NIST Special Publication 800-39

Managing Risk from Information Systems

An Organizational Perspective

Ron Ross
Stu Katzke
Arnold Johnson
Marianne Swanson
Gary Stoneburner

I N F O R M A T I O N S E C U R I T Y

SECOND PUBLIC DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

April 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
James M. Turner, Acting Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than classified national security information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

NIST Special Publication 800-39, 67 pages

(April 2008)

The public comment period for this document is April 7-30, 2008.

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic mail: sec-cert@nist.gov

Compliance with NIST Standards and Guidelines

NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.

- Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.
- Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB FISMA Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.[1]
- Other security-related publications, including NIST interagency and internal reports (NISTIRs) and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when so specified by OMB.

Schedule for Compliance with NIST Standards and Guidelines

- For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST.[2]
- For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines immediately upon deployment of the system.

[1] While agencies are required to follow NIST guidance in accordance with OMB policy, there is flexibility within NIST's guidance in how agencies apply the guidance. Unless otherwise specified by OMB, the 800-series guidance documents published by NIST generally allow agencies some latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. When assessing agency compliance with NIST guidance, auditors, evaluators, and/or assessors should consider the intent of the security concepts and principles articulated within the particular guidance document and how the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

[2] The one-year compliance date for revisions to NIST Special Publications applies only to the new and/or updated material in the publications resulting from the periodic revision process. Agencies are expected to be in compliance with previous versions of NIST Special Publications within one year of the publication date of the previous versions.

Acknowledgements

The authors, Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, and Gary Stoneburner, wish to thank their colleagues who reviewed drafts of this document and contributed to its development. A special note of thanks goes to John Woodward and Harriett Goldman from the MITRE Corporation for their valuable insights on defending against advanced cyber threats and to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support. The authors also gratefully acknowledge and appreciate the many contributions from individuals in the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

DEVELOPING COMMON INFORMATION SECURITY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by the Federal Information Security Management Act (FISMA), NIST consults with other federal agencies and offices as well as the private sector to improve information security, avoid unnecessary and costly duplication of effort, and ensure that NIST standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems. In addition to its comprehensive public review and vetting process, NIST is working with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS) to establish a common foundation for information security across the federal government. The common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their support contractors, more uniform and consistent ways to manage the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation that results from the operation and use of information systems. In another collaboration initiative, NIST is working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001, Information Security Management System (ISMS).

Notes to Reviewers

Special Publication 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, is the flagship document in the series of FISMA-related security standards and guidelines developed by NIST. The second public draft contains substantial improvements in a variety of areas based on the feedback obtained from our customers during the initial public comment period. Some of the more significant changes include:

- Providing specific linkages from the NIST Risk Management Framework to the Federal Enterprise Architecture to help ensure the seamless integration of information security into organizational missions and business processes;
- Providing guidance on applying the steps in the Risk Management Framework in an organization-wide manner, focusing initially on the mission and business processes of organizations, and subsequently on the information systems supporting those processes;
- Extending the recommendations in the Strategic Planning Considerations section to address some of the issues dealing with sophisticated adversaries and advanced cyber attacks;
- Consolidating the *select* and *supplement* steps in the Risk Management Framework to define a single activity for security control selection that covers the selection of the initial security control baseline, application of tailoring guidance, and supplementation of additional controls based on an organizational assessment of risk;
- Distributing the *document* step in the Risk Management Framework across multiple steps to include the development of the security plan, security assessment report, and the plan of action and milestones.
- Extending the concept of *security plans* to include both information systems and the infrastructure supporting those systems to help ensure all security controls needed to protect the mission/business processes of an organization are assigned to responsible parties with accountability for development, implementation, and assessment.

The material in this draft publication benefited from the close collaboration and cooperation with the Office of the Director of National Intelligence and the Department of Defense as part of the ongoing transformation initiative that is fostering convergence on key information security standards and guidelines across the federal government. The unified framework resulting from these activities will provide the Civil, Defense, and Intelligence Communities a standardized approach for achieving information security building on a common foundation of best practices while allowing communities of interest to define unique security requirements as the need arises.

