. Specific questions are listed beginning on page 126.

Step 1

Identify the Systems, Single System, or System Part for Which You Will Develop Security Policies

Many law enforcement agencies do not have formal and clearly articulated security policies for their IT systems. If your agency falls into this category, we recommend you take an enterprise look at your IT holdings and develop policies governing all of them. Of course, this means much more work than, say, just looking at one system, but there is a danger that any policies or procedures (including those surrounding IT security) are only as good as the weakest link in the system. Thus, if you have comprehensive policies and procedures for one system, but not another, are you merely defeating your security goals in the long run? This becomes even more problematic if the systems are integrated.

List the systems and/or locations that you initially want to include for your security self-assessment activities. As the self-assessment project progresses, you may discover that you need to add more systems/locations to your list as you discover how your system is used or how it is interconnected to other systems. (Note, if you add additional systems, it may also affect who will be part of the self-assessment team described in Step 2.)

- For each location in your list, create a list of the IT systems that you want to assess.
- For each system, create a list of people who understand the system, both technically and functionally.

Step 2

Assemble the Appropriate Participants for the Process and Hold a Kickoff Meeting

As discussed in Chapter 2 regarding assembling the Security Policy Development Team, it is important that key individuals not only participate in the self-assessment process, but also that they understand *why* conducting the self-assessment activity and doing it completely and accurately is so important. Take the time here—now that you have determined the scope of your project—to make sure you have the right people involved.

We know that the **executive sponsor** of the agency must be involved, as well as top **management** whose divisions or units are affected by the system and policies you are developing. The **project manager**, as you already know, is also key to successful completion of your policies. At this time it is important that you make sure you also reassess the involvement of the following individuals or teams in your policy development team:

- **Administrators**: These are the actual administrators of the various parts of your system that will be assessed. This may be a single individual or several administrators of multiple systems. Each plays an integral role in the development, implementation, and maintenance of the system and, thus, an important part of the assessment process.
- **Data owners:** Individuals who are responsible for the proper maintenance and care of the data that resides in a particular system are integral to this effort. They will understand the rules, policies, and regulations regarding capturing, maintaining, and disseminating the data stored in the IT systems. Because they are ultimately responsible for the data, they will be key to developing the right security policies.
- **System owners and users:** System owners could include persons outside of the agency who actually own the hardware that contains your data. They may be part of the larger community government or an agency that by agreement stores your data. Including them in the process will be important to obtaining correct information during the assessment process. Users may be obvious—their inclusion is always important for gaining acceptance.
- **Legal assistance/research:** Your security policy team may need help in locating and assessing legislation, agreements, and/or agency policies that may affect the operation of the IT systems under review. If not legal counsel, your agency needs to assign someone the task of researching these important documents.
- **External system users/contributors and/or beneficiaries**: Your staff may also need input from and access to external resources. Part of the self-assessment process is to understand what data or operational links exist between the system being assessed and any other system, be it internal or external to your agency.

Once you determine the individuals who will participate in the self-assessment, you should hold an initial meeting to discuss the process of self-assessment, including the following steps.

Step 3

Gather Organizational Data

You must now gather a variety of relevant organizational data regarding the IT systems that will be assessed. In November 2001, the National Institute of Standards and Technology (NIST) laid out a methodology to facilitate the self-assessment process by organizing it into the three broad categories: **Management**, **Operational**, and **Technical**.[9] We believe this remains one of the most appropriate, streamlined,

[9] This methodology appeared in NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*.

The project manager should be the point person and repository for all information collected during Step 3.

and straightforward approaches for state and local law enforcement agencies to organize information pertaining to their IT systems. The information gathered in these three categories will form the basis for the self-assessment process.

The best place to begin your data collection is by talking with the owners of the IT systems under review. These are the people who, among other things, may be responsible for funding the system, or responsible for the data in the system, or for the access to and use of the system. In addition, the actual users of the system can provide good information about the system as it relates to security. Throughout this process, you are trying to determine:

1. How and where your IT systems are accessed.
2. What are management's expectations of how the system is used?
3. What are the legal or policy requirements that pertain to the system?
4. How many people actually use or maintain the system?
5. Where the system documentation is located, and how accurate is it?

The self-assessment process itself is not a 5-minute exercise! It will take some time to complete and it will require you to do quite a bit of research. Your goal is to try to really understand your IT system so that ultimately all potential risks are discovered.

For your benefit, we have created a list of possible information sources that you should research and collect. As preparation for the self-assessment, you should gather and organize as much of the following information as possible. Obviously, each agency is different, so your agency may or may not have some of the sources listed below. If this is the case, you should try to locate other similar sources of information unique to your environment that will be helpful to your security activities.

Here are your categories of information collection and why they are important:

Management Information

The **Management** category addresses how IT systems are managed, including identifying risks to the system. It includes questions about such issues as:

- *Risk Management*: Whether the organization has a risk-management process in place and whether it takes steps to reduce and maintain the risks at an acceptable level.
- *Security Reviews*: Whether the organization has implemented routine evaluations of and responses to identified system vulnerabilities.
- *Lifecycle*: Whether security policies and procedures development and maintenance is part of the technology lifecycle development process within the agency. (Meaning it is dynamic, not static.)
- *Certification and Accreditation*: Normally reserved for federal agencies' compliance for certifying their IT systems in accordance with NIST guidelines.

As we begin describing the information to collect, you will note it is voluminous. We have created a tool to help facilitate the assessment process, downloadable at **www.search.org**. It is in Microsoft Excel spreadsheet format and is described in more detail starting on page 61.

You may also use **Appendix A: Assessment Worksheets and Questions from the SEARCH Information Security Self- and Risk-Assessment Tool** to help you through this chapter.

However, many state and local agencies fall under these rules based on the data that they maintain according to federal programs (such as compliance with Health Insurance Portability and Accountability Act [HIPAA] regulations or Child Protective Services regulations).

- *System Security Plan*: Does the agency maintain a formal security plan that includes the security requirements of the system(s), as well as procedures to fulfill those requirements? The plan should delineate individual responsibilities and expected behavior of all individuals who access, maintain, and otherwise interact with the system.

Here are the types of organizational information you should collect to inform the management self-assessment.

1. **Controlling organizations.** Identify and list all the controlling organizations of your agency, up to and including the federal level, if applicable.
   a. If you are a local police department, the first level outside your agency will probably be your city or county government.
   b. If you are working at the state level, you may not have a controlling *organization* if the head of your agency already reports to the governor or a state legislative committee; nevertheless, your agency will be responsible to these entities in a similar manner—with often more pressure due to the political sensitivity.
   c. The federal level becomes important if your agency either uses services from or receives funding from a federal agency.

   The list you develop should contain the following information at the minimum:

   - Agency name.
   - Relationship to your organization.
   - The areas of control related to your organization. What oversight does this agency exercise with respect to your organization?

- The first-level contacts within those agencies that your people would normally contact. These are the "go-to" people in the other agency.

2. **Business/mission statement(s) for your agency.** These should be easily located in your agency's strategic plan.
3. **Audit reports.** These documents will potentially provide you with a lot of good information related to your organization and IT systems. Specifically, you need to identify and collect any audit reports created that relate to:
   a. Your agency—the audit reports may have been created for any purpose (financial, security, or otherwise).
   b. The IT infrastructure—the audit reports may have been created for the data network, physical security, emergency preparedness, and so forth.
4. **Policies/procedures.** Collect existing policies, procedures, memoranda, and so forth, related to IT systems control and/or IT security in particular and or any other compliance requirements based on law or agreement (for example, the FBI Criminal Justice Information Services [CJIS] Division's *CJIS Security Policy*, HIPAA, Sarbanes-Oxley Act,[10] and so forth).
5. **Building design and construction details.** Collect these for any location housing IT systems or users of IT systems that are part of this self-assessment activity.
6. **Project-related documents.** Obtain, if they exist, the project plans, project specifications, proposals, requests for proposals (RFPs), and other documents for all IT systems that are part of this self-assessment.
7. **Existing agreements.** Do any agreements made between your department and any other entities relate to the IT systems that are part of this self-assessment? Some examples of such agreements may be the following:
   a. Service-level agreements—these agreements typically are between the service provider (usually an IT department, which may be part of another agency) and your organization.
   b. Availability agreements—these typically would be made with your end users to guarantee system availability. In addition, they may also cover their responsibilities to maintain security, confidentiality, and controlled access to the system.
8. **Position description and related correspondence.** Identify the most senior person in your organization responsible for each IT system under review.
   a. Obtain a copy of his or her job description.
   b. Obtain any memos or letters of understanding addressed to this person that are related to the IT system under review.

[10] Public Law 107-204.

9. **Responsible party information.** Identify the organization that is responsible for maintaining the IT system. Gather the following information:
   a. If the IT system is a commercial product—
      i. License agreement.
      ii. Support agreement.
      iii. Policies and procedures related to maintenance and support of the IT system.
      iv. Documentation of how the organization maintains system records regarding changes, modifications, and/or upgrades.
   b. If the system was developed in house (this may be the city or county IT department)—
      i. System design documentation.
      ii. Copies of structured walk-throughs or other development documentation that was created when the system was built.
      iii. Maintenance logs.
      iv. Requests for system changes/modifications.
10. **Budget information.** Obtain the initial and subsequent budget proposals and justifications for the IT system. Determine the financial justifications for the IT system.
11. **External information-sharing system information.** Identify any other IT systems that either supply information to, or receive information from, the IT system under review. Obtain the same information for those systems as you are doing for this system.
12. **Business continuity plans.** Does your agency have any business continuity plans? If so, obtain copies of these plans.

Operational Information

The **Operational** category addresses security methods implemented and executed by people (as opposed to systems). Since people are usually the weakest link in the chain of security, this area is important to understand. Your employees and users of the IT systems must understand their jobs and how they both affect, and are responsible for, security. It is designed to answer questions about issues such as:

- *Personnel Security*: How personnel interacts with the organization's computerized systems and the access and authorities they need (and use) to do their jobs.
- *Physical Security*: How physical and environmental security measures have been taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment.

- *Production, Input/Output Controls*: There are many aspects to supporting general IT operations. This topic area discusses items such as whether or not you have a functioning user help desk, or your internal procedures for media handling, including their storage and destruction.
- *Contingency Planning*: Whether the agency has contingency plans for disasters and other disruptions. It involves more than planning for a move off site after a disaster destroys a facility, but also how to keep an organization's critical functions operating in the event of any disruptions, large or small.
- *Hardware and Systems Software Maintenance*: Whether and how the organization monitors the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained.
- *Data Integrity*: How data are protected from accidental or malicious alteration or destruction and how the user is assured that the information meets expectations about its quality and integrity.
- *Documentation*: Whether documentation of the hardware, software, policies, standards, procedures, and approvals related to the system are maintained and account for the system's security controls. Agencies should also make sure there are procedures for ensuring that the documentation is obtained and maintained.
- *Security Awareness, Training, and Education*: People are a crucial factor in ensuring the security of computer systems and their valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely.
- *Incident Response Capabilities*: Whether an agency has plans for responding to computer security incidents. Such incidents are becoming more common and their impact far-reaching.

Here are the types of organizational information you should collect to inform the operational self-assessment:

1. **Users.** Compile a list of authorized persons who use, maintain, or otherwise interact with the IT system under review.
   a. Obtain a copy of the personnel policies related to the job performance of these individuals.
   b. Obtain job descriptions for these individuals.
2. **Personnel policies.** Obtain a copy of the personnel policy for your organization and any other organization that provides support for the IT system under review.

3. **Administrator information.** Identify the people who are responsible for controlling and/or administering the IT system under review.
   a. Request, if they exist, memos, procedures, or guides that are used in the administration of the IT system.
   b. If these individuals reside in other agencies, you need to obtain copies of their job descriptions and a copy of that agency's personnel policies.
4. **Maintenance and support documents.** Identify the personnel (such as the system administrator or a specific subordinate of the system administrator) responsible for the maintenance/support of the IT system under review.
   a. Request, if they exist, any memos, procedures, or guides that are used in the maintenance/support of the IT system under review.
   b. If these persons reside in other agencies, then you need to obtain copies of their job descriptions and a copy of that agency's personnel policies.
5. **Physical security.** Identify the agency and/or people responsible for the physical security of any location where the IT system is either used or resides.
   a. Obtain copies of any policies, memos, procedures, or guidelines that determine how physical security is established and maintained.
   b. If the responsible agency is outside of your organization, then you need to obtain copies of its job descriptions for persons responsible for security and a copy of that agency's personnel policies.
6. **Building maintenance.** Identify the agency and/or people responsible for the building maintenance and support at any location where the IT system under review is either used or resides.
   a. Obtain copies of any policies, memos, procedures, or guidelines that determine how this support is established and maintained.
   b. If the responsible agency is outside of your organization, you need to obtain copies of the job descriptions of persons involved in supporting the physical plant and a copy of that agency's personnel policies.
7. **Disaster recovery plans.** Determine if any external agencies maintain disaster recovery plans relating to the physical plant where your users and/or IT system reside.
   a. If they exist, obtain copies of these plans.
   b. Do these plans provide for backup power, utilities, air conditioning, and so on?
8. **Data security.** Gather controls, policies, or procedures that have been developed that address data security.
9. **Contingency plans.** If available, collect contingency plans that have been developed, such as your response plan to a natural disaster or other incident.

10. **Data quality/integrity documents.** Determine if there are controls and/or audits that relate to data integrity.
11. **Training materials.** If your organization has a training section, it should be tasked with security awareness training. Collect the training charter and training material related to security.
12. **Incident response plans.** If your organization has an incident response team, it may have plans for a response to an IT security breach. Obtain a copy of the charter and procedures.

Technical Information

The **Technical** category examines security controls that the computer system executes. Systems themselves can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. Issues you will examine here include those pertaining to the following:

- *Identification and Authentication*: A measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. It requires that the system be able to identify and differentiate among users.
- *Logical Access Controls*: The system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.
- *Audit Trails*: This activity maintains a record of system activity by system or application processes, as well as user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems.

Here are the types of organizational information you should collect to inform the technical portion of the self-assessment:

1. **Identify the system—**
    a. System name.
    b. Describe what the system is used for (give detail, at least one-half to one full page).
    c. Date first installed.
    d. Current release or version number.
    e. Major system components (create a written technical overview of the system).
    f. Person or persons responsible for maintaining the system.
        i. This group should maintain a list of system changes, updates, modifications, and maintenance. Collect copies of this information.

g. Location of the installed system.

h. Record all system configuration parameters made during and subsequent to the system's installation. Identify, if possible, any justifications made for the selection of system configuration parameters. When computer systems are installed, certain configurations of the software are made at that time to enable the specific use of the system by the installing agency. System configurations could include who can access the system, what levels of security are required, and other system behavior. These parameters are configured to the individual agency workflow.

2. **Create a data flow diagram—**

   a. Identify input data, and its source and form. Input data are any data a user or another computer system provides as input to your system.

   b. Identify output data, where used, and in what form. Output data are information that is created by your system.

   c. Identify stored data within the system. Stored data are any data that your system stores for any length of time, i.e., historical data or databases. It is the long-term storage of input data.

      i. Where are the data stored?

      ii. Are the data backed up and, if so, where are the backups stored?

3. **Create a workflow diagram—**

   a. Identify all locations from which the system is accessed.

   b. Identify all individuals who access the system and how they relate to the data flow of the system.

4. **Authentication information.** If the system requires authorization for use, identify the people responsible for administration.

   a. Obtain, if they exist, copies of policies or procedures this group uses to administer access to the system.

   b. Does this group have review policies relating to the administration activities? If so, obtain copies of the policies.

5. **System owners.** Is any person or group considered to be the owner(s) of the system? If so, obtain a list of their expectations related to the operation of the system.

At this point, you will have collected a large amount of information relating to the IT systems you are preparing to examine. Coalesce and organize this information so you can locate the various pieces easily. All the work you have done will be of great benefit as you begin the self-assessment process.

Step 4

Conduct the Self-Assessment

Now that you have gathered all of your management, organizational, and technical information, you are ready to answer a series of questions designed to help you assess the current state of your IT security. This process mainly consists of ranking the level to which the agency has developed, implemented, and evaluated policies, procedures, and controls regarding the security of the subject systems.

A description and tour of the Assessment Tool begins on page 61.

Specific questions that focus on management, operational, and technical issues related to the systems under review are designed to illustrate how your agency is currently dealing with the issue. **You will find a comprehensive list of the key questions you will need to consider in *Appendix A: Assessment Worksheets and Questions from the SEARCH IT Security Self- and Risk-Assessment Tool,* which follows the NIST framework for this process.** These questions are provided in four main categories—Management, Operational, Technical, and State and Local Law Enforcement-Specific IT Security—that are further divided into the 18 subcategories listed on page 63.

A Look at How You Will Answer the Key Assessment Questions Using "Levels"

Before we begin, let us explain how the questions are posed in the Assessment Tool, and how your team will need to consider and answer those questions. We will use the first question in the Management category as our example (Figure 5).

Management

1. Risk Management

1.1 Is risk periodically assessed?

- Is the current system configuration documented, including links to other systems?

Figure 5: First Question in Management Category in the Assessment Tool

The Management category includes 61 questions that relate to the management of your systems (**you should also feel free to add your own questions to the suggested list**). These questions are divided into five distinct subcategories:

1. Risk Management.
2. Review of Security Controls.
3. Lifecycle.
4. Authorize Processing (Authentication and Certification).
5. System Security Plan.

Each subcategory contains the specific questions that your agency must answer to explore in detail how it is addressing the particular issue.

The policy development team reviews the questions, consults the management-related data gathered as described earlier in this chapter, conducts additional research, if necessary, and then answers the questions using the SEARCH IT Security Self- and Risk-Assessment Tool. Each question must be answered by addressing five specific levels with a simple "yes," "no," "partial," or "not applicable" (n/a) answer. Each of the five levels measures how mature the agency is in addressing a particular security issue—such as the existence of a documented policy. See Figure 6 for a detailed description of the five levels.

Levels	Meaning	Answers
LEVEL 1: Documented Policy	Does your agency have a formally documented and disseminated policy on that security control? Does the policy define 1) purpose and scope of the policy, 2) responsibilities required for its execution, and 3) compliance requirements and penalty specification?	Each level must be answered with **Yes**, **No**, **Partial**, or **N/A** (not applicable)
LEVEL 2: Documented Procedures	Does your agency have formal, complete, and well-documented procedures for the policies defined at level 1? Do the procedures: • List the control areas and clearly state the agency's position? • Document their applicability—clearly list when, where, how, to whom, and about what the procedure applies? • List the assignment of IT responsibilities and define explicit behavior? • Identify points of contact and where supplementary information can be found?	
LEVEL 3: Implemented Procedures and Controls	Have the procedures and controls been implemented? Are the following statements true? • Are the owners and users aware of the security policies and procedures? • Have the policies and procedures been formally adopted and the technical controls installed? • Is a security metrics program in place? (ongoing security compliance measurement) • Has management formally authorized the use of the system? • Have employee job descriptions been updated to include security responsibilities that the implemented controls require? • Have employees been trained on security procedures?	
LEVEL 4: Tested and Evaluated Procedures and Controls	Is a metrics program in place that routinely evaluates the adequacy and effectiveness of security policies, procedures, and controls? Are the following elements in place? • An effective program for evaluating the adequacy and effectiveness of security policies, procedures, and controls. • A mechanism for identifying vulnerabilities revealed by security incidents or security alerts. • A process for reporting significant security weaknesses and ensuring rapid and effective remedial action.	
LEVEL 5: Fully Integrated Procedures and Controls	Does your agency have a fully operational, comprehensive security program that is an integral part of your agency's culture? Are the following statements true? • There is an active agencywide security program that achieves cost-effective security. • IT security is an integrated practice within the asset (IT system). • Security vulnerabilities are understood and managed. • Threats are continually reevaluated, and controls are adapted to a changing security environment. • Additional and/or more cost-effective security alternatives are identified as the need arises. • Costs and benefits of security are measured as precisely as practicable. • Status metrics for the security program are established and met.	

Figure 6: Levels in SEARCH IT Security Self- and Risk-Assessment Tool

So, using the example question shown in Figure 5, and addressing the five levels shown in Figure 6, our answers could look as follows (Figure 7):

Management

1. Risk Management

1.1 Is risk periodically assessed?

- Is the current system configuration documented, including links to other systems?
  - — Level 1–Documented Policy: Yes

    (meaning there is a formal policy in place regarding keeping documentation of system configuration)
  - — Level 2–Documented Procedures: Yes

    (meaning there are procedures in place about how to enact the policy described in level 1).
  - — Level 3–Implemented Procedures and Controls: Yes

    (meaning that owners and other users are aware of management-adopted policies and procedures, and are trained on their implementation)
  - — Level 4–Tested and Evaluated Procedures and Controls: No

    (the agency has not implemented a means for testing or evaluating the policies, procedures, and implementation strategies)
  - — Level 5–Fully Integrated Procedures and Controls: No

    (the agency has not reached a level of a full, comprehensive security program related to this particular issue)

Figure 7: Answers to First Question in Management Category

The SEARCH IT Security Self- and Risk-Assessment Tool: Easy to Use, Visible Results

Download this Assessment Tool spreadsheet at **www.search.org** or see Appendix A for a hard copy version of the assessment questions and worksheets to record your responses.

The Assessment Tool was developed using Microsoft Excel. If you do not have this application, you can download a free Excel reader at **www.microsoft.com/downloads**.

To complete your self-assessment, you can use the questions we have adopted and revised from the NIST guidance under SP 800-26.[11] To make the process a little easier, SEARCH has built an **IT Security Self- and Risk-Assessment Tool**, based on the information described in this chapter, to aid you in this process.

The Assessment Tool is a Microsoft Excel spreadsheet containing worksheets that cover the three information categories and subcategories described in Step 3—**Management**, **Operational**, and **Technical**—*and* a fourth category, developed and added by SEARCH, **State and Local Law Enforcement-Specific IT Security Controls**, which assists with recording information on additional state and local government issues.

The Assessment Tool allows your policy development team to walk through the process and record their answers in one location. The Assessment Tool provides your team with a simple and concise methodology by which to assess your systems and their potential risk. It gives a graphical view of the systems assessed and their current status, based on the team's input. Because of the graphical nature of the Assessment Tool, it is immediately obvious where important issues need to be addressed. The answers can give managers a roadmap to their response to the risk and offer guidance on funding requirements for their systems.

[11] *Security Self-Assessment Guide for Information Technology Systems,* November 2001.

A Tour of the Assessment Tool

The first page of the Assessment Tool is the Table of Contents (Figure 8), an indexed listing of the spreadsheet contents. Each topical area is hyperlinked to the worksheet containing the questions to be completed. When you highlight the section and left click on it with your mouse, you will be taken immediately to that worksheet.

Figure 8: Table of Contents, SEARCH IT Security Self- and Risk-Assessment Tool

■ Introduction

The introduction page provides an overview of the Assessment Tool and its use. It also references the NIST documents that were used to build the Assessment Tool.

■ Gathering Preliminary Information

This section is a resource page containing much of the information already discussed in this chapter, describing the kinds of information that the team must have available before it starts this project.