The development of Special Publication 800-39 is the first step in a two-step process to redesign the NIST risk management guidelines. The current NIST recommendation on risk management, Special Publication 800-30, is being revised to focus exclusively on risk assessment as it applies to the various steps in the Risk Management Framework described in Special Publication 800-39. The initial public draft of Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, is projected for publication in July 2008.

Your feedback to us, as always, is important. We appreciate each and every contribution from our reviewers. The very insightful comments from both the public and private sectors continue to help shape our publications and ensure that they are meeting the needs of our customers.

-- RON ROSS
FISMA IMPLEMENTATION PROJECT LEADER

Table of Contents

Prologue

"…Through the process of risk management, leaders must consider risk to US interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations… "

"…For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated in order to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities; and assess, coordinate, and deconflict all cyberspace operations…"

"…Leaders at all levels are accountable for ensuring readiness and security to the same degree as in any other domain…"

-- THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS
OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

CHAPTER ONE

INTRODUCTION

THE NEED FOR MANAGING ORGANIZATIONAL RISK FROM INFORMATION SYSTEMS

Information technology is widely recognized as the engine that drives the U.S. economy, giving industry a competitive advantage in global markets, enabling the federal government to provide better services to its citizens, and facilitating greater productivity as a nation. Organizations[3] in the public and private sectors depend on information technology and the information systems[4] that are developed from that technology to successfully carry out their missions and business functions. Information systems can be very diverse entities ranging from high-end supercomputers to very specialized systems (e.g., industrial/process control systems, telecommunications systems, and environmental control systems). Information systems are subject to serious *threats* that can have adverse effects on organizational operations (including missions, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation by compromising the confidentiality, integrity, or availability of information being processed, stored, or transmitted by those systems. Threats to information systems include environmental disruptions, human errors, and purposeful attacks. Attacks on information systems today are often well-organized, disciplined, aggressive, well-funded, and in a growing number of documented cases, extremely sophisticated. Successful attacks on public and private sector information systems can result in great harm to the national and economic security interests of the United States. Given the significant danger of these attacks, it is imperative that leaders at all levels understand their responsibilities in managing the risks from information systems that support the missions and business functions of organizations.

Risk related to the operation and use of information systems is another component of organizational risk that senior leaders must address as a routine part of their ongoing risk management responsibilities. Organizational risk can include many types of risk (e.g., investment risk, budgetary risk, program management risk, legal liability risk, safety risk, inventory risk, and the risk from information systems). Effective risk management requires recognition that organizations operate in a highly complex and interconnected world using state-of-the-art and legacy information systems—systems that organizations depend upon to accomplish critical missions and to conduct important business. Leaders must recognize that explicit, well-informed management decisions are necessary in order to balance the benefits gained from the use of these information systems with the risk of the same systems being the vehicle through which adversaries cause mission or business failure. Managing risk is not an exact science. It brings together the best collective judgments of the individuals responsible for the strategic planning and day-to-day operations of organizations to provide adequate security[5] and risk mitigation for the information systems supporting the missions and business functions of those organizations.

[3] The term *organization* describes an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements) that is charged with carrying out assigned mission/business processes and that uses information systems in support of those processes.

[4] An information system is a discrete set of information resources (people, processes, and technology) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[5] The Office of Management and Budget (OMB) Circular A-130, Appendix III, describes adequate security as security commensurate with risk. This risk includes both the likelihood and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

The complex, many-to-many relationships among mission/business processes and the information systems supporting those processes require a holistic, organization-wide view for managing risk. The role of information security in managing risk from the operation and use of information systems is also critical to the success of an organization in achieving its strategic goals and objectives. Historically, senior leaders have viewed information security as a technical matter that was independent of organizational risk. This narrow view resulted in inadequate consideration of how risk from information systems, like other organizational risks, affects the likelihood of mission and business success. The risk management concepts in this publication establish a relationship between aggregated risks from information systems and mission/business success. Establishing this type of relationship will:

- Encourage senior leaders (including authorizing officials) to recognize the importance of engaging in the management of risk from the operation and use of information systems;
- Foster an organizational climate where the risk from information systems will automatically be considered within the context of an overarching enterprise architecture and at all phases of the system development life cycle; and
- Help individuals with information system implementation and operational responsibilities to better understand how the information security issues associated with their systems translate into organizational security concerns.