■ System Questionnaire

This system questionnaire cover sheet is used to document or describe the system or systems that are the focus of the assessment, who is involved with the assessment, and the purpose of the assessment.

Categories

The Assessment Tool is broken down into four main categories—three of these are used as described by NIST, and we have added a fourth category for questions specific to state and local law enforcement.

As discussed on page 57, the four categories contain 18 subcategories of questions your policy development team should answer during the assessment. The four categories and their subcategories are listed in Figure 9.

Management

1. Risk Management
2. Review of Security Controls
3. Lifecycle
4. Authorize Processing (Certification and Accreditation)
5. System Security Plan

Operational

6. Personnel Security
7. Physical and Environment Protection
8. Production, Input/Output Controls
9. Contingency Planning
10. Hardware and System Software Maintenance
11. Data Integrity
12. Documentation
13. Security Awareness, Training, and Education
14. Incident Response Capability

Technical

15. Identification and Authentication
16. Logical Access Controls
17. Audit Trails

State and Local Law Enforcement-Specific IT Security

18. FBI CJIS Compliance

Figure 9: Assessment Tool Categories/Subcategories

When you click on the hyperlink to one of the subcategories, you are immediately taken to the worksheet containing the particular set of questions for that subcategory. The questions are listed down the left side of the worksheet. A group of "Effectiveness Ranking" fields runs across the top. SEARCH has tried to make answering these questions as simple as possible for policy development teams that are using the self- and risk-assessment processes laid out in this Tech Guide.

Figure 10 shows the worksheet for the "1. Risk Management" subcategory within the Management category.

Assessment Questions	References	Effectiveness Ranking				
		L1 Policy	L2 Procedures	L3 Implemented	L4 Measuring	L5 Feedback/ Reassessment
Risk Management						
1.1. Critical Element: **Is risk periodically assessed?**						
1.1.1 Is the current system configuration documented, including links to other systems?						
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change, and is management made aware of any new risks?						

Figure 10: Worksheet for Risk Management Subcategory

As shown in this worksheet, the five effectiveness ranking levels are listed across the top of the Assessment Tool. (See Figure 6 on page 59 for a detailed description of these levels.) In its documentation of this process, NIST asserts that the process should be followed from left to right: build your policy first, then your procedures, implement both, build your measurements, and then create a feedback loop.[12]

This linear process is ideal, but probably not realistic for most agencies. Many agencies have existing systems in which policies and procedures have been developed in *some* areas, and a certain amount of measures have been put in place to evaluate these. **But few agencies have successfully—or adequately—covered *all* levels, and this is where the Assessment Tool will really benefit your security planning.** Answering the questions in the Assessment Tool will immediately

[12] Note: The SEARCH IT Security Self- and Risk-Assessment Tool diverges from the NIST methodology by assuming few organizations have completed a full and detailed self-assessment and risk assessment of their IT systems—an exercise central to understanding what vulnerabilities exist and, therefore, what policies are needed. By beginning with a detailed analysis of an organization's IT environment, this Assessment Tool will then identify risks, gaps, and policy needs.

highlight those areas you have not yet addressed and give you a methodology with which to adequately address all of your security issues.

Going back to our original example question from the Risk Management subcategory, here's how the self-assessment immediately indicates those areas you need to address in your policy development and implementation. Let's say your answers to the question: "Is risk periodically assessed?" for each level are:

Level 1: "Yes," a policy exists.

Level 2: "Partially," we have *some* procedures in place for periodic risk assessment.

Level 3: "No," we have not implemented the policies and procedures.

Level 4: "No," we have not developed any process for measuring the implementation of our policies and procedures.

Level 5: "No," we have not built any feedback mechanisms into the process.

So how does the Assessment Tool make this easier for your team to answer the questions? As the team reviews the questions, they can use the <arrow> keys to highlight the specific field under the Effectiveness Ranking section and record an answer for that particular question and level. Highlighting the field displays a down arrow in that field, as shown in Figure 11. Clicking on the arrow displays a drop-down menu from which you can select an answer of "NO," YES," "PARTIAL," or "N/A."

Assessment Questions	References	Effectiveness Ranking				
		L1 Policy	L2 Procedures	L3 Implemented	L4 Measuring	L5 Feedback/ Reassessment
Risk Management						
1.1. Critical Element: **Is risk periodically assessed?**			▲▼ YES NO PARTIAL N/A			
1.1.1 Is the current system configuration documented, including links to other systems?						
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change, and is management made aware of any new risks?						

Figure 11: Using Drop-down Menus to Answer Questions in Worksheet

Selecting an answer for that field provides the team with a *visual* representation of the answer. Red for "NO," green for "YES," yellow for "PARTIAL," and no color for "N/A," as illustrated in Figure 12. This gives the team and any managers using the Assessment Tool an immediate understanding of the status of that question in relation to the system. It also can give a manager an overall sense of the system by visually depicting the green "YES" answers versus the red "NO" and yellow "PARTIAL" answers. (In Figure 12, the green is represented by light gray, the red by light purple, and the yellow by dark gray.)

Assessment Questions	References	Effectiveness Ranking				
		L1 Policy	L2 Procedures	L3 Implemented	L4 Measuring	L5 Feedback/ Reassessment
Risk Management						
1.1. Critical Element: **Is risk periodically assessed?**		YES	PARTIAL	NO	NO	NO
1.1.1 Is the current system configuration documented, including links to other systems?		NO	PARTIAL	NO	NO	NO
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change, and is management made aware of any new risks?		PARTIAL	PARTIAL	NO	NO	NO

Figure 12: Worksheet After Effectiveness Ranking Questions are Answered

The Assessment Tool's ease of use and its ability to aid the team by quickly documenting answers to the assessment questions makes using it a much easier process by which the team can complete the self- and risk-assessment processes.

Use the Assessment Tool!

Now it's time to complete all the questions in your self-assessment in the four categories of **Management**, **Operational**, **Technical**, and **State and Local Law Enforcement-Specific IT Security Controls**. Please use the assessment questions and response worksheets included in the Assessment Tool, located in Appendix A. Or, download the Microsoft Excel spreadsheet Assessment Tool from our web site at **www.search.org**.

Once you have completed the questions in the Assessment Tool, the next phase of the IT security policy development process requires you to identify and assess all the security *risks* you will uncover from this self-assessment process. Once you have identified these risks (see Chapter 4), developed controls to mitigate these risks (see Chapter 5), and developed and implemented measures that will assess the effectiveness of the controls (see Chapter 6), then you can begin actually *formalizing* your agency's security policies (see Chapter 7).

CHAPTER 4
PHASE II—
ASSESS SECURITY RISKS

"An assessment is one method agency officials can employ to help determine the current status of their information systems and agency-wide information security program. Ideally, assessments ... on an ongoing basis should be conducted to systematically identify programmatic weaknesses and where necessary, establish targets for continuing improvement."

—NIST Special Publication 800-26, *Guide for Information Security Program Assessments and System Reporting Form*

Chapter 4:
Phase II—Assess Security Risks

What Activities designed to identify, categorize, and prioritize the potential security risks to your IT systems.

Why Once you have assessed the risks, you can build risk mitigation strategies that ultimately form the basis of your security policies and procedures.

Who The Security Policy Development Team assesses risks and proposes mitigation strategies. When the risks have been identified, prioritized, and quantified, senior management decides which risks will be the subject of agency policies and procedures.

When The risk-assessment process begins *after* you complete the self-assessment process. You need to understand your information technology (IT) systems and how they are used before you can determine the risks inherent to the systems' operation.

Risk:
"An expectation of loss or threat that can be expressed as the probability that a particular threat (or set of threats) will exploit a particular vulnerability with particularly harmful results."
—*Applying Security Practices to Justice Information Sharing*, Global Justice Information Sharing Initiative Security Working Group

Assessing the risk to your agency's IT assets is critical to the successful development of your information security policy. Failure to do so can ultimately lead to a potential compromise of your system. When you complete the self-assessment process, you are likely to expose a number of potential risks of which you were probably unaware. The goal of the risk-assessment is to protect the operation of the organization, and both IT personnel and management are responsible for this.

Risk assessment contributes to an agency's effectiveness by:

1. Identifying potential problems and thereby developing plans to protect IT assets that store and process data.
2. Enabling well-informed decisions about how to address risks to the system.
3. Providing managers with specific system information to justify IT budget expenditures in the area of security.

Why Is the Risk-Assessment Process Important?

Risk assessment is: "The process of examining all risks, then ranking those risks by level of severity. Risk analysis involves: —determining what you need to protect, —what you need to protect it from, and —how to protect it."

—*Applying Security Practices to Justice Information Sharing*, Global Justice Information Sharing Initiative Security Working Group

No system can be *100 percent secure*—unless it is unplugged. Period. But that's not realistic in this world where information has a mission-critical role in law enforcement. Also, to be effective, information must be captured, shared, and exchanged with automated systems. So law enforcement agencies must calculate every potential risk to their information systems and then balance the risks they are willing to accept and those they must avoid.

The purpose of the risk assessment is to allow you to identify, classify, and prioritize the existing risks in your IT systems. Once this is done, and with input from management, you can determine how you are going to handle each specific risk. You will either choose to live with the risk or—through developing security policies and controls—reduce or mitigate these risks to an acceptable level for your agency (we'll discuss risk mitigation in Chapter 5).

By conducting a thoughtful analysis of the potential risks to an agency's information systems, executives and managers can build plans to address them. In addition, following a thorough investigation of potential exposures, managers can determine the costs of protecting the systems, both financially and in terms of human resources. Providing adequate security can be expensive. Given the limitations faced by most government agencies, there must be a fine balance in providing enough security but at an affordable level when addressing identified risks.

Let's not forget that assessing risk is a fairly common practice for law enforcement. Every day officers assess risks to themselves, other officers, and the public while responding to calls for service. Assessing risk in these situations is instinctive and automatic. When officers respond to an address, for example, they survey the scene as they approach, observing multiple avenues of approach and retreat. Officers evaluate what is occurring on the other side of a door by listening before knocking and, as the door opens, they make a visual assessment of what is happening inside before entering. Perhaps most important, the agency, based on previous assessments of similar risk, has adopted policies and procedures for handling particular situations. Officers are trained to act according to policy and standard procedures, so they know *exactly* what to do when presented with a certain set of circumstances.

Risk: The net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence.

—NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*

We are talking about applying the same level of assessment and scrutiny to vulnerabilities associated with your agency's information systems. The goal is for IT risk assessment to become a routine activity within your department, just like any other type of risk assessment.

Conduct a Risk Assessment

Conducting a risk-assessment exercise is a relatively simple task, particularly now that you have completed the self-assessment in Chapter 3. Based on that exercise, you now know what policies and procedures you currently have, and where you may be lacking specific security policies.

In the original *Law Enforcement Tech Guide*, risk management for IT projects and their implementation were explored. In that publication, risk management was defined as "a forward-thinking process that requires project leaders to envision challenges or threats to the project and develop contingencies for handling such events." This definition easily applies to IT security risk assessments.

Record the identified risk and other risk-decision responses using the SEARCH IT Security Self- and Risk-Assessment Tool spreadsheet at **www.search.org**, or use the assessment worksheets and questions provided in Appendix A.

In the original *Law Enforcement Tech Guide*, we introduced several key steps for creating a risk management plan. We've modified those a bit here and tailored them to the security risk-assessment process:

Step 1: Based on the self-assessment, identify and write a description of the risk.

Step 2: Categorize and quantify each identified risk.

Step 3: Determine your tolerance for levels of risk.

Step 4: Develop a risk-mitigation strategy. (This step is addressed in Chapter 5.)

Step 1

Identify the Risk and Write a Description of It

For each assessment question your team answered during the self-assessment, your team will assess its "Effectiveness Ranking" responses and write a description of the identified risk. For example:

Based on the agency's responses to this assessment question...

Is appropriate background screening for assigned positions completed prior to granting access?

This may be the description of the identified risk:

Individuals who have not undergone background screening may be able to access the information system.

Step 2

Categorize and Quantify the Identified Risks

Now it is time to put some rationale around each risk you've identified so that you can categorize them and, ultimately, prioritize the handling of them. Borrowing from our original *Law Enforcement Tech Guide*, categorizing risks consists of analyzing the *likelihood* that the risk will actually occur; how *severe* the risk is, ultimately; and what type of *impact* its occurrence would have on the organization, as well as on people both inside and outside of the agency.

Determine the Likelihood of the Risk

In dealing with likelihood, take each identified risk and rate the possibility that it will occur:

- **Remote**: The risk probably will not occur because the risk would be difficult to realize, or there are solid means in place to limit the risk appropriately.
- **Possible**: The risk has a chance of occurring, but it may be difficult or there are controls in place to help avoid the risk.
- **Likely**: The risk, due to conditions and capabilities, is likely to occur.

In assessing likelihood, ask the following questions about each risk:

1. Who or what would cause the risk to occur (e.g., a former employee)?
2. Is there a motivating factor in operation to cause someone or something to expose the risk (e.g., the employee was recently fired and is disgruntled)?
3. Does your existing environment have any mechanisms at this point that would lessen the risk (e.g., immediately upon an employee's separation for any reason, the organization removes all of the employee's identifiers, passwords, etc., from the system)?

Answering these questions for each risk will allow you to properly determine whether there is a possibility of the risk occurring—from remote to highly likely.

Determine the Severity of the Risk

Next, it's time for the team to make judgments about the consequences of a particular risk by ranking its severity as high, medium, or low. You have enough information to make an overall judgment about each particular risk, but it still is a clearly subjective exercise. As you analyze all data you've collected about the risk so far, give it one of the following overall rankings:

- **Low**: The risk is manageable through planning and action and the impacts generally are minimal.
- **Medium**: The risk will be mitigated through planning and action, although if it

occurs, it will still have some impact on some more important areas of concern.

- **High**: The risk will have serious impact and, without extensive planning and action, its consequences will be severe.

Identify the Area of Impact of the Risk

This risk category is *not* captured in the Assessment Tool, but is information that will be valuable to your team's decision-making process. Here, you and your team need to contemplate all of the ways damage can be caused if a risk is realized. Some risks can cause damage in multiple areas both within and outside of your organization. We suggest organizing the areas of potential impact into several categories, such as these:

Human

- Loss of life or injury
- Jeopardy to reputations

Liability

- To the organization and/or parent agency such as city, county, state
- To individuals

Operations

- Impede or disable ability to conduct business
- Impede or disable decision-making

Financial

- Lost revenue
- Cost to correct damage

System data and information

- Data integrity
- Availability of the system and/or data
- Confidentiality of data and/or information

Public

- Loss of confidence
- Jeopardy to citizen safety

You may choose to add other categories of impact, such as political or managerial. For each risk, you should articulate the impact in detail.

Figure 13 shows how we took one of the self-assessment questions and illustrates how we would analyze it as a risk.

Assessment Question	Description of Identified Risk	Likelihood	Severity	Impact
Is appropriate background screening for assigned positions completed prior to granting access?	Individuals who have not undergone background screening may obtain access to the information system.	Possible	Medium	• Liability • Systems data and integrity • Financial

Figure 13: Illustration of "Risk Decision" Responses to an Assessment Question

Step 3

Determine Your Tolerance for Levels of Risk

Use the Assessment Tool to capture risk-tolerance decisions for each identified risk.

Having categorized and quantified the identified risk, the policy team should next develop recommendations on the specific tolerance level for that risk and present them to the management team. Tolerance decisions are based on facts, research, and other information compiled by the team, but executive sponsors make the final tolerance determination for each risk. The tolerance decision begins to drive your strategy toward mitigating each risk.

There are the four levels of risk tolerance: avoid, assume, mitigate, or transfer. You should assign one "Tolerance Level" to each identified risk. Figure 14 provides a detailed definition of each tolerance level, and provides two scenarios of how two sample agencies would choose to avoid, assume, mitigate, or transfer risk.

Tolerance Level	Definition	Example 1	Example 2
Avoid	Avoidance is often used for risks that have the capacity for negative impact, but have little known recourse. In security projects, a decision to avoid a risk often means a decision not to let your agency put itself in the situation where it could incur the risk. Therefore, your decision would also be to avoid the cause of the risk. This is an extreme decision, but one where the benefit of automated systems to the agency would be negated entirely compared to the risks the technology would expose the agency to. Generally the decision here is that the system or component of a system would be shut down or eliminated to completely avoid the risk.	*A police department's records management system (RMS) did not use encryption and the RMS data were stored in plain text on the server. Anyone who could gain physical access to the server could potentially get to confidential data.* To avoid this risk completely, the department may consider replacing or upgrading the RMS altogether with encryption-based software.	*An agency is interested in implementing new intrusion detection software that requires an upgrade of new routers within the system. However, the purchase of the new routers is not within the current budget. Without the upgraded routers, the software will not function properly. The software has a known attack if the existing routers are used.* The agency can avoid the risk by simply not implementing the new software and seeking other solutions compatible with its current routers.
Assume	In this case, the decision to assume a risk means accepting the risk as-is, and not implementing any policies or procedures to lessen it. This is often the decision in cases where the risk is so minimal and of limited impact should it occur that the cost of implementing a mechanism to minimize or reduce it would be far greater than the agency's concern.	The department could decide to merely assume the risk and not do anything about it. Given the potential for major impact on the system and the department, as well as the liability involved, this certainly would not be a recommended decision.	The agency implements a newer operating system for a portion of its network. The new operating system allows for more than eight-character passwords. However, several parts of the network still have an operating system that allows only six-character passwords. The agency chooses to allow the use of six-character passwords as its standard because the cost to upgrade all systems would be prohibitive.
Mitigate	This is the most common decision to make for identified risks: to implement policies, procedures, and other security controls to limit the risk to an acceptable level.	The decision to mitigate would be made based on the critical role the RMS plays in the department and the conduct of business. If the department decides to mitigate risk, then it needs to balance the need for this RMS with the risk and determine strategies for mitigation, such as physically locking the server in a separate room, adding a lock to the server enclosure, limiting the number of individuals who are authorized to access the server, or moving the server to a secure location within the agency.	The agency has a six-character password for users to enter a database containing gang intelligence files. The current software in use does not allow for a more secure password to these sensitive and attack-prone files. Management recognizes that this is insufficient to protect the data contained on the system and limits the risk by isolating the systems in use to an office occupied only by the gang investigators and who are the only ones who have a key to that office.
Transfer	Pass the buck! Seriously, though, one option is to transfer the responsibility for a system or the risk itself to another party that can better accept and deal with the risk and/or has the resources necessary to properly mitigate the risk.	The department could potentially transfer the risk by outsourcing the server and its security to the city or county IT department, if that agency had appropriate controls to manage the risk.	The agency outsources data storage for its system to another agency in a multiagency project. The risks associated with maintaining the information is transferred to the agency that actually maintains the data.

Figure 14: Risk Tolerance Levels—Definitions and Examples

Make Your Risk Assessment Easier by Using the SEARCH Assessment Tool

The Assessment Tool was developed using Microsoft Excel. If you do not have this application, you can download a free Excel reader at **www.microsoft.com/downloads**.

To complete your risk assessment, use the SEARCH IT Security Self- and Risk-Assessment Tool. Visit **www.search.org** to download this Microsoft Excel spreadsheet tool, or use the worksheets provided in Appendix A.

In Chapter 3, we described how your team answers each assessment question in the Assessment Tool by filling in responses in the "Effectiveness Ranking" section of each worksheet. In this way, your team recorded the current status of your system by recording the level of documented, implemented, tested, and integrated policies, procedures, and controls in your agency.

Now, for each assessment question, you will record responses in the "Risk Decisions" section. Using the Assessment Tool during your risk assessment will help your team to walk through the process and record answers in one location, providing a simple and concise methodology by which to assess risk. It also provides decision-makers with a graphical view of your systems and risk assessments.

When you begin to use the worksheet, which is located on page 123 (in Appendix A) or the Microsoft Excel spreadsheet Assessment Tool at **www.search.org**, you will notice a header titled "Risk Decisions." As in the self-assessment, the team reviews each question. Using this chapter as a guide, assess your risk decisions about each question in the Assessment Tool and document your risk.

First, write a statement that describes the identified risk. Then you will be able to record issues such as the likelihood of occurrence, the potential severity of a realized risk, the tolerance level you choose to accept for that risk, and a numeric priority for action on that risk.

So how does the Assessment Tool make this easier for your team to answer the questions? As your team reviews the questions, use the <arrow> keys to highlight the specific field under the Risk Decisions section and record an answer for that particular question (Figure 15).

Risk Decisions				
Description of Identified Risk	Likelihood	Severity	Risk Tolerance	Action Priority

Figure 15: Risk Decisions Questions in the Assessment Tool

The "Description of Identified Risk" is a free-form text field that allows your team to record the risk statement. (This process will build off of the "Effectiveness Ranking" questions your team already answered in Phase I.) When highlighted, the four other fields in the Risk Decisions section display a down arrow. Clicking on the arrow displays a drop-down menu that has different answers, depending on the field. There are four fields: "Likelihood," "Severity," "Risk Tolerance," and "Action Priority." The drop-down answer options for each column are:

Check out the following pages of this IT Security Tech Guide for descriptions of:
—Likelihood (page 74)
—Severity (page 74)
—Tolerance (page 76)

- **Likelihood**
  - Remote
  - Possible
  - Likely
- **Severity**
  - High
  - Medium
  - Low
- **Tolerance**
  - Avoid
  - Mitigate
  - Assume
  - Transfer
- **Action Priority** (1 being highest priority, and 3 the lowest priority)
  - 1
  - 2
  - 3

To facilitate a quick visual evaluation, each of these answers also has a corresponding color that appears in the block along with the answer (Figure 16). This again allows the team to quickly view its responses to its risk assessment and provides managers with a quick visual overview of the entire process. Here's a completed example of the analysis of an identified risk:

Risk Decisions				
Description of Identified Risk	**Likelihood**	**Severity**	**Risk Tolerance**	**Action Priority**
Not conducting thorough background checks	LIKELY	HIGH	MITIGATE	1

Figure 16: Example Risk Decisions Responses in the Assessment Tool

What's Next?

So far you have conducted a self-assessment (Chapter 3) of your systems and determined your security risks (Chapter 4). The next phase of the IT security policy development process requires you to develop your risk mitigation strategy, which includes developing security controls for each risk that your team has determined needs to be mitigated. So, keep up the good work and let's move on to Chapter 5!

CHAPTER 5
PHASE III—
DEVELOP A RISK-MITIGATION STRATEGY

"It must be recognized that justice information technology systems are a vital part of the nation's critical infrastructure, and as such, information technology infrastructure requires comprehensive security architecture. Protecting this critical resource is not just a matter of operational good sense; it is increasingly a matter of national security and public safety."

—*Applying Security Practices to Justice Information Sharing*
Global Justice Information Sharing Initiative Security Working Group

Chapter 5: Phase III—Develop a Risk-Mitigation Strategy

What Once you know your information technology (IT) system's exposure to risk, you must establish controls and procedures to safeguard your information system.

Why Establishing the risk-mitigation strategy is the heart of protecting your IT assets from compromise. It fulfills the management directive regarding risk tolerance.

Who The Security Policy Development Team designs the strategy. A variety of individuals will be responsible for helping to design and implement security controls and document their effectiveness.