Figure 1 illustrates the concept of managing risk from information systems from an organization-wide perspective.

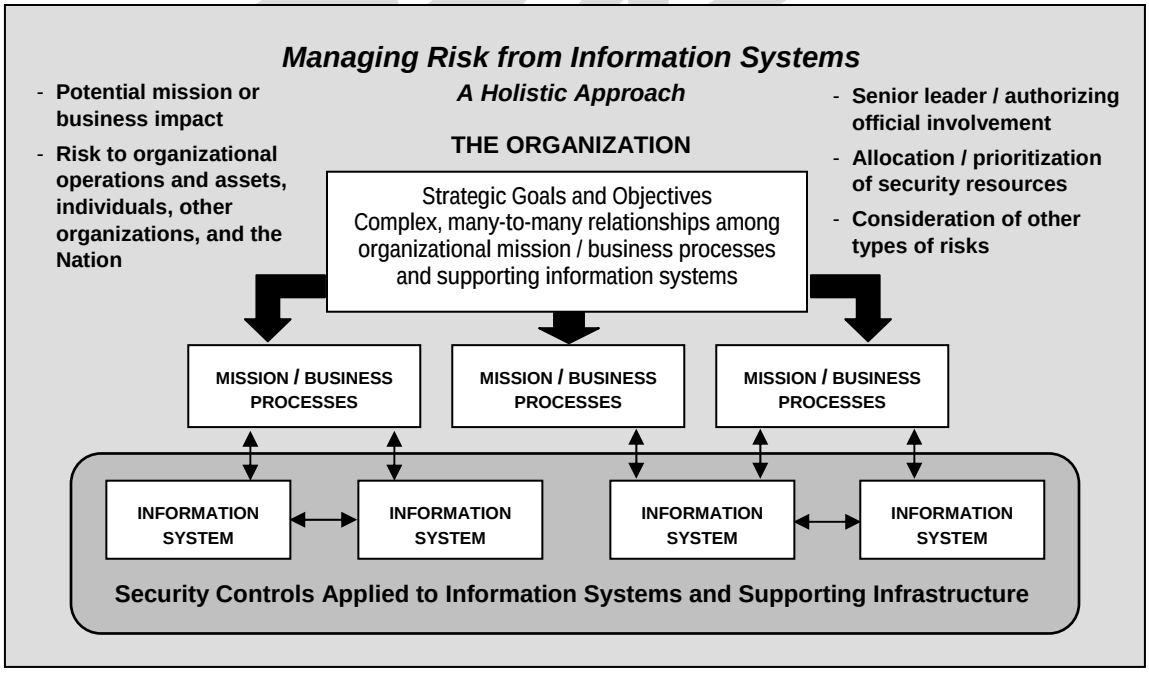

FIGURE 1: ORGANIZATIONAL VIEW OF RISK MANAGEMENT

To achieve success with information system-dependent processes, senior leaders must be committed to making information security a fundamental mission/business requirement. This top-level commitment ensures that sufficient resources are available in the design, development, implementation, operation, and disposition of information systems to provide adequate levels of security for the systems in light of the explicit expectations being placed upon those systems.

Information security is a *strategic* capability and an *enabler* of missions and business functions across the organization. However, information security is but one important factor among many factors that should be considered by senior leaders in carrying out their risk management responsibilities within the organization. Effective management of risk from information systems involves the following key elements:

- Assignment of information security responsibilities to senior leaders/executives within the organization;
- Understanding by senior leaders/executives of the degree of protection or risk mitigation that implemented security controls provide against today's sophisticated and diverse threats;
- Recognition and acceptance by senior leaders/executives of the risks (including potential magnitude of harm) to organizational operations and assets, individuals, other organizations, and the Nation arising from the use of information systems; and
- Accountability by senior leaders/executives for their risk management decisions.

Managing that portion of organizational risk related to information systems begins with an effective information security program. The E-Government Act of 2002 (Public Law 107-347) recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, known as the Federal Information Security Management Act (FISMA), states that effective information security programs include:

- Periodic assessments of risk, including the likelihood and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and address information security throughout the life cycle of each organizational information system;
- Plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization;
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures for continuity of operations for information systems that support the operations and assets of the organization.