When This process occurs after you complete the self- and risk-assessment processes and have made risk-tolerance decisions.

With your self-assessment results in hand, and after you have categorized and quantified all risks and made decisions about your agency's tolerance for each identified risk, you are ready to create a strategy to mitigate those risks.

Process to Identify and Develop Controls
—Prioritize risks
—Build security controls
—Document the controls
—Select which controls to implement; assign responsibility for these
—Develop an implementation plan

Remember, the goal here is to implement risk-mitigation strategies that will reduce the likelihood of system harm should it be exposed to the security vulnerabilities your team has identified. Here are a few points to keep in mind as you develop mitigation strategies:

- If there is a high probability that the risks will occur, *multiple layers* of security controls may be the most effective method to mitigate this exposure.
- When addressing the issue of hacking or other criminal attack, if the cost of attacking the system is relatively minimal compared to the potential gain for the attacker, you should develop controls that will dramatically increase the cost of an attack. A basic security axiom states: ***Your fence should be a foot higher than your neighbors.*** This discourages attackers from tampering with your system.

- If the potential for loss to the agency is extremely large—monetary, political, or otherwise—your agency needs to consider some more rigorous approaches to risk mitigation. Among them are:
  - Redesigning the entire system (this could be a lengthy and costly process).
  - Shutting the system down.
  - Adding both technical and nontechnical protections that would limit the extent of the attack (properly implemented, these protections may provide the best solution).

Mitigating your risks primarily comprises developing **controls**—specific measures you implement that are designed to lessen or negate the impact of a risk that actually occurs. This chapter outlines a process that will help your team identify and develop these controls.

Prioritize Your Agency's Risks

Before developing security controls, your first task is to rank, in order of concern, the risks identified during the risk-assessment exercise. Once you have categorized, quantified, and established a tolerance level for all these identified risks, it should become readily apparent which risks rise to the top of the list. Management can now use this list to determine its IT security priorities.

What Are Security Controls?

Security controls are the methods you put into place to lessen the impact or negate the effect, if any, of an identified risk.

Developing security controls is the heart of your mitigation strategy and we'll spend a great deal of the rest of this chapter focused on showing how you can properly develop these controls.

Security controls are processes your agency puts into place to adequately protect your information system. They seek to control the likelihood of each risk occurring. You will establish numerous controls—there can be one or more controls implemented for each risk exposure you are trying to mitigate. The controls are developed based on your completion of the two previous phases: Phase I, self-assessment, and Phase II, risk assessment. You will not be able to properly develop security controls if you have not properly assessed your system and determined your system's risk.

This chapter addresses the development of security controls that are required to mitigate the identified security risks of your IT system. Once the controls are implemented, you also need a way to verify that the controls are performing as designed—in other words, that they are effectively mitigating the specific identified risks. These activities are discussed in Chapter 6, which focuses on how to develop and implement a security measurement process.

Security Controls Defined

According to the National Institute of Standards and Technology (NIST), "Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information."[13]

In other words, a control is a mechanism you put in place to mitigate a risk you identify. It can range from:

- A change in management strategy (such as how the agency deals with securing systems in general)
- To using software applications within the system that automatically implement particular controls (such as enforcing a password)
- To changing mandates on personnel (such as requiring each system user to include a biometric when logging onto the system, or instituting a policy requiring passwords to be changed once a month).

Because we conducted the self-assessment and risk assessment across the three critical areas of management, operations, and technology, you should develop security controls that focus on those same issues.

Management controls affect how IT systems are *managed*. An example of such a control might be the development of a physical security plan for IT assets.

Operational controls address security methods implemented and executed by *people* (as opposed to systems), such as using an enhanced password methodology.

Technical controls address security mechanisms that a *computer system* executes, such as using encryption to control access to sensitive data.

[13] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.

There are literally thousands of possible controls that can be applied to IT systems security depending on the risks identified, so listing all of them here does not make sense. Instead, we refer you to NIST literature that addresses this subject at **http://csrc.nist.gov/publications/nistpubs**. That web site provides many documents containing examples of controls.

Another document that provides many excellent examples of controls used in managing and operating information sharing systems is *Applying Security Practices to Justice Information Sharing.* This resource document, prepared by the Global Justice Information Sharing Initiative Security Working Group, is designed to educate justice executives and managers in good, basic, foundational security practices that they can deploy within their enterprise and between multiple enterprises. This document and its companion CD contain background information, overviews of best practices, and guidelines for secure information sharing. The document (in PDF) and CD (a browser-style, graphical overview of the document) are available at **http://it.ojp.gov/global**.

Meanwhile, let's take a look at *how* you should develop controls. NIST proposes a structure for security controls that includes these three components:

1. *Control*

   A control is the mechanism that is adopted to mitigate a risk.

2. *Supplemental guidance*

   Supplemental guidance provides further detail on how the control will be implemented or any exception to its implementation.

3. *Control enhancements*

   Control enhancements provide the detail and results of implementing the control.

Let's look at an example of this structure taken from NIST Special Publication 800-53 regarding how to deal with "*Unsuccessful Login attempts.*"

UNSUCCESSFUL LOGIN ATTEMPTS

Control: The information system enforces a limit of [*organization-defined number*] consecutive invalid access attempts by a user during a [*organization-defined time period*] time period. The information system automatically [*locks the account/node*] for an [*organization-defined time period*], and delays the next login prompt according to [*organization-defined delay algorithm*], when the maximum number of unsuccessful attempts is exceeded.

Supplemental guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.

Control enhancements: The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

Let's also look at an example of how controls are established to mitigate a risk, as illustrated in the Global document *Applying Security Practices to Justice Information Sharing.*

In this example, a common risk of "*Identification of Unauthorized Hardware Attached to a System"* is used. This example shows that a risk occurs when agency personnel attach unauthorized hardware to an existing system, an action that may compromise the system's integrity. In this case, the agency has articulated its policy directives, followed by the controls it established to mitigate the risk.

Identification of Unauthorized Hardware Attached to a System
Establish policies to limit employees from attaching unauthorized hardware to the office system. Unauthorized hardware includes computers, modems, terminals, printers, and disk or tape drives. The policies should also restrict software that employees may load onto the office system. Implement policies regarding opening unidentified e-mail attachments and downloads off the Internet.

- Perform monthly audits of all systems and peripherals attached to the network infrastructure.
- Make random inspections of equipment to search for unauthorized hardware attached to the network.
- Identify missing or misplaced hardware.
- Search and identify any unauthorized hardware attached to the network.
- Inspect computers and networks for signs of unauthorized access.
- Search for intrusion or tampering with CD-ROMs, tapes, disks, paper, and system components that are subject to physical compromise by damage, theft, or corruption.

No set of security controls will ever completely eliminate risk from your agency.

Build Your Agency's Controls in Six Steps

How do you build your security controls? We created a six-step process to make building security controls easier (Figure 17). A worksheet for building each control, as described in this chapter, is provided in Appendix B. The worksheet is titled **SEARCH IT Security Control Development Worksheet**. We suggest that you make numerous copies of this worksheet and get ready to build your controls!

BUILDING A CONTROL		
	STEP	**ACTION**
1	Identified risk	Start with an identified risk that must be mitigated
2	Existing controls	List controls, either full or partial, that currently exist for the risk
3	All other possible controls	List all possible controls that could be used to mitigate the risk
4	Control implications	Analyze the implications associated with each control
5	Control recommendation	Make a recommendation to management regarding a control to adopt
6	Management control decision	Management makes a decision as to which controls to implement

Figure 17: The Six Steps to Building a Control

Step 1

Start with an identified risk that must be mitigated

As discussed earlier, conducting a risk assessment of your system results in identified areas of risk. In developing appropriate controls, you must start with an identified area of risk. As an example, let's use an actual question from the SEARCH IT Security Self- and Risk-Assessment Tool that illustrates a risk: Question 6.2, Section 6, **Personnel Security**, of the Assessment Tool.

> "*Is appropriate background screening for assigned positions completed prior to granting access?*"

Let's assume an agency used the Assessment Tool to answer the questions, as shown in Figure 18.

Assessment Questions	References	Effectiveness Ranking				
		L1 Policy	L2 Procedures	L3 Implemented	L4 Measuring	L5 Feedback/ Reassessment
Personnel Security						
6.2. Critical Element: Is appropriate background screening for assigned positions completed prior to granting access?		NO	PARTIAL	PARTIAL	NO	NO

Figure 18: Example Effectiveness Ranking Responses in the Assessment Tool

The answers given by the agency's security team using the Assessment Tool indicates that the agency:

- Has no written policy (Level 1)
- Has *partially defined* procedures for conducting background screening of the assigned positions (Level 2)
- Has *partially implemented* those procedures (Level 3)
- Has not yet determined methods for measuring the effectiveness of such a control (Level 4)
- Has no continuous feedback method to determine compliance with the policy, procedure, or implemented control (Level 5).

After analyzing the responses in the Effectiveness Ranking section, the agency records its risk decisions, as shown in Figure 19. It determines that "Not conducting thorough background checks" is the identified risk; that it is *likely* this risk will occur; the severity of this risk is *high*; and the agency chooses to *mitigate* the risk as a *#1* top priority. Now the agency will build controls to mitigate this risk.

Risk Decisions				
Description of Identified Risk	**Likelihood**	**Severity**	**Risk Tolerance**	**Action Priority**
Not conducting thorough background checks	LIKELY	HIGH	MITIGATE	1

Figure 19: Example Risk Decisions Responses in the Assessment Tool

Enter the identified risk in Step 1 of the Security Control Development Worksheet, as shown below.

Step 1: Identified risk	Personnel who have not undergone thorough background checks have access to information systems.

Reminder: See Appendix B for the entire SEARCH IT Security Control Development Worksheet. Photocopy and use this worksheet to build your controls.

Step 2

List controls, either full or partial, that currently exist for the risk

You may already have some formal or informal procedures in place to address the risk identified in Step 1 and for which this control is being built. Refer to the analysis you did during your self-assessment and the effectiveness rankings you identified during that part of the process to help you define the existing controls.

Enter the existing controls for this risk in Step 2 of the Worksheet.

Step 2: Existing controls	New employees who will have access to the agency's IT systems receive a criminal background check.

Step 3

List all possible controls that could be used to mitigate the risk

Here your team should brainstorm all possible controls that would be available to your organization to mitigate the risk. These should include all possibilities—regardless of their cost or effect on the system. Developing as complete a list of controls as possible will give your team several options for selecting the most appropriate control.

Enter a list of all possible controls in Step 3 of the Worksheet.

Step 3: All other possible controls	• Conduct background checks of all agency employees who may not be authorized to use the system, but who still could get access to the system. • Enhance background screening by adding a reference check for each new employee. • Establish a "rapback" process so that any new activity on an employee's criminal record is made available to the agency.

Step 4

Analyze the implications associated with each control

Every identified control has certain implications for the agency. Many controls may provide a solution to mitigate an identified risk—but which particular one will best meet your user's needs and protect the data to the level you require? Each control must be realistic in its concept and within the ability of the organization to implement. Will a simpler control be as effective? Each agency must decide which control fits its individual needs through some analysis.

Such analysis can include looking at the financial impact of a particular control, the required staff expertise to implement and manage it, and any needed changes (such as revisions to organizational policy or training requirements). Costs may include the cost of the control itself, installation, maintenance, and updates.

Budget considerations

A major consideration regarding a control is the fiscal implications of developing, implementing, and monitoring it. An option to consider is to conduct a cost-to-benefit analysis.

For example, if an agency wishes to purchase a firewall to help protect a system, the cost to implement this control could include:

a) The purchase price of the firewall.
b) The installation of the firewall (even if it is done by agency personnel).
c) Regular firewall maintenance.
d) Review of firewall logs for irregularities.
e) Checking for and updating firewall firmware.

Implementation

For each control you identify, you also need to analyze whether your current staff are capable of implementing the controls. Do they have the technical knowledge, the resources, the training, and the funding to exercise a particular control? Do you have the technical expertise in the agency or will you have to hire outside experts? Perhaps you will need additional training for the personnel responsible for the control. Everyday users may also have to be trained if they are required to implement or be involved in any part of a control.

Depending on your analysis, you may need to train staff prior to control implementation or bring an outside consultant in to assist your agency and staff. Each of these decisions will surely have budget implications.

After analyzing the implications for the identified control(s), enter a list of these implications in Step 4 of the Worksheet.

Step 4: Control implications	• Overtime cost of assigning personnel additional duties • Loss of patrol/detective personnel due to reassignment to background investigations • Forty hours of training required per assigned officer

Step 5

Make a recommendation to management regarding a control to adopt

Review all of the controls your team has assembled and prepare a recommendation to the executive management about the best control to adopt. Determining which control is best, as discussed in the steps leading up to your decision, is based on an evaluation of the risk, the possible controls you can implement to mitigate the risk, anything you can add to enhance that control, the costs to implement the control, and the expertise required to implement and maintain that control.

This is the tough part of the process. The team's expertise and detailed knowledge of the system and your available resources is a key asset at this point. Executive managers will be expecting the team to deliver an informed recommendation for controlling the agency's risk.

Enter the policy development team's control recommendation in Step 5 of the Worksheet.

Step 5: Control recommendation	• Use internal resources to conduct thorough background checks

Step 6

Management decides which controls to implement

Management must decide which control(s) to implement to mitigate the risk identified in Step 1 of the Worksheet. Management may have a variety of controls from which to select—any of which might suffice. In this example, the agency chooses a solution that is financially acceptable and offers a solid mechanism for eliminating risk.

Record management's control decision in Step 6 of the Worksheet.

Step 6: Management control decision	*Conduct background investigations internally using our own employees. Training will be provided by a neighboring agency that conducts its own investigations. Access to a public information database will be purchased and a policy will be written to ensure that proper background investigations are conducted.*

Document the Controls

As your team develops the controls, it is critical that the controls are effectively documented in some detail. It is during this phase that your security policy is beginning to emerge. Ultimately, the controls you settle on during this phase of the process will require effective policy statements to guide their successful implementation. Even though we save the discussion about writing the agency's formal security policy until Chapter 7, you will find that it is at this stage that writing the policy and completing the rest of the tasks set forth in this guide are often done simultaneously. See Chapter 7 for details on how to formalize your information security policy.

Select Which Controls to Implement and Assign Responsibility

By now you should have most—if not all—of the information necessary to select the most effective security controls to address each identified risk. Now the management team needs to select what security controls to implement.

Next, identify the appropriate person(s), both within and outside of your agency, who will implement, manage, and be responsible for each security control.

Develop an Implementation Plan

"The Implementation Plan is the blueprint for *completing* the project."

A solid strategy for implementation is key to ensuring the controls are properly developed, applied, and maintained. Here your team should develop a plan that specifically articulates decisions made, individual and group responsibilities, and "how" each control is implemented.

In the original *Law Enforcement Tech Guide*, a process for developing a project implementation plan is described in Chapter 16. Although that chapter focuses on project implementation plans, many of its principles apply directly to security implementation plans, so we encourage you to read it.

Your implementation plan should contain much of the information you have gathered through the self-assessment and risk-assessment exercises. It should contain a list of the controls management has decided to implement and should indicate who is responsible for each control. This plan should also contain detailed *schedules* for implementing the control, monitoring the control, and revisiting the control to determine its effectiveness and viability.

Congratulations! You have now implemented security controls that will go a long way to reduce security risks and exposure to your agency. Keep in mind that the implementation of these controls does not end the process. A critical next step is the evaluation and measurement of those controls to ensure that they continue to effectively protect your organization.

At this point you have conducted a self-assessment (Chapter 3) of your systems, determined your security risks (Chapter 4), and developed controls in this chapter to mitigate that risk. The next phase of the IT security policy development process requires you to measure your security controls. This next phase in the process is discussed fully in Chapter 6.

CHAPTER 6
PHASE IV—
MEASURE YOUR SECURITY CONTROLS

"The success of an information security program implementation should be judged by the degree to which meaningful results are produced."

—NIST Special Publication 800-55,
Security Metrics Guide for Information Technology Systems

Chapter 6: Phase IV—Measure Your Security Controls

What Creating and implementing a program that allows you to continuously measure, monitor, and provide feedback on your security program.

Why To find out if you have created an effective security program, and modify the program if it's found to be deficient.

Who The Security Policy Development Team designs the measures. A variety of individuals will be responsible for helping measure the controls and document the results.

When This process often occurs in parallel with determining the security controls you'll put in place (the outcome of the risk-assessment exercise). When deciding on the control, you need to ask how you will measure its performance and cost-effectiveness.

Note: Strong measures to determine the effectiveness of your controls are key. However, you should NOT limit your policies based on your current ability to measure them.

Sometimes the approaches you take to mitigate a risk just don't work. Sometimes they work for a while, but as technology and other processes change, they lose their effectiveness over time. We already know how mission-critical it is to keep the law enforcement agency's information technology (IT) systems secure. Today, we are also obligated to consistently assess how *well* the security program we put in place is working: That is the mission of the security-measurement program.

The key goal here is to develop measurements (sometimes referred to as metrics) that show, in quantifiable terms, the agency's effective implementation and maintenance of the security controls you developed. Each control should be easily measured and produce repeatable results that can be tracked to identify conformance to your policy. You gain maximum benefit with controls that are designed to be measured regularly and, thereby, can show trends over time. Your measures provide hard evidence that the operation of your IT system and your control implementation conforms to the risk mitigation you intended for your agency. As such, measuring is not a one-time activity!

The purpose of this program is to put in place a *permanent methodology* that will monitor, on a continuous basis, security controls and provide feedback to determine if corrective action is required. **An effective measurement program is one that is**

integrated into the daily operation of the system. A comprehensive program of measurement often incorporates multiple tracking mechanisms that document and quantify the performance of all adopted measures.[14]

What Are Security Measures?

Security measures are tools you put into place to help facilitate your decision-making. They can improve your system's performance and its accountability by collecting and analyzing data, and providing a report of performance. Measures allow your security team to monitor specific controls and take corrective action, if necessary.

Measuring can be complex, but its design is to simplify and organize an agency's approach to achieving the best security program for IT systems as possible. The fundamental product of measuring and testing is to ensure that you collect valid information about the performance of your system. It also is an iterative process that helps to analyze the security data and determine what changes need to be made to the system to ensure its security.

If **risk avoidance** or **transference** is used or considered for a particular risk, that risk may not immediately need a process in place to measure it because your team consciously decided to avoid or transfer your risk. Therefore, the controls that do require ongoing measurement will naturally rise to the top of your list of concerns.

Develop and Select Measurement Methods

The measurement development process deals with creating and implementing metrics. **This is a critical part of the overall policy development process because it provides the necessary feedback to control and ultimately improve the security of your system.** In addition, each of these steps is designed to feed back into the entire process that we have described so far in this Tech Guide. Your measurement program, therefore, should be able to continually self-correct and guide improvements to the security of the system.

After your security policy team conducted your agency's risk-assessment, it prioritized the risks from the greatest to the least (as described in Chapter 4). This was done so the team could focus on the most critical risks first. Your policy team then decided which specific risks your agency intended to mitigate through the development of security controls (as described in Chapter 5).

[14] For more information on performance measurement, see *Law Enforcement Tech Guide for Creating Performance Measures that Work: A Guide for Executives and Managers* funded by the COPS Office (publication pending).

A Measurement Example:
Measuring Password Strength within an Agency

Let's assume that agency X has performed the self-assessment, risk assessment, and risk mitigation processes described so far in this Guide and have used the SEARCH IT Security Self- and Risk-Assessment Tool. During those exercises, the agency analyzed all of the pertinent information regarding its password usage. For example, Question 15.1.6, located in Section 15, Identification and Authentication, of the Assessment Tool, asks the following:

> *"Are passwords unique and difficult to guess (e.g., do passwords require alphanumeric, upper/lower case, and special characters)?"*

The agency identified a risk to its system because it had no policy regarding password usage. Using the control development process, the team selected the following control, which agency management approved as the proper control for password usage on its system:

> ***All passwords must be at least eight characters long and contain at least one digit and at least one character. In addition, no English words of four characters or less may be used.***

The agency then took the following actions to establish a control and a way to measure this control in the agency:

First, after advising users of the new control to regulate passwords and the need for it, all passwords were reset so that at the next login the user had to enter a new password.

Second, the agency implemented procedures, educated users, and conducted testing to confirm that 100 percent of passwords met or exceeded the established standard. The testing gave the security policy team specific data on the use of the control. In this instance, the control was a success.

But there are other factors outside the control that may negate its effectiveness over time. In this same situation, the other data that play into measuring the effectiveness of the control is an environmental scan. Agency X did some research on eight-character passwords and found that, due to increases in computer power and better cracking programs, eight-character passwords can be broken in 10 seconds or less. This could lead to a refinement of the initial policy whereby passwords must now contain at least one special character in addition to the other existing requirements.

The passwords are tested, measured, and evaluated on a regular basis and any deviations from the standards or new technological impacts are addressed in a timely fashion.

Three Methods to Measure Security Controls

There are three methods to measure the security controls in place in your system. Each of these methods can be used by any agency, depending on its needs and ability. Method 1 is a simple method of monitoring a security control and developing feedback on its success. That may be all an agency needs if the identified risk that the control was intended to mitigate is small. However, implementation of Methods 2 or 3 may be warranted, depending on the complexity of the control being measured.

■ Method 1. Monitor the Level of Implementation and Develop Feedback

This is perhaps the easiest and the most commonly used method to measure your security controls on a single system or application. Your team starts with an identified risk your agency chose to mitigate. Your team then extracts relevant data related to that risk from the system. Your agency reviews and processes these data to determine whether the security control has mitigated that risk in the manner the agency intended. This information can then be used as feedback into the policy development process to ensure compliance and that expectations are met. If they are not, this tells the agency that an improved control is needed.

Monitor and Feedback example:
One of your security controls may be that a confidential system containing criminal history information requires the reauthentication of the current user every 5 minutes. You develop a method to measure this control by implementing a program that extracts logs of personnel usage information and creates a report of how long your users were active before being challenged by an authentication request. If you determine that one or more sessions violate your standards, then the process is reviewed for changes that can be made so the original control is met.

■ Method 2. Analyze Multiple System Results

This method looks at the measurement results developed for multiple individual systems or applications using the same process used in Method 1. Your policy team will then concurrently review and analyze the measurements from these activities and agency policies. This helps to develop an understanding of the overall security of the IT system and its security program. Based on this review, law enforcement managers can determine what changes should be made to multiple systems, if any, to achieve and or maintain the security controls originally established, based on the risk to the systems.

Analyze Results example:

Let's say that you determine that two or more persons are accessing a confidential program from multiple systems with authenticated connectivity to the program. The users do so within a 5-minute window. The agency can review the activity from multiple systems concurrently to determine if there is proper use occurring on their systems by these users. Based on this information, management evaluates the user controls in place to determine if they are effective. Any new decisions then feed back into the overall policy development process to help modify the agency's IT security policies, guidance documents, and/or procedures.

■ Method 3. Assess Overall Agency Effectiveness

This method is used to determine whether an agency's overall information security program is effective and whether it meets or exceeds the agency's security goals and objectives. The team collects information using either Method 1 or 2. When compiled, these data are then used to provide senior managers with the organization's overall picture of information security health. Based on the analysis of these data, feedback is generated back into the policy development process so the agency can modify and improve its initial goals and objectives.