In addition to developing and deploying an effective information security program, there is great benefit to be obtained in reducing risk from information systems by building an information technology infrastructure that promotes the use of shared services, common solutions, and information sharing.[6] Applying the principles and concepts used in enterprise architectures (e.g., the methodology employed in the OMB Federal Enterprise Architecture Initiative), provides a disciplined, structured, systems engineering-based approach to achieving consolidation, simplification, and optimization of the information technology infrastructure and the information systems that operate within that infrastructure. Risk reduction can be achieved through the full integration of management processes[7] organization-wide, thereby providing greater degrees of security, privacy, reliability, and cost effectiveness for core missions and business functions being carried out by organizations. This unified and balanced approach gives senior leaders the opportunity to make informed decisions in a dynamic environment on the tradeoffs between fulfilling and improving organizational missions and business processes and managing the many sources of risk that must be considered in their overall risk management responsibilities.

1.1 PURPOSE AND APPLICABILITY

The purpose of NIST Special Publication 800-39 is to provide guidelines for managing risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of information systems. Special Publication 800-39 is the flagship document in the series of FISMA-related publications and provides, through the implementation of a risk management framework, a structured, yet flexible approach for managing that portion of risk resulting from the incorporation of information systems into the mission and business processes of organizations. The risk management concepts described in this publication are intentionally broad-based, with the specific details of assessing risk and employing appropriate risk mitigation strategies provided by supporting NIST security standards and guidelines.[8]

The guidelines provided in this special publication have been broadly developed from a technical perspective to be generally useful across a wide range of organizations employing information systems to implement mission and business processes. The guidelines are directly applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542. The guidelines complement similar guidelines for national security systems and may be used for such systems with the approval of the Director of National Intelligence (DNI), the Secretary of Defense (SECDEF), or the Chairman of the Committee on National Security Systems (CNSS), or their designees. The guidelines are also complementary to the risk management approaches and associated activities defined in the Department of Homeland Security (DHS) National Infrastructure Protection Plan (NIPP) and the supporting Sector Specific Plans (SSPs). State, local, and tribal governments, as well as private sector organizations that compose the critical infrastructure of the United States, are also encouraged to consider the use of these guidelines, as appropriate.

[6] The concept of information sharing continues to be a central construct in how the U.S. Government carries out it critical missions and business functions and transforms those processes to provide greater productivity and value to citizens. For example, information sharing requirements in the counter-terrorism, law enforcement, homeland security, and healthcare space are widely accepted and at the core of mission/business success in those areas. In addition, the information technology infrastructure and information systems operating within that infrastructure play a critical role in supporting continuity of operations and government in the event of a natural or man-made disaster.

[7] A management process is a process for planning and controlling the performance or execution of organizational activities (e.g., programs, projects, tasks, processes). Management processes are often referred to as performance measurement and management systems.

[8] The *Risk Management Framework* described in Chapter Three of this publication provides references to the specific security standards and guidelines needed to effectively implement risk management programs within organizations.

1.2 RELATIONSHIP TO OTHER INFORMATION SECURITY PUBLICATIONS

The risk management concepts and associated *Risk Management Framework (RMF)* described in this publication bring together the supporting security standards and guidelines necessary for managing risk related to information systems. Figure 2 provides an overview of the RMF along with the organization-wide inputs necessary for organizations to effectively apply the framework to the information systems supporting the organization's missions and business processes.

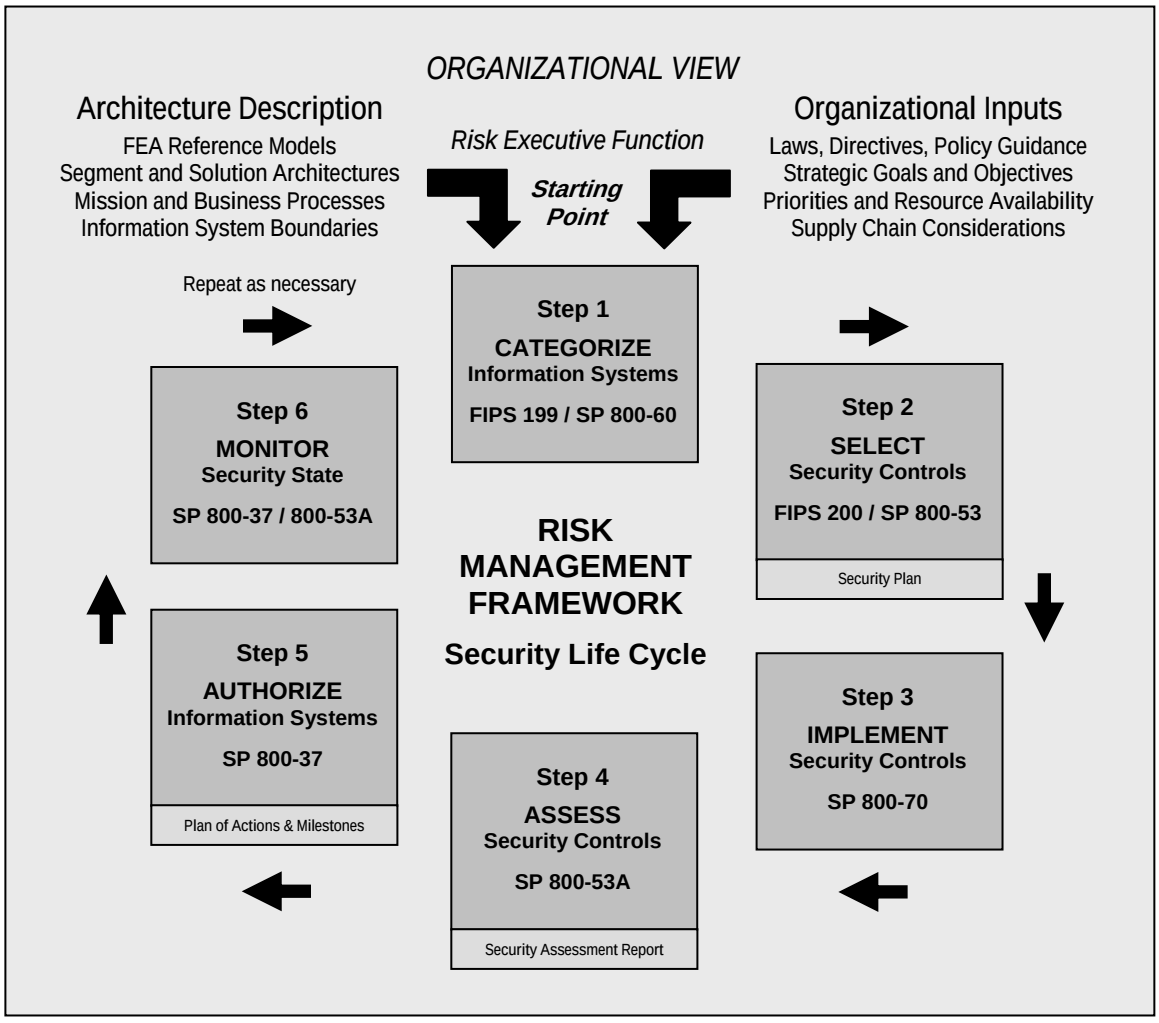

FIGURE 2: RISK MANAGEMENT FRAMEWORK

The following FIPS and NIST Special Publications support the implementation of the RMF:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*;

- NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*;[9]
- NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*;
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*;
- NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*;
- NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*;
- NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*;
- NIST Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*; and
- NIST Special Publication 800-100, *Information Security Handbook, A Guide for Managers*.

ISO/IEC 27001, *Information technology–Security techniques–Information security management systems–Requirements* was published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). There is considerable similarity in the NIST RMF and ISO/IEC 27001. Since NIST's mission includes harmonization of international and national standards where appropriate, NIST intends to pursue convergence to reduce the burden on organizations that must conform to both sets of standards.[10]

1.3 TARGET AUDIENCE

This publication is intended to serve:

- Individuals with mission/business/information ownership responsibilities (e.g., agency heads, authorizing officials,[11] information owners);
- Individuals with information system/security management responsibilities (e.g., chief information officers, senior agency information security officers, security managers);
- Individuals with information system design and development responsibilities (e.g., program managers, enterprise architects, information technology product vendors, system integrators);
- Individuals with information system/security implementation and operational responsibilities (e.g., information system owners, system security officers); and
- Individuals with information system/security assessment and monitoring responsibilities (e.g., auditors, assessors, Inspectors General, evaluators, validators, and certification agents).