There are commercial products that can assist you in building security measures. A quick Internet search will provide a list of those vendors.

Build Your Agency's Measures in Seven Steps

How do you build your security measurements? Again, we created a seven-step process to make building security measures easier (Figure 20). A worksheet for building each measurement, as described in this chapter, is provided in Appendix B. The worksheet is titled **SEARCH IT Security Measurement Development Worksheet**. We suggest you make numerous copies of this worksheet and get ready to build your measures!

The first two steps to **building a measure** require you to list an identified risk and the control(s) that management decided upon to mitigate this risk. You have already completed these steps in the **building a control** process (Phase III, described in Chapter 5)!

Therefore, you can pull this information *directly* from the SEARCH IT Security Control Development Worksheet.

BUILDING A MEASUREMENT		
	STEP	**ACTION**
1	Identified risk	Start with an identified risk that your agency decided must be mitigated
2	Management control decision	List the control your agency's management decided upon to mitigate this risk
3	Existing measures	List any existing measures in place for assessing the effectiveness of this control
4	All other possible measures	List all possible measures that could be used to assess the effectiveness of this control
5	Measure implications	List the implications associated with each possible measure
6	Measure recommendation	Make a recommendation to management regarding measures to adopt
7	Measure implementation	Management decides which measure(s) to implement

Figure 20: The Seven Steps to Building a Measurement

Step 1

Start with an identified risk that your agency decided must be mitigated

As we have already discussed, conducting a risk assessment of your systems results in identified areas of risk. In Chapter 5, we discussed controls your agency would develop and implement to mitigate these risks. Now, you'll want to measure those controls to determine their effectiveness.

In developing measures to assess these controls, you must first start with an identified area of risk. During Phase III, as outlined in Chapter 5, you already identified areas of risk and developed appropriate controls. This information was recorded on the SEARCH IT Security Control Development Worksheet. **Use this information to help you fill out Steps 1 and 2 of the Security Measurement Development Worksheet.**

Reminder: See Appendix B for the entire SEARCH IT Security Measurement Development Worksheet. Photocopy and use this worksheet to build your measures.

As an example, let's say your agency, through the risk-assessment process, identified this risk: Your agency is not conducting thorough background screening of staff who had access to information systems.

Write the identified risk in Step 1 of the Measurement Development Worksheet, as shown below, copying it from Step 1 of the Control Development Worksheet.

Step 1: Identified risk	Personnel who have not undergone thorough background checks have access to information systems.

Step 2

List the control your agency's management decided upon to mitigate this risk

In Step 2, you will list the control that management selected to mitigate the particular risk, as determined by your agency in Phase III.

Write the management control decision in Step 2 of the Measurement Development Worksheet, as shown below, copying it from Step 6 of the Control Development Worksheet.

Step 2: Management control decision	Conduct background investigations internally using our own employees. Training will be provided by a neighboring agency that conducts its own investigations. Access to a public information database will be purchased and a policy will be written to ensure that proper background investigations are conducted.

Step 3

List any existing measures in place for assessing the effectiveness of this control

Your agency may already have some measures in place to assess the effectiveness of the control for which this measure is being built. Refer to the analysis you did during your self-assessment and the effectiveness rankings you identified during that part of the process to help you define these existing measures.

List existing measures in place at your agency that assess the effectiveness of the control listed in Step 2 of the Worksheet.

Step 3: Existing measures	New employees who will have access to the agency's IT systems must complete a personal history statement.

Step 4

List all possible measures that could be used to assess the effectiveness of this control

Here your team should brainstorm all possible measures that could be used by your organization to gauge the effectiveness of the control. These should include all possibilities, regardless of their cost or effect on the system. Developing as complete a list as possible gives your team options for selecting the most appropriate measurements.

Enter a list of all possible measures in Step 4 of the Worksheet.

Step 4: All other possible measures	• The agency will establish a policy requiring that background investigations be audited every 6 months to ensure that investigations are completed according to procedures. • The agency will complete an annual review of the training received by investigators who conduct the background investigations. • The agency will review the policy governing background investigations every 2 years for currency.

Step 5

List the implications associated with each possible measure

Every suggested measure will have some implication for the agency. Those implications can include the cost of the measure, its installation, maintenance, and update. Your team should discuss and analyze these implications.

Analyze the implications for all possible measures listed in Step 4, and enter them in Step 5 of the Worksheet.

Step 5: Measure implications	Personnel time expended to review measures.

Step 6

Make a recommendation to management regarding measures to adopt

Review all of the possible measures your team has assembled and prepare a recommendation to the agency's executive management about the best measure(s) to implement. Determining which measures are best, as discussed in the steps leading up to your decision, is based on an evaluation of the risk, the controls you implement to mitigate the risk, the costs to implement the measure, and the expertise required to implement and maintain the measure. Your agency management will be expecting your team to provide a substantive recommendation for measuring the agency's controls.

Enter your team's measure recommendation in Step 6 of the Worksheet.

Step 6: Measure recommendation	• The agency will establish a policy requiring that background investigations be audited every 6 months to ensure that investigations are completed according to procedures. • The agency will complete an annual review of the training received by investigators who conduct the background investigations.

Step 7

Management decides which measure(s) to implement

Management now makes a decision as to the measure(s) to implement to evaluate the control listed in Step 2 of the Worksheet. Management may have a variety of possible measures to select from—any of which may effectively assess the control. In this example, the agency chooses a solution that is financially acceptable and effectively measures the control.

Record management's measurement decision in Step 7 of the Worksheet.

Step 7: Measure implementation	The Personnel Division commander will conduct an annual audit of the background investigations section to ensure that they are complying with the agency policy.

As we near the end of this process, you have conducted a self-assessment (Chapter 3) of your systems, determined your security risks (Chapter 4), developed controls to mitigate the risks (Chapter 5), and in this chapter developed measures to assess the effectiveness of these controls. The next phase of the IT security policy development process is actually formalizing and writing your policy, discussed fully in Chapter 7.

CHAPTER 7
FORMALIZE YOUR IT SECURITY POLICIES

"Producing an information security policy should not be seen as a difficult task. What is important is that it should give clear policy direction and management support for the implementation and maintenance of information security. ...Sound policies are the basis for good information security."

—Department of Trade and Industry, United Kingdom

Chapter 7: Formalize Your IT Security Policies

What Writing a security policy involves first reviewing your agency's self-assessment results and identifying your risks. Then it requires that you document your agency's risk decision process and prioritize your response.

Why Management is responsible for properly developing and implementing all organizational policies. A properly written policy allows for consistent administration of a formal information technology (IT) security plan agencywide.

Who Agency leadership (chief, sheriff, and upper management) and the Security Policy Development Team.

When This is the tricky part. You won't be able to complete your written policy until Phases I through IV have been finalized, but your documentation should begin as early as your self-assessment and continue as you work through the phases.

Congratulations! If you have worked through the Tech Guide to this point, you have made it through the most rigorous aspects of completing your security policy. Now, all you have to do is *formalize* the policy for your organization. At this point, when you actually begin writing your agency's IT security policies, your team will have *already completed* significant areas of the policy development process. You will have completed a self-assessment and risk assessment of your systems; you will have determined controls to mitigate your identified risks; and you will have determined how you plan to measure the effectiveness of those controls.

The process up to the point of formalizing your security polices has been a laborious endeavor for any agency. However, now that you and many others have completed the processes in this Tech Guide, you have a better understanding of your system, the risks associated with maintaining it, and, as a result, a rigorously developed policy statement. Your security policy is the foundation for providing *continuous and effective* information security for your agency. Now, quite frankly, all that is left to do is write it!

Remember, a security policy is a document that spells out specific rules and adds structure to the organization's procedures. It gives your agency staff guidance regarding how they should act and respond to given events or situations.

Also keep in mind what we told you in Chapter 1. Security policies must be:

- **Implementable**
- **Enforceable**
- **Responsible**
- **Documented**.

Before you begin writing, here are some frequently asked questions about documenting security policies:

Should the policy be specific or general in nature?

Policy: A plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters.

The answer is: "It depends." Let's take an example that involved a large agency that had many different IT systems. When it came to password control, the security group agreed on what it considered an acceptable password policy at that time. However, because the agency had so many different systems (different operating systems and applications), its target password policy could not be technically implemented equally on all of its systems.

So, what could be done? The security group had two choices:

1) It could formulate an individual policy for each system or groups of systems that can be configured in the required manner.
2) It could write one policy that includes a general exception or language that will accept the strongest password controls available on each system.

As an example, if it chose the latter, the security group could develop a policy that looks something like this:

> "All corporation IT computer systems will require a unique user ID and an eight-character password for access. In addition, the password may not be a dictionary word and it must contain at least one numeric or special character and at least one alphabetic character. If a system cannot be configured to meet this policy, the security group should be contacted immediately to gain an exception to this policy. It is management's goal to implement the strongest possible password controls on each IT system that cannot meet the above guidelines."

Should the policy be all-inclusive or specific in nature?

The answer, again, is: "It depends." You may want to create a policy just for a specific system that has a specific solution. However, if other systems are then installed with

the same characteristics, you would have to go through the policy development process for each new system.

A generalized policy statement dealing with encryption of the case history database might look something like this:

> *"All case investigation data shall be encrypted when stored on any department computer or IT server."*

The implication of this policy is that not only should the case history database be encrypted, but if any investigation data are stored on department PCs or laptops, the data must also be encrypted. This greatly expands the scope of this policy. Management needs to provide guidance in this area if you want to generalize the policies.

When should the policy be reviewed?

Of course, that always depends on the agency involved, the size of the systems, and the perceived risks to the system. At a minimum, if no new risks arise, you should review your policy annually. However, that being said, if new risks arise or new systems or applications are put into service, then your agency should review all relevant policies to ensure that they still apply. Also, when conducting your review, maintain a record of your previous reviews and any changes you made. This will make reviewing a new policy easier if you have a record of the previous area of concern.

Write an Information Security Policy in Six Steps

How do you write security policies? Before you can even *think* about writing security policies, your agency must first complete the self-assessment and risk assessment of its IT systems. As described in earlier chapters, the purpose of these assessment processes is to fully identify the risks inherent in your systems. Only after a full system assessment can you successfully create and write comprehensive security policies.

Once your team completed the risk assessment and identified the risks in your systems, the team presented this list of risks to your senior management. Management will have responded with thoughts about the risks that are acceptable and those that are not. (Remember the four levels of risk tolerance? They are **avoid, assume, mitigate,** or **transfer**.) In addition, management will have provided ideas on how much the unacceptable risks need to be reduced to be acceptable.

How do you start writing your information security policies? We have developed a six-step process to make it easier to write these policies (Figure 21). A worksheet for writing your policy, as described in this chapter, is provided in Appendix B. The

worksheet is titled **SEARCH IT Security Policy Development Worksheet**. We suggest you make numerous copies of this worksheet and get ready to write your policies!

Remember: Your worksheets and risk statements should not be accessible to anyone outside of your organization. You do not want to advertise your vulnerabilities!

This step-by-step process will help guide you through the process of writing your security policy. You should create one Security Policy Development Worksheet for each risk identified during the risk-assessment process. Only one risk should be enumerated on each sheet. Remember, these worksheets are not designed to be published. You really don't want to advertise what risks you have so the "bad guys" know where your weaknesses are!

WRITING AN IT SECURITY POLICY		
	STEP	**ACTION**
1	Identified risk	Start with an identified risk that your agency decided must be mitigated (Phase II)
2	Management control decision	List the control your agency's management decided upon to mitigate this risk (Phase III)
3	Measure implementation	List the measure(s) your agency management decided to implement in order to assess the effectiveness of this control (Phase IV)
4	Existing policy	Document any existing policy the agency has that addresses the risk identified in Step 1
5	Proposed security policy	List any proposed security policy
6	Policy recommendation	Make a recommendation to management regarding security policy to adopt

Figure 21: The Seven Steps to Writing an IT Security Policy

Again, much of your writing here should be informed by the work completed in the preceding phases of your security policy development process, as outlined in Chapters 3 through 6. For each step below, we'll indicate which "source documents" you should use to help complete that particular step.

Source Document—Control Development Worksheet

Reminder: See Appendix B for the entire Security Policy Development Worksheet. Photocopy and use this worksheet when writing your policies.

Step 1

Start with an identified risk that your agency decided must be mitigated (Phase II)

Conducting a risk assessment of your system, as done in Phase II, results in specific identified areas of risk. Your agency will determine which ones to mitigate through the development of controls, as done in Phase III.

Remember we said that writing a policy will build on work you have already done? Since you have *already* identified areas of risk, you can use that information now!

Need a refresher course?
—Phase II: Identify risk areas (Chapter 4)
—Phase III: Select controls (Chapter 5)
—Phase IV: Select measures (Chapter 6)

The specific identified risk was recorded on the SEARCH IT Security Control Development Worksheet. Use this to help you fill out the Security Policy Development Worksheet. Let's use the same "risk" example cited earlier in this Guide—inadequate background checks of agency personnel.

Write the identified risk in Step 1 of the Policy Development Worksheet, as shown below, copying it from Step 1 of the Control Development Worksheet.

Step 1: Identified risk	Personnel who have not undergone thorough background checks have access to information systems.

Step 2

List the control your agency's management decided upon to mitigate this risk (Phase III)

Source Document
—Control Development Worksheet

In Step 2, you will list the management control decision made to mitigate the risk, as determined by your agency in Phase III.

Write the management control decision in Step 2 of the Policy Development Worksheet, as shown below, copying it from Step 6 of the Control Development Worksheet.

Step 2: Management control decision	Conduct background investigations internally using our own employees. Training will be provided by a neighboring agency that conducts its own investigations. Access to a public information database will be purchased and a policy will be written to ensure that proper background investigations are conducted.

Step 3

List the measure(s) your agency management decided to implement in order to assess the effectiveness of this control (Phase IV)

Source Document
—Measurement Development Worksheet

In Step 3, you will list the measure(s) your agency management implemented for this control, a task completed in Phase IV. Remember, the measure is intended to assess the control's effectiveness at mitigating the stated risks.

Write the measurement implementation statement in Step 3 of the Policy Development Worksheet, as shown below, copying it from Step 7 of the Measurement Development Worksheet.

Step 3: Measure implementation	The Personnel Division commander will conduct an annual audit of the background investigations section to ensure that they are complying with the agency policy.

Source Documents
—Existing agency policy documents
—Documents collected during the self-assessment process

Step 4

Document any existing policy the agency has that addresses the risk identified in Step 1

Your agency may already have some policies in place to aid in the security of your systems. You should list all of them here that pertain to the statement identified in Step 1. Refer to the analysis you did during your self-assessment exercise and the effectiveness rankings you identified during that exercise to help you identify these policies.

In Step 4 of the Worksheet, document any existing policy the agency has that relates to the risk identified in Step 1.

Step 4: Existing policy	No current policy statement exists within the agency for this identified risk.

Step 5

List any proposed security policy

Now let's write your *proposed security policy*. This is where you actually begin to create the policy statement for this risk, which can be used to guide your organization. The policy statement should focus only on the item listed in Step 1. You are merely trying to (a) create a policy that (b) refers to the measurement that (c) is related to a specific control that (d) deals with a specific identified risk in your organization. The policy statement should not simply reiterate the identified risk stated in Step 1. The policy should be as clear and unambiguous as possible.

Things to consider when writing a policy statement:

Who will be affected by the policy?
Describe what portion of the agency will be affected by this policy. You need to clearly describe the roles and responsibility of those who will implement the policy and for anyone else the policy affects.

What will be allowed and what will not?
The policy should describe not only what will be allowed, but what will *not* be allowed. It is important to clearly define the things that your personnel can and cannot do.

What will happen if the affected agency personnel do not comply with the policy?
Compliance is always an important factor in policy development. Your policy should clearly delineate what will happen if personnel fail to comply with the policy or any of its provisions.

Record your agency's proposed policy statement in Step 5 of the Worksheet.

Step 5: Proposed security policy	This policy will affect all members of the agency. The agency will immediately begin conducting thorough background checks of all employees, civilian or sworn, who have access to agency systems. The checks will be conducted by the background unit, which will be an ancillary responsibility of the Detective Division commander. Any personnel failing to complete the background process will be administratively suspended until such time as the background can be properly completed. Personnel who, through the investigation, do not obtain a satisfactory background check shall be referred to the personnel section for reassignment within the agency.

Step 6

Make a recommendation to management regarding the security policy to adopt

The IT security policy team makes a recommendation to the agency management about the security policy that it has determined should be adopted. Using the Security Policy Development Worksheet, your team can show management the lengthy and in-depth process involved in making a policy determination for the agency. With the recommendation and the supporting development process in hand, your executive management can make a well-educated policy determination.

Record your team's security policy recommendation in Step 6 of the Worksheet.

Step 6: Policy recommendation	• This policy will affect all new employees who have been given a conditional offer of hire. • A thorough background check of the new hire will be completed prior to the person's assignment to a position that will give him or her access to the agency's system. • Under the direction of the commander in charge of Administration, the detectives assigned to background investigations will conduct a thorough background check according to the procedures developed at the direction of the commander and approved by the chief of the agency. • Due to the sensitive nature of the background check process, only the commander in charge of Administration, the agency assistant chief, the agency chief, and the agency counsel will be allowed to review the completed background information. • New hires failing to complete the background process will be promptly notified of their status and referred to the personnel section.

Conclusion

Throughout this process you have evaluated your agency and its systems. You looked at the systems and determined their associated risk. You have developed controls and measurements for those controls. Last, you have worked on developing policy based on all the reviews you have completed of your system. Each step in the process of writing the IT security policy has been fed from another phase of the process. The work you did in each phase has helped to determine the direction that your organization desired to take.

Based on everything you have done up to this point, you will have a better understanding of your system. You will have developed a cohesive working group to determine future risk to the system. You will have developed controls that will assist you in protecting your system. By implementing a process for regularly assessing the effectiveness of those controls, you will also have developed measures that will help to maintain the security of your system. Finally, you will have developed a set of comprehensive policy statements that can help to guide your agency with its continuing requirements to protect your systems.

Appendix A: Assessment Worksheets and Questions

from the
SEARCH IT Security Self- and Risk-Assessment Tool

Appendix A: Assessment Worksheets and Questions

from the SEARCH IT Security Self- and Risk-Assessment Tool

The Assessment Tool was developed using Microsoft Excel. If you do not have this application, you can download a free Excel reader at **www.microsoft.com/downloads**.

The following are the assessment questions from the SEARCH IT Security Self- and Risk-Assessment Tool, a Microsoft Excel-based spreadsheet tool that enables an agency to perform assessments of its IT systems. (See Chapter 3 for an overview of this Assessment Tool, which can be downloaded at **www.search.org**.)

The questions are listed here to enable you to replicate the exercises in this Assessment Tool spreadsheet on paper. This appendix includes the following:

- Blank "Effectiveness Ranking/Risk Decisions" response worksheets. We recommend that you photocopy additional copies of these because you will fill one copy of these out for each question in the Assessment Tool. The response worksheets include these fields:
  - —**Effectiveness Ranking**, Levels 1 through 5.
  - —**Description of Identified Risk** (a narrative text description).
  - —**Risk Decisions**, which include Likelihood, Severity, Risk Tolerance, and Action Priority.
  - —**Comments** (narrative text).
- An Effectiveness Ranking table, which describes the five effectiveness ranking levels, includes comments on each level that are available in the online Assessment Tool, and provides the appropriate response key (Y for yes, N for no, Partial, N/A).
- A Risk Decisions table, which lists the four types of risk decisions that need to be answered for each identified risk, and provides the appropriate response key for each risk decision.

- Eighteen groups of assessment questions, which are divided into four main categories. The questions include reference document notations, and comments, if any.

Management

1. Risk Management.
2. Review of Security Controls.
3. Lifecycle.
4. Authorize Processing (Certification and Accreditation).
5. System Security Plan.

Operational

6. Personnel Security.
7. Physical and Environment Protection.
8. Production, Input/Output Controls.
9. Contingency Planning.
10. Hardware and System Software Maintenance.
11. Data Integrity.
12. Documentation.
13. Security Awareness, Training, and Education.
14. Incident Response Capability.

Technical

15. Identification and Authentication.
16. Logical Access Controls.
17. Audit Trails.

State and Local Law Enforcement-Specific IT Security

18. FBI CJIS Compliance.

Question # _____

Effectiveness Ranking					Description of Identified Risk	Risk Decisions				Comments
Level 1	Level 2	Level 3	Level 4	Level 5		Likelihood	Severity	Risk Tolerance	Action Priority	

Question # _____

Effectiveness Ranking					Description of Identified Risk	Risk Decisions				Comments
Level 1	Level 2	Level 3	Level 4	Level 5		Likelihood	Severity	Risk Tolerance	Action Priority	

Levels	Meaning	Answers
LEVEL 1: Documented Policy	Does your agency have a formally documented and disseminated policy on that security control? Does the policy define 1) purpose and scope of the policy, 2) responsibilities required for its execution, and 3) compliance requirements and penalty specification?	Each level must be answered with **Yes**, **No**, **Partial**, or **N/A** (not applicable)
LEVEL 2: Documented Procedures	Does your agency have formal, complete, and well-documented procedures for the policies defined at level 1? Do the procedures: • List the control areas and clearly state the agency's position? • Document their applicability—clearly list when, where, how, to whom, and about what the procedure applies? • List the assignment of IT responsibilities and define explicit behavior? • Identify points of contact and where supplementary information can be found?	
LEVEL 3: Implemented Procedures and Controls	Have the procedures and controls been implemented? Are the following statements true? • Are the owners and users aware of the security policies and procedures? • Have the policies and procedures been formally adopted and the technical controls installed? • Is a security metrics program in place? (ongoing security compliance measurement) • Has management formally authorized the use of the system? • Have employee job descriptions been updated to include security responsibilities that the implemented controls require? • Have employees been trained on security procedures?	
LEVEL 4: Tested and Evaluated Procedures and Controls	Is a metrics program in place that routinely evaluates the adequacy and effectiveness of security policies, procedures, and controls? Are the following elements in place? • An effective program for evaluating the adequacy and effectiveness of security policies, procedures, and controls. • A mechanism for identifying vulnerabilities revealed by security incidents or security alerts. • A process for reporting significant security weaknesses and ensuring rapid and effective remedial action.	
LEVEL 5: Fully Integrated Procedures and Controls	Does your agency have a fully operational, comprehensive security program that is an integral part of your agency's culture? Are the following statements true? • There is an active agencywide security program that achieves cost-effective security. • IT security is an integrated practice within the asset (IT system). • Security vulnerabilities are understood and managed. • Threats are continually reevaluated, and controls are adapted to a changing security environment. • Additional and/or more cost-effective security alternatives are identified as the need arises. • Costs and benefits of security are measured as precisely as practicable. • Status metrics for the security program are established and met.	

Risk Decisions	
Decision	***Response Key***
Likelihood	REMOTE: The risk probably will not occur because the risk would be difficult to realize, or there are solid means in place to limit the risk appropriately. POSSIBLE: The risk has a chance of occurring, but it may be difficult or there are controls in place to help avoid the risk. LIKELY: Due to conditions and capabilities, the risk is likely to occur.
Severity	LOW: The risk is manageable through planning and action, and the impacts generally are minimal. MEDIUM: The risk will be mitigated through planning and action, although if it occurs, it will still have some impact on some of the more important areas of concern. HIGH: The risk will have serious impacts and without extensive planning and action, its consequences would be severe.
Risk Tolerance	AVOID: Avoidance is often used for risks that have the capacity for negative impact, but have little known recourse. In security projects, a decision to avoid risks often means a decision not to let your agency put itself in the situation where it could incur the risk. Therefore, your decision would also be to avoid the cause of the risk. ASSUME: The decision to assume a risk means accepting the risk as-is, and not implementing any policies or procedures to lessen it. This is often the decision in cases where the risk is so minimal and of limited impact should it occur that the cost of implementing a mechanism to minimize or reduce it would be far greater than the agency's concern. MITIGATE: This is the most common decision to make for identified risks: to implement policies, procedures, and other security controls to limit the risk to an acceptable level. TRANSFER: Transfer the responsibility for a system or the risk itself to another party that can better accept and deal with the risk and/or has the resources necessary to properly mitigate the risk.
Action Priority	Ranking the risk according to your categorization, quantification, and tolerance of each based on the likelihood, severity, and tolerance levels. This simple weighting allows for the agency to easily rank the priority of action required to eliminate the greatest risks first. Examples of possible weighting: 1 = Likely+High+Assume 2 = Possible+Medium+Mitigate 3 = Remote+Low+Transfer

MANAGEMENT

1. Risk Management
Ref: NIST SP 800-53 RA-2; OMB Circular A-130, III

ASSESSMENT QUESTIONS

1.1. Critical Element: Is risk periodically assessed?
Ref: None

1.1.1 Is the current system configuration documented, including links to other systems?
Ref: None

1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change, and is management made aware of any new risks?
Ref: None

1.1.3 As changes are made to the system, are risk assessments completed and presented to management?
Ref: None

1.1.4 Have data sensitivity and integrity of the data been considered?
Ref: NIST SP 800-53 RA-2; FISCAM SP-1

1.1.5 Have threat sources, both natural and man-made, been identified?
Ref: NIST SP 800-53 RA-3; FISCAM SP-1

1.1.6 Have you identified, documented, and maintained a current list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources?
Ref: NIST SP 800-53 CA-5, RA-3; NIST SP 800-30

1.1.7 Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities?
Ref: NIST SP 800-53 RA-3; NIST SP 800-30

1.2. Critical Element: Does the manager responsible for the system understand the risk to systems under his or her control and determine the acceptable level of risk?
Ref: None

1.2.1 Are final risk determinations and related management approvals documented and maintained on file?
Ref: NIST SP 800-53 RA-3; FISCAM SP-1

1.2.2 Has a mission/business impact analysis been conducted?
Ref: NIST SP 800-53 RA-3; NIST SP 800-30

1.2.3 Have controls been identified to sufficiently mitigate identified risks?
Ref: NIST SP 800-53 CA-5, RA-3; NIST SP 800-30

COMMENTS

1.1 IT systems exist in ever-changing environments. Consequently, the risk profile of your IT system changes over time. **Does your agency have any policy that requires a reassessment of IT system risk on a periodic basis?** This needs to be done to manage the overall risks of the IT system and keep the level of risks acceptable to management.

1.1.1 In order to understand the risks to your IT system, the system must be fully documented. At a minimum, it should contain the following: 1) a description of all functions, 2) a data dictionary of all data collected / used by the system, and 3) a description of all reports / output data. In addition, links to other systems must be fully documented. This documentation should contain: 1) a description of the link (what it is, how it is established, and so forth), and 2) a description of the data sent over the link and under what circumstances.

1.1.2 Your agency should have a policy that requires periodic security reassessments of IT systems. Your agency should document the results of the assessments and store them for reference.

1.1.4 Sensitive data – Any data whose release could cause adverse consequences to your agency.

Data integrity – The high probability that data are not altered inadvertently.

All data collected and processed in your IT system should be classified as to their sensitivity and by their integrity requirements. Data such as social security numbers, child protective services case data, and investigative data would be considered sensitive data. Data such as drug test results would require a high level of integrity.

1.1.5 Threat – The potential that something bad may happen to your IT system.

Some natural threat sources are earthquake, tsunamis, or fire. Some man-made threat sources are theft of hardware, fire, hacking, theft of data, etc.

1.1.6 Your agency should have a policy in place that requires a periodic assessment of the potential threats to your IT system. Write this list down and maintain it.

Your agency will need to conduct research to determine what threats might apply to your IT system. If you are using commercial software, your vendor may be able to help you with the list.

1.1.7 This question assumes the following:

1) An existing security policy program is in place.
2) Your management team has reviewed the prepolicy risks and recommended security policies.
3) You have developed security controls, contained within security policies, that are expected to reduce the risks to acceptable levels.

From the above information, you need to determine the probability that the security controls will reduce the risk exposures down to levels that are acceptable to the management team.

1.2 Management must be involved in all levels of risk-management activities. Senior management sets and determines the acceptable risk levels for your agency.

1.2.1 Written records are one of the keys to an effective risk-management program. Without written records, you cannot keep track of where your agency started or why the decisions were made to bring you to where you are now.

1.2.2 The risk-management process first identifies risks associated with your IT system. The impact analysis refers to what would happen if one or more of these risks became reality. The impact focuses on the three security goals of integrity, availability, and confidentiality. You need to quantify, for each risk, the loss of integrity, the loss of availability, and the loss of confidentiality.

2. Review of Security Controls
Ref: NIST SP 800-53 CA-1; OMB Circular A-130, III; FISCAM SP-5; NIST SP 800-18

ASSESSMENT QUESTIONS

2.1. Critical Element: Have the security controls of the system and interconnected systems been reviewed?
Ref: None

2.1.1 Has the system and all network **boundaries** been subjected to periodic reviews?
Ref: NIST SP 800-53 CA-2; FISCAM SP-5.1

2.1.2 Has an independent review been performed when a significant change occurred?
Ref: NIST SP 800-53 CA-4; FISCAM SP-5.1; OMB Circular A-130, III; NIST SP 800-18

2.1.3 Are routine self-assessments conducted?
Ref: NIST SP 800-53 CA-2; NIST SP 800-18

2.1.4 Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing?
Ref: NIST SP 800-53 CA-2; OMB Circular A-130, 8B3; NIST SP 800-18

2.1.5 Are security alerts and security incidents analyzed and remedial actions taken?
Ref: NIST SP 800-53 IR-4; FISCAM SP-3-4; NIST SP 800-18

2.2. Critical Element: Does management ensure that corrective actions are effectively implemented?
Ref: None

2.2.1 Is there an effective and timely process for reporting significant weakness and ensuring effective remedial action?
Ref: NIST SP 800-53 CA-4; FISCAM SP-5.1, 5.2; NIST SP 800-18

COMMENTS

2.1 Very few IT systems are stand-alone systems. Most systems receive data from and/or supply data to other systems. The security of your target system under review is dependent on the security of these other systems. It is critical that you identify ALL interconnected systems and understand how they relate to your target system.

Management has the responsibility to request a review of these security interrelationships.

2.1.1 Systems and networks change all the time. You should have a policy in place that requires a formal review of system and network interconnections relating your IT systems.

2.1.2 A common human tendency is to be oblivious to various facts at various times. It is simply difficult for any single person to see all the security issues concerning a particular IT system. An independent review brings another set of eyes to look at your system and perhaps see things that you missed. You should encourage independent reviews of your system to gain this perspective.

2.1.3 The self-assessment process is not an all-or-nothing activity. You may choose to do a simple self-assessment on an annual basis for small systems. Only if you identify that complex changes have occurred should you do a more in-depth self-assessment. It is really up to you to determine how often self-assessments should be conducted.

2.1.4 These tests and examinations are part of the security measurement program. The purpose of this program is to establish ongoing tests to verify that your security controls (which derive from your security policies) are effective in reducing risks as expected. These tests and subsequent reporting should be as automated as possible to reduce the possibility that someone will fail to accomplish a required task.

2.1.5 This activity is part of the security metric program. You should verify that management has appointed a person or a group that is responsible for reacting to and handling security alerts and incidents.

2.2 Management should mandate that corrective actions must be implemented for security issues. This will generally require some form of communication on security issues to be presented to management on a recurring basis.

2.2.1 Identify how management has elected to receive input on security matters. If there is no formal process, a process needs to be created to ensure effective communication.

3. Lifecycle
Ref: NIST SP 800-53 SA-1; OMB Circular A-130, III; FISCAM CC-1.1

ASSESSMENT QUESTIONS

3.1. Critical Element: Has a system development lifecyle methodology been developed?
Ref: None

Initiation Phase

3.1.1 Is the sensitivity of the system determined?
Ref: NIST SP 800-54 RA-1; OMB Circular A-130, III; FISCAM CC-1.1, 1.2; NIST SP 800-18

3.1.2 Does the plan document the resources required to adequately secure the system?
Ref: NIST SP 800-53 SA-2; Clinger-Cohen

3.1.3 Are authorizations for software modifications documented and maintained?
Ref: NIST SP 800-53 CM-3; FISCAM CC-1.1

3.1.4 Does the budget request include the security resources required for the system?
Ref: NIST SP 800-54 RA-1; GISRA

Development/Acquisition Phase

3.1.6 During the system design, are security requirements identified?
Ref: NIST SP 800-54 SA-4; NIST SP 800-18

3.1.7 Was an initial risk assessment performed to determine security requirements?
Ref: NIST SP 800-54 RA-3, SA-4; NIST SP 800-30

3.1.8 Is there a written agreement with program managers on the security controls employed and residual risk?
Ref: NIST SP 800-54 RA-3; NIST SP 800-18

3.1.9 Are security controls consistent with and an integral part of the IT architecture of the agency?
Ref: NIST SP 800-54 CM-2; OMB Circular A-130, 8B3

3.1.10 Do the solicitation documents (e.g., requests for proposals) include security requirements and evaluation/test procedures?
Ref: NIST SP 800-54 SA-4; NIST SP 800-18

3.1.11 Do the requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented?
Ref: NIST SP 800-54 SA-4; NIST SP 800-18

Implementation Phase

3.2. Critical Element: Are changes controlled as programs progress through testing to final approval?
Ref: None

3.2.1 Are design reviews and system tests run prior to placing the system in production?
Ref: NIST SP 800-54 SA-8, SA-11; FISCAM CC-2.1; NIST SP 800-18

3.2.2 Are the test results documented?
Ref: NIST SP 800-54 SA-8, SA-11; FISCAM CC-1.1, 1.2; NIST SP 800-18

3.2.3 If required to meet a required federal standard, is certification testing of security controls conducted and documented?
Ref: NIST SP 800-54 CA-4, SA-5; NIST SP 800-18

3.2.4 If security controls were added since development, has the system documentation been modified to include them?
Ref: NIST SP 800-54 SA-5; NIST SP 800-18

3.2.5 If security controls were added since development, have the security controls been tested and the system recertified?
Ref: NIST SP 800-54 CA-4; FISCAM CC-2.1; NIST SP 800-18

3.2.6 Has the application undergone a technical evaluation to ensure that it meets applicable state, local, and federal laws, regulations, policies, guidelines, and standards?
Ref: NIST SP 800-54 SA-11; NIST SP 800-18

Operation/Maintenance Phase

3.2.7 Has a system security plan been developed and approved?
Ref: NIST SP 800-54 S5-1; OMB Circular A-130, III; FISCAM CC-2.1; NIST SP 800-18

3.2.8 If the system connects to other systems, have controls been established and disseminated to the owners of the interconnected systems?
Ref: NIST SP 800-54 CA-3; NIST SP 800-18

3.2.9 Is the system security plan kept current?
Ref: NIST SP 800-54 PL-3; OMB Circular A-130, III; FISCAM CC-2.1; NIST SP-800-18

Disposal Phase

3.2.10 Are official electronic records properly disposed of or archived?
Ref: NIST SP 800-54 MP-6; NIST SP 800-18

3.2.11 Are information or media purged, overwritten, degaussed, or destroyed when disposed of or used elsewhere?
Ref: NIST SP 800-54 MP-6, MP-7; OMB Circular A-130, III; FISCAM CC-AC-3.4; NIST SP 800-18

3.2.12 Is a record kept of who implemented the disposal actions and verified that the information or media were sanitized?
Ref: NIST SP 800-54 MP-6, MP-7; NIST SP 800-18

COMMENTS

3.1 If your agency is considering implementing a major IT system, then you need to select one of the several system development life cycle methodologies available. It is not that one methodology is better that another, but it is far more important that one is selected and followed for the life of the project.

3.1.1 The NIST guide SP 800-30 can assist you in determining the sensitivity of the system. The sensitivity of the system may be driven by the nature of the data or by specific legislation. In any event, you should understand why the system is sensitive before you begin the risk management process.

3.1.2 The required elements to secure your system may come from several sources. Some of the sources may be:

1) Management directive.
2) Legislation.
3) External controls (i.e., the FBI Criminal Justice Information Services [CJIS] Division's *CJIS Security Policy*).

3.1.3 As part of the security management process, your agency should record and file all changes to the system. This information is then referenced during subsequent self-assessment activities. This is the only way you can successfully track modifications to and maintenance of your IT systems.

3.1.4 Security needs to be designed into the system, not added on later. It is significantly less expensive to add security during the design process than after the system has been implemented.

3.1.6 During or before system design, your agency should identify security risks through analysis of the data to be processed and/or research of legislation controlling or driving the process.

3.1.7 The risk-assessment process is the best way to establish IT system security requirements.

3.1.8 Since security controls may be implemented in various areas outside your agency, the agreements with outside entities should be in writing.

For example: Assume your county IT department is responsible for all IT system operations. If your agency is running a sensitive application, then it would be reasonable that the systems manager perform background checks on all system personnel. Agreements of this type should be in writing.

3.1.9 The first issue is: What is an "IT architecture"?

An IT architecture is a set of decisions that describe how an IT system should be constructed, how the structural elements of the system should be created, and what the relationships should be between those elements. It is unlikely that your agency has an IT architecture. However, an IT architecture can be quite simple and very general.

If your agency has an IT architecture—which is really a set of design parameters that is applied generally to all systems in your organization—then you can answer this question: "If you have an IT architecture, does the specific system under review adhere to those parameters?" If not, then you need to explain the differences and why the system deviates from the standards established for your agency.

3.1.10 This question simply asks if security planning is part of the process.

3.1.11 Does your agency, when contracting with outside suppliers, include security requirements and/or security specifications, either explicitly or by reference, in IT system acquisition contracts based on an assessment of risk? In other words, can the system be updated to handle new risks that are discovered during the lifetime of the system?

3.2.1 It is prudent to verify the proper operation of a system before it is placed into production.

3.2.2 Like the rest of the risk management process, all test results should be documented.

3.2.3 In support of the security accreditation process, the organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

3.2.4 Is your documentation up to date?

3.2.5 Depending on the complexity of the changes, you may choose to retest the system to verify proper operation of the security controls.

3.2.6 This is one area that will require some investigation to determine what laws apply to your IT system. Since each state is different, you will need to have legal assistance to determine what legislation or policies apply to your system.

For example, if you are a law enforcement agency and are using the FBI's National Crime Information Center (NCIC), then you will need to comply with *CJIS Security Policy* Version 4.0.

3.2.7 The organization should ensure that 1) adequate documentation for the IT system and its constituent components is available, 2) it protects the documentation when required, and 3) distributes the documentation to authorized personnel.

3.2.8 A security policy simply states what needs to happen. Security controls are either the programs or procedures that actually implement the intent of the security policies.

For example, if you had a security policy that said all passwords must be at least eight characters in length, then the security control(s) would be anything that helped to enforce this policy. Depending on the system, the control may simply be a part of a configuration window that enforces a certain password length. For other systems, it may be a short section of code that controls the minimum password length.

The question assumes that your agency has security policies that cover the security aspects of what happens when external systems interface with your systems. It also assumes that you have developed security controls that implement and enforce your security policies and that they have been designed for these foreign systems. The question is simply asking whether you have given these controls to the owners of the foreign systems and if they have been implemented.

For example: You are responsible for the IT system that is used by child protective services. Another agency in the county government needs to have access to some of the data to do its job. Because of the sensitivity of the data and the legislation covering the use of the data, you have created a security policy that states that all users of the system must be identified before they can access the data. The other agency is using a batch program to access and process this data. Because of your policy, you need to be assured that security controls are in place so that only the authorized batch program has access to your data. Whether you developed the controls, or the other agency did, you need to verify that the controls are in place and effective in controlling access to your data.

3.2.9 Is it the intent of management to fund the staff necessary to keep the security plan current?

3.2.10 "Official" is whatever your policies say they are or how any controlling legislation defines them. The responsibility to dispose of or archive records rests solely on the legislative or policy definitions of the data.

For example, if you have a database of what your group orders for lunch once a week, there probably would not be any issues connected with the disposal or archiving of this data. However, if you happen to have a backup tape that contains case records from child protective services, it is doubtful that you would be permitted to throw the tape away if part of the tape is thought to be defective.

3.2.11 Do you have proven procedures and/or mechanisms to enable you to truly purge and/or destroy data?

3.2.12 Depending on the classification or sensitivity of the data to be destroyed, do you keep records of these actions?

4. Authorize Processing (Certification and Accreditation)
Ref: NIST SP 800-53 CA-1; OMB Circular A-130, III; FIPS 102

ASSESSMENT QUESTIONS

4.1. Critical Element: Has the system been certified/recertified and authorized to process (accredited)?
Ref: None

4.1.1 Was a technical and/or security evaluation completed or conducted when a significant change occurred?
Ref: NIST SP 800-53 CA-4; NIST SP 800-18

4.1.2 Was a risk assessment conducted when a significant change occurred?
Ref: NIST SP 800-53 RA-4; NIST SP 800-18

4.1.3 Have rules of behavior been established and signed by users?
Ref: NIST SP 800-53 PL-4; NIST SP 800-18

4.1.4 Has a contingency plan been developed and tested?
Ref: NIST SP 800-53 CP-2, CP-4; NIST SP 800-18

4.1.5 Has a system security plan been developed, updated, and reviewed?
Ref: NIST SP 800-53 PL-4; NIST SP 800-18

4.1.6 Are in-place controls operating as intended?
Ref: NIST SP 800-53 CA-4; NIST SP 800-18

4.1.7 Are the planned and in-place controls consistent with the identified risks and the system and data sensitivity?
Ref: NIST SP 800-53 RA-3; NIST SP 800-18

4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization, or contractor)?
Ref: NIST SP 800-53 CA-3; NIST SP 800-18

4.2. Critical Element: Is the system operating on a temporary or interim authorization in accordance with specified agency procedures?
Ref: None

4.2.1 Has management initiated prompt action to correct deficiencies?
Ref: NIST SP 800-53 CA-5; NIST SP 800-18

COMMENTS

4.1.1 This activity is part of the security measurement process. Simply stated: A significant change could 1) increase risk, and/or 2) reduce risk, and/or 3) render existing security controls ineffective. The security evaluation is necessary to detect these potential changes.

4.1.2 Depending on the complexity of the change, you may choose to do a full risk assessment on the system.

4.1.3 Do the people using the system know how to treat the data under their care? A signed agreement with each employee working on sensitive data is perhaps the best way to communicate the proper behavior.

4.1.4 All agencies or businesses should have a contingency plan for business continuity. If you don't have one, your agency should develop such a plan.

4.1.5 This question is simply asking whether the system security plan is authorized by the proper authority.

4.1.6 Part of the security measurement process includes the monitoring of security control operations. The processes to monitor the controls should be as automated and cost effective as possible.

4.1.7 Was the security policy development process followed? Did management review the risks discovered during the self-assessment and approve the security controls necessary to mitigate the risks to levels acceptable to the agency?

4.1.8 Management should be aware of all interconnections to external systems. This notification should be part of standard operating procedures.

4.2.1 Has management funded and staffed personnel to handle security issues? Is there a charter that directs staff to deal with security issues promptly?

5. **System Security Plan**

ASSESSMENT QUESTIONS

5.1. Critical Element: Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?
Ref: None

5.1.1 Has the system security plan been approved by the managers of the affected parties (stakeholders) within and outside of the agency?
Ref: NIST SP 800-53 PL-2; FISCAM SP-2.1; NIST SP 800-18

5.1.2 Does the plan contain the topics prescribed in NIST Special Publication 800-18?
Ref: NIST SP 800-53 PL-2; NIST SP 800-18

5.1.3 Is a summary of a systems security plan incorporated into the agency's strategic information resources management plan?
Ref: NIST SP 800-53 SA-2; OMB Circular A-130, III; NIST SP 800-18

5.2. Critical Element: Is the plan kept current?
Ref: None

5.2.1 Is the plan reviewed periodically and adjusted to reflect current conditions and risks?
Ref: NIST SP 800-53 PL-2; FISCAM SP-2.1; NIST SP 800-18

COMMENTS

5.1.1 Your agency management needs to be involved, as do external stakeholders.

5.1.2 The NIST topics are guidelines only—good guidelines, but not mandated.

5.1.3 The security plan should be a part of an Information Resources Management (IRM) plan, which is an overarching plan that:

1) Supports enterprise and agency vision, mission, goals, and objectives.
2) Aligns the IT budget with the business plan.
3) Identifies and tests innovative ways to use technology to serve customers and expand opportunities for public access.
4) Improves agency efficiency by effectively managing information and technology.

5) Promotes partnerships with other agencies, local/regional jurisdictions, and the private sector to create mutually beneficial IRM communities.
6) Demonstrates compliance with city/county/state technical architecture and standards through IT asset inventory and the creation of application portfolios.
7) Identifies IT and technical staff resources and training needs.

5.2.1 All plans should be reviewed periodically and adjusted for changes in the environment.

OPERATIONAL

6. **Personnel Security**
Ref: NIST SP 800-53 CA-1; OMB Circular A-130, III; FISCAM SP-5; NIST SP 800-18

ASSESSMENT QUESTIONS

6.1. Critical Element: Are duties separated to ensure least privilege and individual accountability?
Ref: None

6.1.1 Are all positions reviewed for sensitivity level?
Ref: NIST SP 800-53 CA-2; FISCAM SP-5.1

6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties?
Ref: None

6.1.3 Are sensitive functions divided among different individuals?
Ref: None

6.1.4 Are distinct systems support functions performed by different individuals?
Ref: NIST SP 800-53 CM-5; FISCAM SD-1.1

6.1.5 Are mechanisms in place for holding users responsible for their actions?
Ref: NIST SP 800-53 PS-6; OMB Circular A-130, III; FISCAM SD-2, 3.2; NIST SP 800-18

6.1.6 Are hiring, transfer, and termination procedures established for personnel who have access to sensitive agency IT data?
Ref: NIST SP 800-53 PS-2, PS-5; FISCAM SP-4.1; NIST SP 800-18

6.1.7 Is there a process for requesting, establishing, issuing, and closing user accounts?
Ref: NIST SP 800-53 PAC-2; FISCAM SP-4.1; NIST SP 800-18

6.2. Critical Element: Is appropriate background screening for assigned positions completed prior to granting access?
Ref: None

6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access?
Ref: NIST SP 800-53 PS-3; FISCAM SP-4.1; OMB Circular A-130, III

6.2.2 Are confidentiality or security agreements required for employees assigned to work with sensitive information?
Ref: NIST SP 800-53 PS-6; FISCAM SP-4.1

6.2.3 When access controls cannot adequately protect your information assets, are individuals accessing the data screened prior to access?
Ref: NIST SP 800-53 PS-3; OMB Circular A-130, III

6.2.4 Are there conditions for allowing system access prior to completion of screening?
Ref: NIST SP 800-53 PS-6; FISCAM AC-2.2; NIST SP 800-18

COMMENTS

6.1.1 The question depends on whether your agency deals with data that are defined as "sensitive." If you have any such data that are defined as sensitive by either policy or legislation, this is a legitimate question to ask.