[9] NIST Special Publication 800-30 is being revised to focus exclusively on risk assessments with application to the various steps in the Risk Management Framework described in this publication. The initial public draft of Special Publication 800-30, Revision 1, is targeted for release in July 2008.

[10] To promote convergence between FISMA standards (and supporting guidelines) and ISO/IEC 27000-series standards, NIST plans to develop and publish a comprehensive mapping document outlining the similarities and difference among the security requirements and security controls in the respective publications.

[11] Authorizing officials are officials within an organization with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. Authorizing officials are accountable for their authorization decisions.

1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes some of the fundamental concepts associated with managing risk from information systems including: (i) an organization-wide perspective and risk executive function; (ii) risk-based protection strategies; (iii) trustworthiness of information systems; (iv) establishing trust relationships among organizations; (v) global commercial supply chain issues; and (vi) strategic planning considerations for strengthening organizational defenses against sophisticated threats adversaries.
- **Chapter Three** describes the process of applying the NIST Risk Management Framework to organizational mission/business processes and the information systems supporting those processes to include: (i) categorizing information and information systems with regard to mission and business impacts; (ii) selecting and documenting security controls needed for risk mitigation; (iii) implementing security controls in organizational information systems and supporting infrastructure; (iv) assessing security controls to determine effectiveness; (v) authorizing information systems and supporting infrastructure and explicitly accepting mission/business risk; and (vi) monitoring of the security state of information systems and operational environments to determine if security controls continue to be effective and to adequately address changes in the systems and their operational environments.
- **Supporting appendices** provide additional risk management-related information including: (i) references; (ii) terms and definitions; (iii) acronyms; and (iv) integrating risk management concepts into the acquisition and system development life cycle processes.

Since mission/business success depends on information systems, those systems must be dependable. To be dependable in the face of sophisticated 21st century threats, the systems must be adequately protected and used wisely.

CHAPTER TWO

THE FUNDAMENTALS

ORGANIZATIONAL RISK MANAGEMENT AND TRUST RELATIONSHIPS

This chapter describes some of the fundamental issues associated with managing risk from information systems at the organizational level including: (i) an organization-wide perspective and risk executive function; (ii) risk-based protection strategies; (iii) trustworthiness of information systems; (iv) establishing trust relationships among organizations; (v) global commercial supply chain issues; and (vi) strategic planning considerations for strengthening organizational defenses against sophisticated cyber threats.

2.1 ORGANIZATION-WIDE PERSPECTIVE

The complexity and diversity of mission/business processes in modern organizations and the multitude of information systems that are needed to support those processes require a holistic approach to building effective information security programs and managing organizational risks. Developing an organization-wide information security program is not a new concept. However, obtaining a broad-based, organization-wide perspective by authorizing officials and other senior leaders facilitates a more comprehensive view of managing risk from the operation and use of information systems. In today's organizations, a single mission/business process may be supported by multiple information systems. Conversely, there may be multiple mission/business processes supported by a single information system. This many-to-many relationship among mission/business processes and information systems requires an organization-wide approach to managing risk—that is, the risk resulting from the use of information systems in organizational mission/business processes. There are many advantages to employing an organizational approach when developing an information security program.[12] A comprehensive, organization-wide information security program:

- Facilitates prioritization of information security requirements and allocation of information security resources based on risks to the organization's mission/business processes;
- Ensures information security considerations are integrated into the enterprise architecture, the programming, planning, and budgeting cycles for managing information system assets, and the acquisition/system development life cycles;
- Facilitates decisions on risk mitigation activities based on the strategic goals and objectives of the organization and organizational priorities;
- Promotes the development and dissemination of common security policies and procedures;
- Promotes the identification, development, implementation, and assessment of common (infrastructure-based) security controls that support large segments of the organization;
- Promotes the development of organization-wide solutions to information security problems and more consistent and cost-effective information security solutions;
- Facilitates consolidation and streamlining of security solutions across the organization to simplify management, eliminate redundancy of protection, and improve interoperability and communication between dispersed information systems;

[12] OMB Circular A-130 and NIST Special Publication 800-100 provide guidance on organization-wide information security programs.