6.1.2 The need to separate duties may be related to the sensitivity of the data or the need to separate duties.

For example, in an accounting environment, you do not want the person who requests a payment to also be able to authorize the payment. Only if you have sensitive data would you need to write controls into the job descriptions.

6.1.3 Sensitive functions should be divided. One of the questions that should be asked is: Should the person who enters or creates data also have the authority to remove the data? Essentially, you want two or more persons involved in the lifecycle of sensitive data.

6.1.4 Another way to look at this issue is: Have you established checks and balances within the system support functions?

6.1.5 How are violations of rules or procedures handled in your organization? As it relates to security, can security issues be handled in a similar fashion?

6.1.6 All organizations should have clear and unambiguous personnel policies that cover hiring, transfer, and termination of employees.

6.1.7 As employees join, transfer, or leave your department or agency, are there written procedures to follow that cover the adding or removal of user accounts?

6.2.1 System support personnel, network engineers, and others who have broad powers over your computing facility need to be held to a higher standard due to their ability to bypass technical and operational controls within your IT system.

6.2.2 These confidentiality or security agreements help clarify what is expected of employees who access sensitive data.

6.2.3 If this can happen, are the procedures to screen an employee documented, and has management signed off on this process?

6.2.4 If personnel can access sensitive data before they are fully cleared by the screening process, is management fully aware of the risks? Ultimately, management bears responsibility for this risk.

7. **Physical and Environmental Protection**
Ref: NIST SP 800-43 PE-1

ASSESSMENT QUESTIONS

Physical Access Control

7.1. Critical Element: Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?
Ref: None

7.1.1 Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics?
Ref: NIST SP 800-53 PE-2, PE-3; FISCAM AC-3; NIST SP 800-18

7.1.2 Does management regularly review the list of persons with physical access to sensitive facilities?
Ref: NIST SP 800-53 PE-2, PE-3; FISCAM AC-3.1

7.1.3 Are deposits and withdrawals of tapes and other storage media from the library authorized and logged?
Ref: NIST SP 800-53 PE-16; FISCAM AC-3.1

7.1.4 Are keys or other access devices needed to enter the computer rooms and tape/media libraries?
Ref: NIST SP 800-53 MP-4; FISCAM AC-3.1

7.1.5 Are unused keys or other entry devices secured?
Ref: NIST SP 800-53 PE-3; FISCAM AC-3.1

7.1.6 Do emergency exit and reentry procedures ensure that only authorized personnel are allowed to reenter after fire drills, etc?
Ref: NIST SP 800-53 PE-3; FISCAM AC-3.1

7.1.7 Are visitors to sensitive areas signed in and escorted?
Ref: NIST SP 800-53 PE-7; FISCAM AC-3.1

7.1.8 Is entry access to restricted IT assets regularly reviewed and entry codes changed periodically?
Ref: NIST SP 800-53 PE-3; FISCAM AC-3.1

7.1.9 Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken?
Ref: NIST SP 800-53 PE-6, PE-8; FISCAM AC-4

7.1.10 Is suspicious access activity investigated and appropriate action taken?
Ref: NIST SP 800-53 AC-13; FISCAM AC-4.3

7.1.11 Are visitors, contractors, and maintenance personnel authenticated through the use of preplanned appointments and identification checks?
Ref: NIST SP 800-53 PE-7; FISCAM AC-3.1

Fire Safety Factors

7.1.12 Are appropriate fire suppression and prevention devices installed and working?
Ref: NIST SP 800-53 PE-13; FISCAM SC-2.1; NIST SP 800-18

7.1.13 Are fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, reviewed periodically?
Ref: NIST SP 800-53 RA-3; NIST SP 800-18

Supporting Utilities

7.1.14 Are heating and air conditioning systems regularly maintained?
Ref: NIST SP 800-53 PE-14; NIST SP 800-18

7.1.15 Is there a redundant air cooling system?
Ref: NIST SP 800-53 PE-14; FISCAM SC-2.2

7.1.16 Are electric power distribution, heating plants, water, sewage, and other utilities periodically reviewed for risk of failure?
Ref: NIST SP 800-53 PE-9; FISCAM SC-2.2; NIST SP 800-18

7.1.17 Are locations of building plumbing lines known and do they not endanger the system?
Ref: NIST SP 800-53 PE-15; FISCAM SC-2.2; NIST SP 800-18

7.1.18 Has an uninterruptible power supply or backup generator been provided?
Ref: NIST SP 800-53 PE-11; FISCAM SC-2.2

7.1.19 Have controls been implemented to mitigate other disasters, such as floods, earthquakes, etc.?
Ref: NIST SP 800-53 RA-3; FISCAM SC-2.2

Interception of Data

7.2. Critical Element: Is data protected from interception?
Ref: None

7.2.1 Are computer monitors located to eliminate viewing by unauthorized persons?
Ref: NIST SP 800-53 PE-5; NIST SP 800-18

7.2.2 Is physical access to data transmission lines controlled?
Ref: NIST SP 800-53 PE-4; NIST SP 800-18

Mobile and Portable Systems

7.3. Critical Element: Are mobile and portable systems protected?
Ref: None

7.3.1 Are sensitive data files encrypted on all portable systems?
Ref: NIST SP 800-53 AC-19; NIST SP 800-18

7.3.2 Are portable systems stored securely?
Ref: NIST SP 800-53 AC-19; NIST SP 800-18

Wireless Use Within the System

7.4. Critical Element: Is wireless access controlled within the system?
Ref: None

7.4.1 Are all wireless access points attached to the system known?
Ref: None

7.4.2 Are regular searches conducted for rogue wireless access points?
Ref: None

PDA Use Within the System

7.5. Critical Element: Is the use of PDAs and other similar devices controlled within the system?
Ref: None

7.5.1 Are PDAs and similar devices that are allowed access to IT systems controlled?
Ref: None

7.5.2 Are PDAs and similar devices that are allowed access to IT systems required to have access control enabled on the devices and/or encryption of sensitive data?
Ref: None

COMMENTS

7.1 The basic question that needs to be asked is this: Are senior managers aware of the current risks inherent with your agency's IT systems, and are they willing to accept this level of exposure?

7.1.1
1) Identify how access is gained to your facilities.
2) Collect the policies and procedures associated with this access.
3) If you are using commercial hardware and/or software to control physical access, obtain the user and system manuals to document the processes.
4) Create a list of persons responsible for controlling this process.

7.1.2
1) If any controlled access is in place, obtain copies of authorization policies and access lists.
2) Determine if management, at any level, has at any time reviewed these lists for accuracy.
3) Determine if any policies or procedures exist for this review process and, if so, obtain copies.

7.1.3
1) Determine if any tapes or other storage media are created in the normal course of business. The "tape library" may be anything from a bottom drawer in someone's desk to a formally organized tape library.
2) If tapes or other storage media are created, determine if policies, procedures, or logs exist. If so, obtain copies of them.

7.1.4
1) Determine if physical devices (keys, fobs, etc.) are required to enter the computer room, tape library, or other controlled area.

7.1.5
1) Determine which person or persons have control of the keys or access devices.
2) Determine if a sign-out list exists for these items. If so, obtain a copy.
3) Determine if extra or backup items are available.
4) Are these items secured? If so, document where they are kept and the policies and procedures used to control them.

7.1.6
1) If there are emergency exits within the computer room, tape library, or other secured area, determine how people regain entrance after exiting.

2) Determine if procedures exist for the reentry process. If so, obtain copies of the procedures.

7.1.7
1) Determine how visitors gain access to secured areas.
2) Are there policies, procedures, or sign-in lists that control visitor access to the facility? If so, obtain copies of the documents.
3) Determine if visitors simply sign in and enter the facility or if they must be escorted.

7.1.8
1) If the controlled entry to the sensitive areas require codes, determine how often they are changed.
2) If there are policies or procedures to change the codes, obtain copies.
3) Determine how code changes are propagated to authorized personnel.
4) Watch out for maintenance access codes. They often are very simple and seldom changed. You should make sure to change these codes at regular intervals.

7.1.9
1) Determine if physical access is monitored and recorded, either manually or automatically, by the access system.
2) If audit trails exist, determine if anyone reviews these for violations. Obtain examples of the audit trails, if they exist.
3) If violations occur, determine what remedial actions should be taken.

7.1.10
1) Determine how personnel report suspicious access activity.
2) Determine if agency training covers this subject.
3) Determine what actions are to be taken when unauthorized access is detected.
4) Determine who is required to investigate these issues.

7.1.11
1) Determine how people are authorized to enter the sensitive areas.
2) Determine if there are policies or procedures that cover access by visitors, contractors, or maintenance personnel.

7.1.12
1) You may need to contact the city or county building department to determine what appropriate fire suppression and prevention devices are required.
2) Building codes change over time. Accordingly, you should verify the building code year that covers your facility.

7.1.13
1) Determine who or what agency is responsible for this activity.
2) If these items are reviewed, how are the results communicated to your management?

7.1.14
1) Identify who maintains the heating and air conditioning systems.
2) Determine if there is a maintenance contract. If so, obtain a copy for your records.

7.1.15
1) If there is a redundant system, determine how it is activated and/or used when the main system fails.

7.1.16
1) Determine who or what agency is responsible for your physical plant.
2) Determine if there is any risk review on major building subsystems.

7.1.17
1) Contact your building manager or other responsible party and determine where water, sewer, and gas lines run in and around your IT areas.

7.1.18
1) This backup power facility may not be required for your agency.
2) If it has been provided, determine how often it is tested. The minimum test period should be annually.

7.1.19
1) Determine what disaster planning has been done for your local jurisdiction.
2) Determine if the plans are tested.
3) Determine how the controls are expected to reduce the impact of these natural disasters.

7.2.1
1) From your list of systems that contain sensitive data, identify monitors used to access this data.
2) Physically inspect each monitor location to verify difficulty in viewing data by unauthorized persons

7.2.2
1) You may require assistance from system and/or network staff to determine how network lines are run.
2) Determine physical access to areas where these lines run.

7.3.1
1) In today's environment, this is a very critical issue.

7.3.2
1) In today's environment, this is a very critical issue.
2) Have users of portable systems been trained in how to use and store them securely on the road and in the office?

7.4.1
1) In today's environment, this is a very critical issue.

7.4.2
1) In today's environment, this is a very critical issue.

8. **Production, Input/Output Controls**
Ref: NIST SP 800-53 MP-1

ASSESSMENT QUESTIONS

8.1. Critical Element: Is there user support?
Ref: None

8.1.1 Is there a help desk or group that offers advice?
Ref: NIST SP 800-53 IR-7; NIST SP 800-18

8.2. Critical Element: Are there media controls?
Ref: None

8.2.1 Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?
Ref: NIST SP 800-53 MP-2, MP-4; NIST SP 800-18

8.2.2 Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media?
Ref: NIST SP 800-53 MP-2, MP-4, MP-5; NIST SP 800-18

8.2.3 Are audit trails used for receipt of sensitive inputs/outputs?
Ref: NIST SP 800-53 MP-2; NIST SP 800-18

8.2.4 Are controls in place for transporting or mailing media or printed output?
Ref: NIST SP 800-53 AC-15, MP-5; NIST SP 800-18

8.2.5 Is there internal/external labeling for sensitivity?
Ref: NIST SP 800-53 MP-3; NIST SP 800-18

8.2.6 Is there external labeling with special handling instructions?
Ref: NIST SP 800-18

8.2.7 Are audit trails kept for inventory management?
Ref: NIST SP 800-53 MP-2; NIST SP 800-18

8.2.8 Are media sanitized for reuse?
Ref: NIST SP 800-53 MP-6; FISCAM AC-3.4; NIST SP 800-18

8.2.9 Are damaged media stored and/or destroyed?
Ref: NIST SP 800-53 MP-4, MP-6; NIST SP 800-18

8.2.10 Are hard-copy media shredded or destroyed when no longer needed?
Ref: NIST SP 800-53 MP-7; NIST SP 800-18

COMMENTS

8.1.1 The second question that should be asked is: What help is the user support group permitted to offer? The range of users that the help desk is designed to help must be clearly defined.

8.2.1 This awareness of how unauthorized persons can obtain copies of data will derive from the self-assessment process. Be sure to review the low-tech methods of stealing data. Methods such as dumpster diving are often very successful.

8.2.2 How does your agency authorize and control the transfer of data? Whatever your processes are, document them clearly.

8.2.3 If your agency is transferring sensitive data, you should consider creating audit trails to provide confirmation of data transfers.

8.2.4 If your agency rarely has the need to transport or mail media or output, then you might not have a formal system to track these transactions. However, if this is done regularly, you should probably have a written log to document these transactions.

8.2.5 Good labeling is an effective way to identify and track sensitive physical items.

8.2.6 Often media will have both an internal label and an external label. Does the visible external label contain a brief explanation of how the data should be handled?

8.2.7 Keeping audit trails could simplify inventory management of media in your agency.

8.2.8 If you sanitize media for reuse as a cost-cutting measure, have you verified whether the process is effective in removing all data from the media?

8.2.9 Your agency should have a policy that covers damaged media.

8.2.10 If you don't have this service, your agency should consider using one of the many shredding services. These services are readily available and are very effective in destroying data.

9. **Contingency Planning**
Ref: NIST SP 800-53 CP-1; OMB Circular A-130, III

ASSESSMENT QUESTIONS

9.1. Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified?
Ref: None

9.1.1 Are critical data files and operations identified and the frequency of file backups documented?
Ref: NIST SP 800-53 CP-2, CP-9; FISCAM SC-SC-1.1, 3.1; NIST SP 800-18

9.1.2 Are resources supporting critical operations identified?
Ref: NIST SP 800-53 MA-6; FISCAM SC-SC-1.2

9.1.3 Has management established and approved processing priorities?
Ref: NIST SP 800-53 CP-7; FISCAM SC-SC-1.3

9.2. Critical Element: Has a comprehensive contingency plan been developed and documented?
Ref: None

9.2.1 Is the plan approved by key affected parties?
Ref: NIST SP 800-53 CP-2; FISCAM SC- 3.1

9.2.2 Are responsibilities for recovery assigned?
Ref: NIST SP 800-53 CP-2; FISCAM SC 3.1

9.2.3 Are there detailed instructions for restoring operations?
Ref: NIST SP 800-53 CP-2; FISCAM SC-3.1

9.2.4 Is there an alternate processing site? If so, is there a contract or interagency agreement in place?
Ref: NIST SP 800-53 CP-6, CP-7; FISCAM SC-SC-1.1, 3.1; NIST SP 800-18

9.2.5 Is the location of stored backups identified?
Ref: NIST SP 800-53 CP-6, CP-7; NIST SP 800-18

9.2.6 Are backup files created on a prescribed basis and rotated off site often enough to avoid disruption if current files are damaged?
Ref: NIST SP 800-53 CP-9; FISCAM SC-2.1

9.2.7 Is system and application documentation maintained at the off-site location?
Ref: NIST SP 800-53 CP-6, CP-7; FISCAM SC-2.1

9.2.8 Are all system defaults reset after being restored from a backup?
Ref: NIST SP 800-53 CP-10; FISCAM SC-3.1

9.2.9 Are the backup storage site and alternative site geographically removed from the primary site and physically protected?
Ref: NIST SP 800-53 CP-6, CP-7, CP-9; FISCAM SC-SC-1.1, 3.1

9.2.10 Has the contingency plan been distributed to all appropriate personnel?
Ref: NIST SP 800-53 CP-2; FISCAM SC-3.1

9.3. Critical Element: Are tested contingency/disaster recovery plans in place?
Ref: None

9.3.1 Is an up-to-date copy of the plan stored securely off site?
Ref: NIST SP 800-53 CP-5, CP-9; FISCAM SC-3.1

9.3.2 Are employees trained in their roles and responsibilities?
Ref: NIST SP 800-53 CP-3; FISCAM SC-2.3; NIST SP 800-18

9.3.3 Is the plan periodically tested and readjusted, as appropriate?
Ref: NIST SP 800-53 CP-4, CP-5; FISCAM SC-3.1; NIST SP 800-18

COMMENTS

9.1.1 This is your primary insurance on recovering your operations. During the self-assessment, it is very important to identify all the linkages between systems. These linkages will help you identify related data in other systems. Having only part of a backup is not a good thing.

9.1.3 Priorities should be derived during the self-assessment phase of the security policy development process. The priorities are set when management reviews the results of the self-assessment and determines the risk level for the agency.

9.2 All business and civil agencies should have a contingency recovery plan in place for their IT systems.

9.2.1 Contingency planning should involve all parties that use a system. All parties need to understand their role in an emergency. With respect to your question, users need to understand what changes occur when the system is recovered in a contingency situation.

9.2.3 Part of any contingency recovery plan should call for duplication of the recovery instructions and their storage in multiple places. During a disaster, your agency should have several options for where to obtain this information.

9.2.4 The choice of an alternate processing site is critical. If the disaster is local to a single building, then there is normally no problem moving to the recovery site. However, if there is a general disaster, and many companies need services, then having an iron-clad contract to deliver services is necessary.

9.2.5 This is not a silly question. The key to disaster planning is "don't assume anything"! Your recovery instructions must contain the location of backups, as well as codes and/or passwords to gain possession of the media.

9.2.6 This is often one of the weak links in the contingency recovery process. After the backup program has been in place for a while, people get lazy and forget to move the backup tapes off site as soon as they should. This is an area that should have an automated check to verify movement of the tapes or media off site.

9.2.7 All documentation to recover your operations should be stored off site. A good contingency recovery plan forces a formal documentation process that will ensure that up-to-date manuals are printed and moved off site.

9.2.8 Test, Test, Test. The only way to catch these types of problems is to conduct full contingency recovery tests.

9.2.9 This question is formulated for a general or regional disaster. The more remote the recovery site, the better the chance that it will be available for use.

9.2.10 In any contingency recovery plan, communication is the key. The contingency recovery plan should include the creation of "What do I do now" packages for each member of the contingency recovery team. The packages outline the steps each person is expected to perform during a recovery operation.

9.3.1 Multiple copies of the plans should be SECURED off site in multiple locations and documented for each contingency recovery team member.

9.3.2 Testing the contingency recovery plan verifies that the plan will work, and also trains members of the contingency recovery team.

9.3.3 Test contingency recovery plans annually because of regular changes that occur in most IT systems.

10. **Hardware and System Software Maintenance**
Ref: NIST SP 800-53 MA-1; OMB Circular A-130

ASSESSMENT QUESTIONS

10.1. Critical Element: Is access limited to system software and hardware?
Ref: None

10.1.1 Are restrictions in place on who performs maintenance and repair activities?
Ref: NIST SP 800-53 CM-5, MA-2, MA-4, MA-5; OMB Circular A-130, III; FISCAM SS-3.1; NIST SP 800-18

10.1.2 Is access to all program libraries restricted and controlled?
Ref: NIST SP 800-53 AC-3, MA-4; FISCAM CC-3.2, 3.3

10.1.3 Are there on-site and off-site maintenance procedures (e.g., escort of maintenance personnel, sanitization of devices removed from the site)?
Ref: NIST SP 800-53 MA-2, MA-3, MA-5; NIST SP 800-18

10.1.4 Is the operating system configured to prevent circumvention of the security software and application controls?
Ref: NIST SP 800-53 CM-5; FISCAM SS-1.2

10.1.5 Are up-to-date procedures in place for using and monitoring the use of system utilities?
Ref: NIST SP 800-53 CM-5; FISCAM SS-3.1

10.2. Critical Element: Are all new and revised hardware and software authorized, tested, and approved before implementation?
Ref: None

10.2.1 Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control?
Ref: NIST SP 800-53 CA-7, CM-4, MA-2; NIST SP 800-18

10.2.2 Are system components tested, documented, and approved (operating system, utility, applications) before promoted to production?
Ref: NIST SP 800-53 CM-3; FISCAM SS-3.1, 3.2, CC-2.1; NIST SP 800-18

10.2.3 Are software change request forms used to document requests and related approvals?
Ref: NIST SP 800-53 CM-3; FISCAM CC-1.2; NIST SP 800-18

10.2.4 Are detailed system specifications prepared and reviewed by management?
Ref: NIST SP 800-53 CM-4; FISCAM SS-3.1

10.2.5 Is the type of test data to be used specified, i.e., live or made up?
Ref: NIST SP 800-53 SA-11; NIST SP 800-18

10.2.6 Are settings of security features set to the most restrictive mode?
Ref: NIST SP 800-53 CM-6; PSN Security Assessment Guidelines

10.2.7 Are software distribution implementation orders, including the effective date, provided to all locations?
Ref: NIST SP 800-53 CM-2; FISCAM SS-3.1

10.2.8 Is there version control?
Ref: NIST SP 800-53 CM-3; NIST SP 800-18

10.2.9 Are programs labeled and inventoried?
Ref: NIST SP 800-53 CM-2, MP-3; FISCAM SS-3.1

10.2.10 Are the distribution and implementation of new or revised software documented and reviewed?
Ref: NIST SP 800-53 CM-3, SA-6, SA-7; FISCAM SS-3.1

10.2.11 Are emergency change procedures documented and approved by management, either prior to the change or after the fact?
Ref: NIST SP 800-53 CM-3; FISCAM SS-3.1

10.2.12 Are contingency plans and other associated documentation updated to reflect system changes?
Ref: NIST SP 800-53 CP-5; FISCAM SC-2.1; NIST SP 800-18

10.2.13 Is the use of copyrighted software or shareware and personally owned software/equipment documented?
Ref: NIST SP 800-53 AC-20, SA-6; NIST SP 800-18

10.3. Are systems managed to reduce vulnerabilities?
Ref: NIST SP 800-53 CM-6

10.3.1 Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls)?
Ref: NIST SP 800-53 CM-7, RA-5; NIST SP 800-18

10.3.2 Are systems periodically reviewed for known vulnerabilities and are software patches promptly installed?
Ref: NIST SP 800-53 SI-2; NIST SP 800-18

COMMENTS

10.1.1 System personnel often have broad authority and access to systems. You should know the background of the people who have these rights. You should also consider controls to track what they do as they perform maintenance and repair activities.

10.1.2 Controlling access to program libraries simply avoids problems. You want your users not to have to worry about inadvertently doing something that adversely affects the system.

10.1.3 While there should always be some procedures for on-site and off-site maintenance, the nature of your data is the determining factor.

10.1.4 This is part of the security assessment and security control development process. The security controls should not be easily circumvented by simple changes to the operating system or application.

10.1.5 System utilities often can be used to access data and bypass security controls. You should evaluate the need for system utilities access in the production environment.

10.2 If an agency had unlimited funds, this would be a nonissue. However, hardware and software would not normally be tested in this fashion except for the more complex or sensitive IT systems.

The basic issue is risk. Management simply needs to understand and accept the risk associated by not conducting this testing. Whatever your answer, the only thing that matters is that management is aware of and accepts the risks associated with the decision.

10.2.1 All changes, especially to security controls, need to be thought through before they are implemented.

10.2.2 This should be part of your agency's standard system implementation procedures.

10.2.3 Communication is the key. Requests for changes should be documented and accepted by management before they are implemented.

10.2.4 System specifications should be as explicit as possible and approved by management before the system is purchased or built.

10.2.5 Creating good test data is very difficult. Processing a copy of production data is good, but usually will not exercise the application completely.

10.2.6 If the security controls can be set to different levels of control, then management must make the decision as to what settings are to be used. The most restrictive mode is not necessarily the one management will select.

10.2.7 This question applies to situations where there is more than one production location. The goal is to keep the organization in sync with each other when the new system is moved into production. This question also applies to distribution of utilities, such as Microsoft Word. Essentially, you want all employees using the same level of software at the same time.

10.2.8 Version control is also sometimes a difficult issue. In the best situation, you should have strong controls to limit the ability of users to use older or newer versions of a specific software product.

10.2.9 This usually relates to original source media and documentation.

10.2.10 Regardless of whether you are using electronic or manual software distribution, management should document and approve these activities.

10.2.11 Emergency change procedures, while necessary, need to be designed carefully so the change can be backed out, if necessary.

10.2.12 This is one of the major costs of maintaining a contingency recovery (CR) plan. IT systems are changed all the time. These changes must be reflected in your CR plans as quickly as possible. The procedures for making software changes or applying maintenance should include updating the CR plans as part of the process.

10.2.13 Businesses and agencies should use only lawfully licensed software. If you permit your employees to use personally owned software, what happens when that employee leaves? Would you have to purchase a copy of the software to access the work product created with that software?

10.3.1 Networks need to be protected because they often connect to the Internet. Unnecessary services should be disabled in the firewall or routers to protect the interior environment. In the mainframe arena, minimizing supervisor calls helps stabilize the application and reduces overhead.

10.3.2 The application owner should ensure that available maintenance is tested and then applied on a regular basis. Researching for systems vulnerabilities does take time, but when these vulnerabilities are identified they can help specify what changes are needed in the system to avoid the problem.

11. **Data Integrity**

ASSESSMENT QUESTIONS

11.1. Critical Element: Is virus detection and elimination software installed and activated?
Ref: None

11.1.1 Are virus signature files routinely updated?
Ref: NIST SP 800-53 SI-1, SI-3; NIST SP 800-16

11.2. Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and that the system functions as intended?
Ref: NIST SP 800-53 SI-3

11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts?
Ref: NIST SP 800-53 SC-8, SI-6, SI-7; NIST SP 800-18

11.2.2 Is inappropriate or unusual activity reported, investigated, and appropriate actions taken?
Ref: NIST SP 800-53 AC-13, SI-2, SI-6; FISCAM SS-2.2

11.2.3 Are procedures in place to determine compliance with password policies?
Ref: NIST SP 800-53 IA-1; NIST SP 800-18

11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?
Ref: NIST SP 800-53 SC-8, SI-7, MA-3; NIST SP 800-18

11.2.5 Are intrusion detection tools installed on the system?
Ref: NIST SP 800-53 SI-4; NIST SP 800-18

11.2.6 Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly?
Ref: NIST SP 800-53 SI-4; NIST SP 800-18

11.2.7 Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks?
Ref: NIST SP 800-53 SI-2; NIST SP 800-18

11.2.8 Is penetration testing performed on the system?
Ref: NIST SP 800-53 CA-4; NIST SP 800-18

COMMENTS

11.1.1 When this self-assessment list was first created, spyware and adware were not issues. But they have now become serious issues and you should understand the risks and be prepared to deal with them.

Every agency should have some form of antivirus, antispyware, and anti-adware installed on all workstations. The control files should be updated regularly.

11.2.1 This is more a data integrity design issue. There are a number of mechanisms that can be used to check for data integrity. They should be deployed, as required, to meet management's goal for data integrity.

11.2.2 The difficulty is detecting the inappropriate or unusual activity. Assuming the activity can be detected in your system, personnel need to be authorized to look into the problem and resolve it.

11.2.3 Password policy concerning the structure of the password should be automatically enforced when a password is first entered or changed.

11.2.4 This is a risk issue that management needs to approve. If management agrees, then programs and/or procedures need to be developed to look for and find evidence of data tampering, errors, and omissions.

11.2.5 Intrusion detection is a complex topic. If intrusion detection system (IDS) tools are installed at your agency, they should be as automated as possible. An alternative would be to outsource the IDS function to a third party. These companies are much more efficient in monitoring and detecting intrusions into your network.

11.2.6 The IDS function should be done by professionals and they should supply the reports. Few agencies have the technical depth to provide the monitoring level required to be effective in this arena. The reports should be reviewed and handled quickly.

11.2.7 The decision to monitor system logs in real time is related to the criticality of the application. Real-time monitoring takes resources and should be a cost-effective use of agency funds.

11.2.8 The issue involved here is the level of risk that management is willing to accept. Penetration testing takes time and money. If management is willing to forego the information that could be obtained by a pen-test, then that is its decision.

12. **Documentation**
Ref: OMB Circular A-130, III

ASSESSMENT QUESTIONS

12.1. Critical Element: Is there sufficient documentation that explains how software/hardware is to be used?
Ref: None

12.1.1 Is there vendor-supplied documentation of purchased software?
Ref: NIST SP 800-53 SA-5; NIST SP 800-18

12.1.2 Is there vendor-supplied documentation of purchased hardware?
Ref: NIST SP 800-53 SA-5; NIST SP 800-18

12.1.3 Is there application documentation for in-house applications?
Ref: NIST SP 800-53 SA-5; NIST SP 800-18

12.1.4 Are there network diagrams and documentation on setups of routers and switches?
Ref: NIST SP 800-53 AC-8, CM-2; NIST SP 800-18

12.1.5 Are there software and hardware testing procedures and results?
Ref: NIST SP 800-53 SA-11; NIST SP 800-18

12.1.6 Are there user manuals for all software and hardware in use on the systems?
Ref NIST SP 800-53 SA-5; NIST SP 800-18

12.1.7 Are there emergency procedures?
Ref: NIST SP 800-53 CP-2; NIST SP 800-18

12.1.8 Are there backup procedures?
Ref: NIST SP 800-53 CP-9; NIST SP 800-18

12.2. Critical Element: Are there formal, documented security and operational procedures?
Ref: None

12.2.1 Is there a system security plan?
Ref: NIST SP 800-53 PL-2; OMB Circular A-130, III; FISCAM SP-2.1; NIST SP 800-18

12.2.2 Is there a contingency plan?
Ref: NIST SP 800-53 CP-2; NIST SP 800-18

12.2.3 Are there written agreements regarding how data are shared between interconnected systems?
Ref: NIST SP 800-53 CA-3, SA-9; OMB Circular A-130, III; NIST SP 800-18

12.2.4 Are there risk-assessment reports?
Ref: NIST SP 800-53 RA-3; NIST SP 800-18

12.3. Critical Element: Are there formal service-level agreements?
Ref: None

12.3.1 Are formal service-level agreements in place for all outside agencies' users?
Ref: None

COMMENTS

12.1 The question is reasonably simple. Could a person, using the available documentation, access and/or run the system? While the development of documentation specifications occurred prior to this question, this question is simply asking if the documentation effort was successful.

12.1.1 Most vendors have PDF versions of their documentation available. The issue is generally maintaining copies of older versions of the documentation. Not all vendors keep older documentation available online.

12.1.2 Hardware documentation is generally available via PDF downloads from the Internet. Each agency should consider a common library for systems documentation.

12.1.3 The documentation for in-house applications should be created and updated not only for the users of the system, but also for contingency recovery planning.

12.1.4 You should determine if this documentation exists. This information may indicate that your system is exposed to outside risk. This question is also important for contingency planning activities or determining if there is outside access to a system or server.

12.1.5 Your agency should develop testing plans for large hardware acquisitions.

A major problem to be aware of is something called "level creep." Level creep occurs in chip manufacturing. Changes or minor revisions are often introduced in the chip production line with minimal notification to end users. If you obtain a test unit for evaluation, be sure that truly identical units can be purchased when you have successfully completed your testing program.

This can be a major problem for software distribution. The software drivers for one level of chips may not work with later revised chips. This problem would force you to maintain two or more versions of your software distribution prototype.

12.1.6 User manuals should be available and cover all aspects of each job function.

12.1.7 The previous contingency section dealt with the creation of the emergency procedures. This question is asking if the procedures are stand-alone and can be effectively used by themselves. Again, this is addressing the quality of the result, not necessarily its existence.

12.1.8 Do written backup procedures exist? They are normally developed and refined as part of the contingency recovery process.

12.2.1 This question deals with the effectiveness of the documentation. Is the documentation complete, is it readable, and has it been effectively distributed?

12.2.2 Contingency planning is part of business resumption planning. Each agency should have a business continuity plan in place.

12.2.3 Data that are either received from or sent to other systems need to be documented. In addition, if the ownership of these other systems lies outside of your agency, then you should have written agreements with the system owners concerning the data sharing.

12.2.4 Risk-assessment reports should have been generated through the self-assessment process. These reports are important because they form the foundation for all risk analysis and subsequent security controls.

13. **Security Awareness, Training, and Education**
Ref: NIST SP 800-53 AT-1; OMB Circular A-130, III

ASSESSMENT QUESTIONS

13.1. Critical Element: Have employees received adequate training to fulfill their security responsibilities?
Ref: None

13.1.1 Have employees received a copy of the rules of behavior?
Ref: NIST SP 800-53 PL-4; NIST SP 800-18

13.1.2 Are employee training and professional development documented and monitored?
Ref: NIST SP 800-53 AT-4; FISCAM SP-42

13.1.3 Is there periodic or annual refresher training?
Ref: NIST SP 800-53 AT-3; OMB Circular A-130, III

13.1.4 Are methods used to make employees aware of security, i.e., posters, booklets?
Ref: NIST SP 800-53 AT-2; NIST SP 800-18

13.1.5 Have employees received a copy of, or do they have easy access to, agency security procedures and policies?
Ref: NIST SP 800-53 AT-2, AT-3; NIST SP 800-18

COMMENTS

13.1 Training is critical to creating a secure computing environment.

13.1.1 The rules of behavior are essentially an application of the organization's security policies.

13.1.2 The issue is employee efficiency. Tracking employee training and professional development permits supervisors to keep their teams up-to-date in new technologies.

13.1.3 Annual refresher training usually deals with critical skills that need to be exercised perfectly on the job.

13.1.4 Security awareness programs are useful in keeping employees focused on security.

13.1.5 Unless there is a reason not to, security policies, procedures, and plans should be available to all employees.

14. **Incident Response Capability**
Ref: NIST SP 800-53 CA-1; OMB Circular A-130, III; FISCAM SP-5; NIST SP 800-18

ASSESSMENT QUESTIONS

14.1. Critical Element: Is there a capability to provide help to users when a security incident occurs in the system?
Ref: None

14.1.1 Is a formal incident response capability available?
Ref: NIST SP 800-53 IR-4, IR-7, SI-5; FISCAM SP-3.4; NIST SP 800-18

14.1.2 Is there a process for reporting incidents within the agency?
Ref: NIST SP 800-53 IR-4, IR-6, SI-5; FISCAM SP-3.4; NIST SP 800-18

14.1.3 Are incidents monitored and tracked until resolved?
Ref: NIST SP 800-53 IR-5, IR-6; NIST SP 800-18

14.1.4 Are personnel trained to recognize and handle incidents?
Ref: NIST SP 800-53 IR-2; FISCAM SP-3.4; NIST SP 800-18

14.1.5 Are alerts/advisories received and responded to?
Ref: NIST SP 800-53 SI-5; NIST SP 800-18

14.1.6 Is there a process to modify incident-handling procedures and control techniques after an incident occurs?
Ref: NIST SP 800-53 IR-4; NIST SP 800-18

14.2. Critical Element: Is incident-related information shared with appropriate organizations?
Ref: None

14.2.1 Is incident information and common vulnerabilities or threats shared with owners of interconnected systems?
Ref: NIST SP 800-53 IR-6, RA-5; OMB A-130, III; NIST SP 800-18

14.2.2 Is incident information shared with US-CERT concerning incidents and common vulnerabilities and threats?
Ref: NIST SP 800-53 IR-6; OMB Circular A-130, III; GISRA

14.2.3 Is incident information reported to the appropriate investigating law enforcement agency when necessary?
Ref: NIST SP 800-53 IR-6; OMB Circular A-130, III; GISRA

COMMENTS

14.1 This section is driven by OMB Circular A-130. It requires federal agencies to develop the capability to deal proactively with viruses, hackers, or software bugs.

14.1.1 If your state, county, or city has mandated a security incident response program, then you should have funding for an incident response group. These persons will probably belong to other groups for their full-time jobs. The group is activated when an incident occurs and has the skills to handle the problems.

14.1.2 As part of an incident response program, your agency should have a procedure for reporting incidents to the incident response team. This may be either directly to one of the team members or through your help desk.

14.1.3 The incident response team should be responsible for tracking and resolving incidents.

14.1.4 The incident response team needs to receive special or technical training to be able to deal efficiently and effectively with security incidents.

14.1.5 Part of the incident response team's charter should cover reports to management. Management should be aware of the incidents and how they were resolved.

14.1.6 Feedback is very important in the incident response process. Your incident response team should have a process in place to review an incident after it is resolved so lessons learned can be used to make the incident response team more effective.

14.2 The ability to share incident information within your larger government structure is a way to drive down overall program costs.

14.2.1 Depending on the written agreements you have with the owners of interconnected systems, you should seek to share this information with them. Your hope is that these owners will take action to reduce their vulnerability and, subsequently, your level of exposed risk.

TECHNICAL

15. Identification and Authentication

ASSESSMENT QUESTIONS

15.1. Critical Element: Are users individually authenticated via passwords, tokens, or other devices?
Ref: None

15.1.1 Is a current list maintained and approved of authorized users and their access?
Ref: NIST SP 800-53 AC-2, AC-3, IA-4; FISCAM AC-2; NIST SP 800-18

15.1.2 Are digital signatures used?
Ref: NIST SP 800-53 AU-10; NIST SP 800-18

15.1.3 Is emergency and temporary access authorized?
Ref: NIST SP 800-53 AC-2; FISCAM AC-2.2

15.1.4 Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access?
Ref: NIST SP 800-53 AC-2; FISCAM AC-3.2

15.1.5 Are passwords changed periodically?
Ref: NIST SP 800-53 IA-5; FISCAM AC-3.2; NIST SP 800-18

15.1.6 Are passwords unique and difficult to guess (e.g., do passwords require alphanumeric, upper/lower case, and special characters)?
Ref: NIST SP 800-53 IA-5; FISCAM AC-3.2; NIST SP 800-18

15.1.7 Are inactive user identifications disabled after a specified period?
Ref: NIST SP 800-53 AC-2, IA-4; FISCAM AC-3.2; NIST SP 800-18

15.1.8 Are passwords not displayed when entered?
Ref: NIST SP 800-53 IA-5; FISCAM AC-3.2; NIST SP 800-18

15.1.9 Are procedures in place for handling lost and compromised passwords?
Ref: NIST SP 800-53 IA-5; FISCAM AC-3.2; NIST SP 800-18

15.1.10 Are passwords distributed securely and users told not to reveal their passwords to anyone (social engineering)?
Ref: NIST SP 800-53 IA-5; NIST SP 800-18

15.1.11 Are passwords transmitted and stored using secure protocols/algorithms?
Ref: NIST SP 800-53 IA-5; FISCAM AC-3.2; NIST SP 800-18

15.1.12 Are vendor-supplied passwords replaced immediately?
Ref: NIST SP 800-53 IA-5; FISCAM AC-3.2; NIST SP 800-18

15.1.13 Is there a limit to the number of invalid access attempts that may occur for a given user?
Ref: NIST SP 800-53 AC-7; FISCAM AC-3.2; NIST SP 800-18

15.2. Critical Element: Are access controls enforcing segregation of duties?
Ref: None

15.2.1 Does the system correlate actions to users?
Ref: NIST SP 800-53 AC-5; OMB Circular A-130, III; FISCAM SD-2.1

15.2.2 Do data owners periodically review access authorizations to determine whether they remain appropriate?
Ref: NIST SP 800-53 AC-2; FISCAM AC-2.1

COMMENTS

15.1 The basic questions are: Do you know who your users are, and how do you know?

15.1.1 How does your agency authorize users into its systems? Does it maintain a list of these persons?

15.1.2 Most agencies do not require digital signatures. This is primarily a federal requirement. However, if you do use digital signatures, you should investigate if your systems conform to the FIPS 186-2 standard.

15.1.3 You should always develop a procedure for emergency access. The emergency procedure should still have as many controls as possible to minimize security exposure. The process needs to be properly authorized by management and logged for tracking access.

15.1.4 Your agency's personnel department should have a procedure to notify system administrators that the status of an employee has changed. This is a very important process to have in place.

15.1.5 The actual frequency of password changes needs to be set by management. The 90-day limit is simply a recommendation developed within the security industry.

15.1.6 Password complexity is a two-edged sword. If they are made too complex, passwords get written down and usually are accessible at a person's workstation. If they are too simple, then the risk of passwords being cracked or guessed increases.

15.1.7 This is one specification that should be part of the system specifications. Security is more easily administered if some actions can be set on automatic. For example, management may specify that if a user does not log onto a system for 3 weeks, his or her account would be disabled. The time is set at 3 weeks to allow for a 2-week vacation period plus some holidays.

15.1.8 Almost all systems today mask the password when entered. Some systems allow the password to be exposed, but generally this feature cannot be set automatically.

15.1.9 Your agency should identify a limited number of people who are given the authority to reset lost or compromised passwords. The system should be designed to log password changes only by these persons.

15.1.10 The secure distribution of passwords is often difficult. Generally, the system should be configured to require that a new password be established when the distributed password is used the first time.

15.1.11 This is more of a systems question. The answer needs to be provided by the product vendor.

15.1.12 The short answer is: They should be. Generally, however, they are not. This is one of the biggest exposures that most systems experience. Hackers have lists of these IDs and passwords on the Internet.

15.1.13 Systems should be configured to only allow so many attempts before locking the account. Other approaches simply extend the time to make the change from milliseconds to 60 seconds or longer.

15.2.1 The simple question is: Does the system associate specific activities with specific users?

15.2.2 The data owner is that agency and/or persons who have the ultimate responsibility for the protection and preservation of the data. A simple question you should ask is: "Who would be upset if certain data were irretrievably lost?" This would generally help to identify the data owner. The data owner may also be set by legislation and/or policy within the agency. Whoever this person is, it is his or her responsibility to verify that only authorized persons gain access to "their" data.

16. **Logical Access Controls**
Ref: NIST SP 800-53 AC-1; OMB Circular A-130, III; FISCAM AC-3.2; NIST SP 800-18

ASSESSMENT QUESTIONS

16.1. Critical Element: Do the logical access controls restrict users to authorized transactions and functions?
Ref: None

16.1.1 Can the security controls detect unauthorized access attempts?
Ref: NIST SP 800-53 AC-3; FISCAM AC-3.2; NIST SP 800-18

16.1.2 Are access control software or other measures in place to prevent a user from having all necessary authority or information access to allow fraudulent activity without collusion?
Ref: NIST SP 800-53 AC-3, AC-5, AC-6; FISCAM AC-3.2; NIST SP 800-18

16.1.3 Is access to security software restricted to security administrators?
Ref: NIST SP 800-53 AC-2, AC-3, AC-6, IA-5; FISCAM AC-3.2

16.1.4 Do workstations disconnect or screen savers lock the system after a specific period of inactivity?
Ref: NIST SP 800-53 AC-11, AC-12; FISCAM AC-3.2; NIST SP 800-18

16.1.5 Are inactive users' accounts monitored and removed when not needed?
Ref: NIST SP 800-53 AC-2; FISCAM AC-3.2; NIST SP 800-18

16.1.6 If encryption is used, what encryption standard is used (is the federal standard considered)?
Ref: NIST SP 800-53 AC-3, IA-7, SC-12, SC-13; NIST SP 800-18

16.1.7 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving?
Ref: NIST SP 800-53 SC-12, SC-13; NIST SP 800-18

16.1.8 Is access restricted to files at the logical view or field?
Ref: NIST SP 800-53 AC-3; FISCAM AC-3.2

16.1.9 Is access monitored to identify apparent security violations and are such events investigated?
Ref: NIST SP 800-53 AC-13; FISCAM AC-3.2

16.2. Critical Element: Are there logical controls over network access?
Ref: None

16.2.1 Has communication software been implemented to restrict access through specific terminals?
Ref: NIST SP 800-53 AC-3; FISCAM AC-3.2

16.2.2 Are insecure protocols (e.g., UDP, FTP) disabled?
Ref: NIST SP 800-53 CM-6, SC-7; PSN Security Assessment Guidelines

16.2.3 Have all vendor-supplied default security parameters been reinitialized to more secure settings?
Ref: NIST SP 800-53 CM-6, IA-5; PSN Security Assessment Guidelines

16.2.4 Are there controls that restrict remote access to the system?
Ref: NIST SP 800-53 AC-17; NIST SP 800-18

16.2.5 Are network activity logs maintained and reviewed?
Ref: NIST SP 800-53 AC-13, AU-6; FISCAM AC-3.2

16.2.6 Does the network connection automatically disconnect at the end of a session?
Ref: NIST SP 800-53 AC-12, SC-10; FISCAM AC-3.2

16.2.7 Are trust relationships among hosts and external entities appropriately restricted?
Ref: NIST SP 800-53 AC-3, IA-3, SC-7, SC-11; PSN Security Assessment Guidelines

16.2.8 Is dial-in access monitored?
Ref: NIST SP 800-53 AC-17; FISCAM AC-3.2

16.2.9 Is access to telecommunications hardware or facilities restricted and monitored?
Ref: NIST SP 800-53 PE-4, SC-7; FISCAM AC-3.2

16.2.10 Are firewalls or secure gateways installed?
Ref: NIST SP 800-53 AC-3, SC-7; NIST SP 800-18

16.2.11 If firewalls are installed, do they comply with firewall policy and rules?
Ref: NIST SP 800-53 AC-3, CM-6, SC-7; FISCAM AC-3.2

16.2.12 Are guest and anonymous accounts authorized and monitored?
Ref: NIST SP 800-53 AC-2, AC-14; PSN Security Assessment Guidelines

16.2.13 Is an approved standardized logon banner displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished?
Ref: NIST SP 800-53 AC-8; FISCAM AC-3.2; NIST SP 800-18

16.2.14 Are sensitive data transmissions encrypted?
Ref: NIST SP 800-53 SC-7, SC-8; FISCAM AC-3.2

16.2.15 Is access to tables defining network options, resources, and operator profiles restricted?
Ref: NIST SP 800-53 AC-3; FISCAM AC-3.2

16.3. Critical Element: If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?
Ref: None

16.3.1 Is the agency's privacy policy posted on the agency web site?
Ref: NIST SP 800-53 AC-8; OMB Circular 99-18

COMMENTS

16.1.1 Security controls should be designed to detect and report unauthorized access attempts.

16.1.2 This is one area that should be researched thoroughly when acquiring a new system.

16.1.3 This needs to be researched before the software is acquired.

16.1.4 Personnel need to be trained to set their screensavers to this mode. If the workstations are part of a domain, this can be done automatically.

16.1.5 The access-control software should have this reporting capability.

16.1.6 Generally, if you use encryption, the software will have been designed by the vendor to meet the federal standards.

16.1.7 Key management is the most important and yet the most difficult aspect of using encryption. You need well-thought-out procedures to handle encryption keys.

16.1.8 A logical view can be thought of as a special window into the data built just for you. The logical view will let you look at only the data that the security administrators

want you to see. If the security is built at the field level, it may be possible for you to access data that are not logically related to your request and data that you are not supposed to view.

16.1.9 Logging security violations is an important aspect of security. As part of your security program, you need to assign people to review these violations and take action, if required.

16.2.1 The ability to restrict access to data based on the location of a physical terminal is a good security feature.

16.2.2 All unnecessary network protocols should be disabled in a sensitive data environment.

16.2.3 Does your system have the ability to change the default security settings? If this feature is available and implemented, it helps avoid the problem of someone inadvertently resetting his or her security parameters and losing his or her secure status.

16.2.4 Unless absolutely required by your charter, remote access to a system should not be permitted.

16.2.5 As with all logging activities, the maintenance and scanning of the logs need to be as automated as possible. Once detected, problems should be researched and resolved.

16.2.6 The default network behavior needs to be understood. Remote access should automatically tear down a session either on timeout or logout.

16.2.7 A trust relationship is established when one system permits a foreign system access to its secured data. Usually, this is independent of the actual user who is using the foreign system to gain access to the data. Trust relationships between systems can increase your security risk exposure.

16.2.8 All remote access to your systems should be logged and monitored.

16.2.9 Physical access to telecommunications equipment is a security exposure. If possible, this access should be logged and monitored.

16.2.10 All connections to the Internet should be through firewalls or secure gateways.

16.2.11 This question assumes that security policies have been developed concerning how firewall policies and rules are created.

For example: On Check Point© Software Technologies firewalls, before you can create a rule, you must define the objects (networks, nodes, etc.) that will be protected. A security policy could be created that tells the network analyst how the Check Point objects should be named. While this may not seem like much, this is important so there is consistency in how objects are named. Overall, this helps reduce the chance for errors when the network analyst creates a firewall rule set.

16.2.12 Unless required by your charter, all guest and anonymous accounts should be disabled.

16.2.13 This should be standard operating procedure within your agency.

16.2.14 They should be.

16.2.15 Network documentation, while necessary, should be considered confidential and limited to people on a need-to-know basis.

16.3 Effective and secure public access to a system is difficult. Generally, the best design separates the public access from the rest of the system. It is simply easier to control security when you totally control what information is sent to the public server.

16.3.1 This is a federal policy. It required that all federal departments and agencies post clear privacy policies on their World Wide Web sites by September 1, 1999. Each policy must clearly and concisely inform visitors to the site what information the agency collects about individuals, why the agency collects it, and how the agency will use it. Privacy policies must be clearly labeled and easily accessed when someone visits a web site.

17. **Audit Trails**
Ref: NIST SP 800-53 AU-1; OMB Circular A-130, III; FISCAM AC-4.1; NIST SP 800-18

ASSESSMENT QUESTIONS

17.1. Critical Element: Is activity involving access to, and modification of, sensitive or critical files logged and monitored, and are possible security violations investigated?
Ref: None

17.1.1 Does the audit trail provide a trace of user actions?
Ref: NIST SP 800-53 AU-2, AU-3, AU-10; NIST SP 800-18

17.1.2 Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased?
Ref: NIST SP 800-53 AU-2, AU-7; NIST SP 800-18

17.1.3 Is access to online audit logs strictly controlled?
Ref: NIST SP 800-53 AU-9; NIST SP 800-18

17.1.4 Are offline storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled?
Ref: NIST SP 800-53 AU-2, AU-9, AU-11; NIST SP 800-18

17.1.5 Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?
Ref: NIST SP 800-53 AU-5, AU-6; NIST SP 800-18

17.1.6 Are audit trails reviewed frequently?
Ref: NIST SP 800-53 AU-13; NIST SP 800-18

17.1.7 Are automated tools used to review audit records in real time or near real time?
Ref: NIST SP 800-53 AU-13, AU-6, AU-7; NIST SP 800-18

17.1.8 Is suspicious activity investigated and appropriate action taken?
Ref: NIST SP 800-53 AU-6; FISCAM AC-4.3

17.1.9 Is keystroke monitoring used? If so, are users notified?
Ref: NIST SP 800-53 AU-8; NIST SP 800-18

COMMENTS

17.1.1 Audit trails are good security tools that should be part of every system.

17.1.2 The design of audit trails should be part of the system development process. They should be designed to provide sufficient data so both normal or abnormal activities can be detected.

17.1.3 Access to audit logs should be very controlled. If possible, they should be captured on a separate system from the one being monitored.

17.1.4 Audit trail logs need to be managed. You may not detect a problem for days or weeks, so it is important to be able to go back and access the appropriate audit log.

17.1.5 Separation of function is a good thing to have within the security area.

17.1.6 Security administration needs to be cost-effective. The review of audit trails should be as automated as possible.

17.1.7 This is a management decision. There are direct costs associated with real-time review and this has to be part of management's overall risk-mitigation strategy.

17.1.8 How are people trained in your agency to report suspicious activity? Whatever method is used, the process should result in the suspicious activity being recorded and reported to management.

17.1.9 Your employees should be told if keystroke monitoring is taking place. This can be a serious morale issue and needs to be handled properly.

STATE AND LOCAL LAW ENFORCEMENT-SPECIFIC IT SECURITY CONTROLS

18. FBI CJIS Compliance

ASSESSMENT QUESTIONS

18.1. Critical Element: Has the agency implemented the minimum level of technical security controls, as outlined in the *CJIS Security Policy*?
Ref: CJIS Security Policy, Version 4

18.1.1 Is CJIS awareness training conducted for new employees within 6 months of appointment or assignment?
Ref: CJIS Security Policy, Version 4, Section 4.3

18.1.2 Has adequate physical security been provided at all times to protect against unauthorized access to or routine viewing of computer devices, access devices, and printed and stored data?
Ref: CJIS Security Policy, Version 4, Sections 4.4.1 and 7.2

18.1.3 Are all visitors to computer centers and/or terminal areas escorted by authorized personnel at all times?
Ref: CJIS Security Policy, Version 4, Section 4.4.3

18.1.4 Is personnel background screening conducted for all personnel who have systems access and computer terminal/records storage areas access?
Ref: CJIS Security Policy, Version 4, Section 4.5.1

18.1.5 Are all media disposed of or reused in accordance with CJIS policy?
Ref: CJIS Security Policy, Version 4, Sections 4.6 and 4.7

18.1.6 Are security incidents identified, investigated, and properly forwarded to the FBI CJIS Information Security Officer (ISO) or to the Computer Security Incident Response Center (CSIRC)?
Ref: CJIS Security Policy, Version 4, Sections 5.3 and 5.4

18.1.7 Are all criminal/noncriminal justice agency and contractor user agreements in place?
Ref: CJIS Security Policy, Version 4, Sections 6.3, 6.4, and 6.6

18.1.8 Is the network configuration documented?
Ref: CJIS Security Policy, Version 4, Section 7.1

18.1.9 Is the identity of users authenticated according to the methods identified in the *CJIS Security Policy* (Virtual Private Network [VPN], biometrics, public key infrastructure [PKI], smart cards, and tokens), as applicable?
Ref: CJIS Security Policy, Version 4, Section 7.3

18.1.10 Are all nonsecure locations that access CJIS from any Internet, wireless, or dial-in connection using the proper level of authentication, as defined in this policy?
Ref: CJIS Security Policy, Version 4, Section 7.3.2

18.1.11 Are all secure locations that access CJIS from any Internet, wireless, or dial-in connection from a remote location using the proper level of authentication, as defined in this policy?
Ref: CJIS Security Policy, Version 4, Sec. 7.3.3

18.1.12 Are all mobile devices that have been removed from a police vehicle incorporating, at a minimum, the use of a unique password or other personal identifier (PIN), and do they meet the advanced authentication requirement, as well?
Ref: CJIS Security Policy, Version 4, Section 7.3.2(b)

18.1.13 Is each person who is authorized to store, process, and/or transmit information on an FBI CJIS system issued a unique identifier?
Ref: CJIS Security Policy, Version 4, Section 7.4.1

18.1.14 Do all passwords for access and authentication on criminal justice information systems comply with CJIS policy?
Ref: CJIS Security Policy, Version 4, Section 7.4.2

18.1.15 Is access control documented and controlled according to the guidance in Appendix C-8 of the CJIS policy?
Ref: CJIS Security Policy, Version 4, Section 7.5

18.1.16 Is Internet and dial-up access to the system controlled according to CJIS policy?
Ref: CJIS Security Policy, Version 4, Sections 7.6 and 7.7

18.1.17 Are data encryption standards, as outlined in the CJIS policy, being met?
Ref: CJIS Security Policy, Version 4, Section 7.8; and FIPS Publication 140-2, "Security Requirements for Cryptographic Models"

18.1.18 Are encryption keys that are used documented and managed by the agency?
Ref: CJIS Security Policy, Version 4, Section 7.8.1; and Appendix C, "Guidelines and Recommendations for Effective Encryption Key Management"

18.1.19 Do all wirelessly attached devices follow the guidelines, as set forth in the CJIS policy?
Ref: CJIS Security Policy, Version 4, Section 7.9; and Appendix C, "Wireless Implementation Guidelines"

18.1.20 Do firewalls used to protect the criminal justice information system meet the guidelines, as outlined in the policy?
Ref: CJIS Security Policy, Version 4, Section 7.10; Appendix B, "Firewall Security and Profile Web Sites"; and Appendix C, "Firewall Definitions"

18.1.21 Is virus protection used on the system?
Ref: CJIS Security Policy, Version 4, Section 7.12

18.1.22 Is criminal history information controlled according to CJIS policy?
Ref: CJIS Security Policy, Version 4, Section 8.0

Appendix B: SEARCH IT Security Worksheets

Appendix B:
SEARCH IT Security Worksheets

SEARCH IT Security Control Development Worksheet

Step 1: **Identified risk**	
Step 2: **Existing controls**	
Step 3: **All other possible controls**	
Step 4: **Control implications**	
Step 5: **Control recommendation**	
Step 6: **Management control decision**	

For instructions on the use of this form, see pages 89–94

SEARCH IT Security Measurement Development Worksheet

Step 1: Identified risk	
Step 2: Management control decision	
Step 3: Existing measures	
Step 4: All other possible measures	
Step 5: Measure implications	
Step 6: Measure recommendation	
Step 7: Measure implementation	

For instructions on the use of this form, see pages 103–107

SEARCH IT Security Policy Development Worksheet

Step1: Identified risk	
Step 2: Management control decision	
Step 3: Measure implementation	
Step 4: Existing policy	
Step 5: Proposed security policy	
Step 6: Policy recommendation	
Comments:	

For instructions on the use of this form, see pages 113–117

Sample Completed IT Security Policy Development Worksheet

The sample responses recorded during the self- and risk-assessment processes, as shown in these graphics, eventually feed into the policy development, as illustrated below.

Assessment Questions	References	Effectiveness Ranking				
		L1 Policy	L2 Procedures	L3 Implemented	L4 Measuring	L5 Feedback/ Reassessment
Personnel Security						
6.2. Critical Element: Is appropriate background screening for assigned positions completed prior to granting access?		NO	NO	PARTIAL	NO	NO

Risk Decisions				
Description of Identified Risk	**Likelihood**	**Severity**	**Risk Tolerance**	**Action Priority**
Personnel who have not undergone thorough background checks have access to information systems.	POSSIBLE	HIGH	ASSUME	1

Step 1: Identified risk	Personnel who have not undergone thorough background checks have access to information systems.
Step 2: Management control decision	Conduct background investigations internally using our own employees. Training will be provided by a neighboring agency that conducts its own investigations. Access to a public information database will be purchased and a policy will be written to ensure that proper background investigations are conducted.
Step 3: Measure implementation	The Personnel Division commander will conduct an annual audit of the background investigations section to ensure that they are complying with the agency policy.
Step 4: Existing policy	No current policy statement exists within the agency for this identified risk.
Step 5: Proposed security policy	This policy will affect all members of the agency. The agency will immediately begin conducting thorough background checks of all employees, civilian or sworn, who have access to agency systems. The checks will be conducted by the background unit, which will be an ancillary responsibility of the Detective Division commander. Any personnel failing to complete the background process will be administratively suspended until such time as the background can be properly completed. Personnel who, through the investigation, do not obtain a satisfactory background check shall be referred to the personnel section for reassignment within the agency.
Step 6: Policy recommendation	• This policy will affect all new employees who have been given a conditional offer of hire. • A thorough background check of the new hire will be completed prior to the person's assignment to a position that will give him or her access to the agency's system. • Under the direction of the commander in charge of Administration, the detectives assigned to background investigations will conduct a thorough background check according to the procedures developed at the direction of the commander and approved by the chief of the agency. • Due to the sensitive nature of the background check process, only the commander in charge of Administration, the agency assistant chief, the agency chief, and the agency counsel will be allowed to review the completed background information. • New hires failing to complete the background process will be promptly notified of their status and referred to the personnel section.
Comments:	

Appendix C: Glossary of Security Terms

Appendix C: Glossary of Security Terms

Acceptable Risk
A risk that management has decided to accept. It is management's responsibility to balance the cost of reducing risks against the cost to the organization if the risk actually occurs.

Access Control
A procedure used to limit access to a resource to authorized entities.

Access Control Policy
A policy that management has approved and which forms the basis for allowing access to physical or logical objects.

Access Control Procedures
Procedures that are created and implemented to permit effective control of access to either physical or logical objects. The control mechanisms may use software, hardware, or people alone, or in any combination.

Advanced Encryption Standard (AES)
A block cipher algorithm that was adopted in 2001 as an encryption standard by the U.S. government.

Authorization
The act of granting access rights to someone or something. The control of authorization is based on the authentication of the object.

Biometrics
A method of authenticating or verifying an individual based on physical or behavioral characteristics.

Certificate Authority (CA)
A system that issues and manages security credentials and/or public keys that are used for message encryption. A CA is part of a Public Key Infrastructure (PKI).

CERT
Computer Emergency Readiness Team. The official name is the CERT Coordination Center. It is located at Carnegie-Mellon University in Pittsburgh, Pennsylvania. CERT provides official worldwide Internet emergency support.

Contingency Plan
A plan that has been created to permit a company or agency to recover from an emergency or other unanticipated event. The plans usually focus on business resumption activities at an alternate location.

Countermeasure
Any activity that reduces a system's vulnerability to a threat.

Computer Security Act (CSA)
The Computer Security Act (Public Law 100-235) was passed by Congress in 1987. In general, "the act declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use."

Demilitarized Zone (DMZ)
A portion of an internal network that is exposed to an external network—usually the Internet. The amount of exposure is highly controlled. The DMZ serves as a "buffer zone" between the internal, trusted network and the outside, nontrusted network.

Federal Information Processing Standards (FIPS)
Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for federal computer systems.

Firewall
A network appliance that is designed to control network traffic according to a set of rules. A firewall is normally connected to two or more different networks. Firewalls are usually installed to control network traffic between the Internet and a user's private network.

Government Information Security Reform Act (GISRA)
A Federal law (Public Law 106-398) that requires federal agencies to perform an internal risk assessment of their electronic information systems and security processes.

Internet Control Message Protocol (ICMP)
A protocol that is used to send control messages between hosts on a network. One example of the use of this protocol is when someone tries to send a packet to a host that has been turned off or is no longer available. In this case, the last active network appliance will detect this problem and will send a "host unreachable" ICMP message back to the originating host.

Intrusion Detection Systems (IDS)
An IDS seeks to detect intrusion or unauthorized entry into a computer system or network by observation of network traffic.

Lifecycle
The phases of a system as it moves from development through design and implementation, and finally to deactivation and disposal.

Local Area Network (LAN)
A network that is local to your organization. Generally, it is rather small and uses private Internet Protocol (IP) addressing.

Mandatory Access Controls (MAC)
MAC requires information to be categorized—such as Secret, Top Secret, or Confidential—and individuals are granted access to a specific category based on their security clearance.

National Institute of Standards and Technology (NIST)
"NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology ... ."

Physical Security Policy
A document that defines which physical items need to be protected and at what level.

Risk
The probability that a loss of data or a specific threat will occur.

Risk Analysis/Risk Assessment
The risk-assessment process begins with a self-assessment of the target system. Once the system is thoroughly investigated and understood, then the system is analyzed for possible security risks. Risk analysis involves determining what risks are present, and which risks need to be mitigated.

Security Goal
A measurable event that relates to successful implementation of security policies.

Security Objectives
There are five security objectives that organizations should try to achieve: integrity, availability, confidentiality, accountability, and assurance.

Security Policy
A statement that defines specific behavior of individuals or systems that, when achieved, result in reaching a specific security goal.

Virtual Private Network (VPN)

A method of logically connecting a remote host over a network so the remote host is unaware that it is remotely connected.

Vulnerability

An identified weakness in a system that is open to exploitation by anyone. Vulnerabilities are identified during the risk-assessment process. Management must decide how each vulnerability needs to be addressed in order to reduce the overall risk of the organization to an acceptable level.

Appendix D: Security Resources

Appendix D: Security Resources

Key NIST Security Publications

While there are dozens of National Institute of Standards and Technology (NIST) publications relating to a variety of security topics, your agency should review the following key manuals prior to starting its security policy development effort. Please note that most of these manuals contain numerous references to other NIST, Federal Information Processing Standards (FIPS), and General Services Administration (GSA) manuals. Following these references will provide you with additional detail, should you require it. These key NIST security publications are available at **http://csrc.nist.gov/publications/nistpubs/**.

Special Publication (SP) 800-12: *An Introduction to Computer Security: The NIST Handbook*, October 1995

This is an excellent introduction to computer security. This manual will be one of your key references as your agency develops computer policies.

SP 800-18: *Guide for Developing Security Plans for Information Technology Systems*, December 1998

This guide provides an excellent introduction to the process of developing security plans for a law enforcement agency.

SP 800-26: *Security Self-Assessment Guide for Information Technology Systems*, November 2001

This manual outlines a methodology for conducting self-assessments of your IT systems. The manual provides sample questionnaires with detailed instructions for their use.

SP 800-30: *Risk Management Guide for Information Technology Systems*, July 2002

This manual provides an excellent overview of the risk-management process. Major sections address risk assessment, risk mitigation, and evaluation and assessment.

SP 800-35: *Guide to Information Technology Security Services*, October 2003

This guide provides a good overview of the roles and responsibilities within an IT organization. It also provides information regarding the security services lifecycle.

SP 800-53: *Recommended Security Controls for Federal Information Systems*, February 2005

This manual contains an overview of the security control process and provides extensive tables of security controls. The manual provides a "cookbook"-like approach

to listing and explaining the different levels of security controls. The controls are organized into three groups: low, moderate, and high.

SP 800-55: *Security Metrics Guide for Information Technology Systems*, July 2003

This guide forms the core of the security metrics process. It is the key component that helps you establish the security control structure that is necessary to monitor and track security mitigation activities in your systems.

Additional NIST Security Publications

NIST manuals cover a wide variety of security subjects. Depending on your security project, there may be a manual that could be of great assistance to your security team. These additional NIST security publications are available at **http://csrc.nist.gov/publications/nistpubs/**.

Key FIPS Security Publications

NIST, under the Information Technology Management Reform Act (Public Law 104-106), develops standards and guidelines for federal computer systems. These standards and guidelines are issued for governmentwide use and are titled *Federal Information Processing Standards*. While there are many FIPS publications, most are too specialized or technical for use in general security policy development activities.

Two current FIPS publications would be helpful to your security program. Check online at **http://csrc.nist.gov/publications/fips/index.html** to see if updates have been made to either manual. The two manuals are:

FIPS 191: *Guideline for the Analysis of Local Area Network Security*, November 1994

Discusses threats and vulnerabilities and considers technical security services and security mechanisms for local area networks.

FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems*, February 2004

Provides security categorization standards for information and information systems. These standards provide a common framework and method for expressing security in a quantitative manner.

Other Federal Documents

Global Justice Information Sharing Initiative Security Working Group, *Applying Security Practices to Justice Information Sharing*, March 2004 (version 2.0)

This publication is available at **http://it.ojp.gov/global**. It is designed to educate justice executives and managers in basic, foundational security practices that they can deploy within their enterprise and between multiple enterprises.

General Services Administration, *A Guide to Planning, Acquiring, and Managing Information Technology Systems*.

This manual is available at **www.acqsolinc.com/pastperfdoc/acqguid.pdf** (the web site of the GSA contractor that developed the guide).

Federal Information System Controls Audit Manual (FISCAM).

This manual describes the computer-related controls that should be considered when assessing the integrity, confidentiality, and availability of computerized data. Available at **http://csrc.nist.gov/sec-cert/**.

Office of Management and Budget (OMB) CIRCULAR NO. A-130

This document establishes policy for managing federal information resources. Available at **www.whitehouse.gov/omb/circulars/a130/a130trans4.html#2**

Other Security Resources of Interest

Carnegie-Mellon University Software Engineering Institute: **www.sei.cmu.edu**

Carnegie-Mellon University: **www.cmu.edu**

Computer Emergency Response Team: **www.cert.org**

Defense Information Systems Agency: **www.disa.mil**

Department of Homeland Security: **www.dhs.gov**

Generally Accepted Information Security Principles Committee: **www.issa.org/gaisp/gaisp.html**

Information Security Forum: **www.securityforum.org**

Information Systems Audit and Control Association: **www.isaca.org**

Information Systems Security Association: **www.issa.org**

International Organization for Standardization: **www.iso.org**

Internet Security Alliance: **www.isalliance.org**

Microsoft Technet–The Security Risk Management Guide: **www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default.mspx**

National Security Agency: **www.nsa.gov**

SANS: Systems Administration, Audit and Network Security Institute: **www.sans.org**

Systems and Network Attack Center (NSA): **www.nsa.gov/snac**

The Center for Internet Security: **www.cisecurity.org**

US-CERT: U.S. Computer Emergency Readiness Team: **www.us-cert.gov**

For More Information:

U.S. Department of Justice
Office of Community Oriented Policing Services
1100 Vermont Avenue, N.W.
Washington, DC 20530

To obtain details on COPS programs, call the
COPS Office Response Center at 800.421.6770

Visit COPS Online at **www.cops.usdoj.gov**

e01071252