- Provides insights into systemic information security weaknesses and deficiencies;
- Promotes better communication among personnel responsible for information security;
- Increases the information security knowledge base for key individuals responsible for protecting organizational mission/business processes and the information systems supporting those processes; and
- Provides an essential foundation for building trust among organizations/partners.

To be effective, organization-wide information security programs require strong commitment, direct involvement, and ongoing support from senior leaders. The objective is to institutionalize information security into the day-to-day operations of organizations as a priority and an integral part of how organizations conduct their operations in cyberspace, recognizing that this is essential in order to successfully carry out organizational mission and business processes in actual threat-laden operational environments. Building information security into the culture and infrastructure of organizations requires a carefully coordinated set of activities to ensure that fundamental requirements for information security are addressed within the mainstream management and operational processes employed by organizations (e.g., enterprise architecture development, acquisition and procurement processes, system development life cycle processes, concepts of operation).

2.1.1 Incorporating Information Security into Organizational (Enterprise) Architectures

Architecture is a management practice to maximize the contribution of an organization's resources to achieve mission/business success. Architecture can establish a clear line of sight from investments to measurable performance improvements whether for the entire enterprise or a portion (or segment) of the enterprise.[13] Enterprise architectures provide a common language for discussing information security with regard to mission/business processes and performance goals, enabling better coordination and integration of efforts and investments across organizational or business activity boundaries. For the federal government, the Federal Enterprise Architecture (FEA) defines a collection of interrelated *reference models* including Performance, Business, Service Component, Data, and Technical as well as more detailed *segment* and *solution* architectures that are derived from the top-level *enterprise* architecture.[14] Organizational assets (including programs, processes, information, applications, technology, investments, personnel, and facilities) are mapped to the enterprise-level reference models to create a segment-oriented view of the enterprise. Segments, defined by the enterprise architecture, are individual elements of the enterprise describing core mission areas, and common or shared business services and enterprise services. From an investment perspective, segment architecture drives decisions for a business case or group of business cases supporting a core mission area or common or shared service. The primary stakeholders for segment architectures are mission/business owners and managers. These stakeholders, in consultation with the senior agency information security officer (i.e., chief information security officer) should incorporate *information security requirements* from the FISMA legislation and associated NIST security standards and guidelines into the segment architecture to provide appropriate levels of protection for the organization's mission and business processes defined as part of the overall enterprise architecture.

[13] In NIST Special Publication 800-39, the term enterprise is used synonymously with the term organization.

[14] The Federal Enterprise Architecture is described in a series of documents published by the OMB FEA Program Management Office. Additional information on the FEA reference models and the segment and solution architectures can be found in the FEA Consolidated Reference Model Document and FEA Practice Guidance, respectively.

Solution architecture defines the organization's information technology assets such as applications or information system components used to automate and improve individual organizational mission/business processes. The scope of an organization's solution architecture is typically used to implement all or part of an information system or business solution. The primary stakeholders for solution architectures are information system developers and users. Security requirements defined in an organization's segment architecture are allocated in the form of specific *security controls* to individual information systems (and components composing those systems), through the solution architecture.[15] To summarize, information security considerations can be addressed as an integral part of the enterprise architecture by:

- Developing segment architectures to support clear and concise value propositions linked to organizational missions and strategic goals and objectives;
- Identifying where information security is a critical element in mission/business processes, information, applications, or technologies in use within organization-defined segments;
- Defining information security requirements and risk mitigation measures to provide adequate protection for the mission/business processes, information, applications, or technologies within segments based on the organization's tolerance for risk (i.e., risk/reward ratio);
- Translating information security requirements and risk mitigation measures from the segment architecture into security controls for information systems and system components as part of solution architectures;
- Allocating specific security controls to individual information system components defined within solution architectures; and
- Documenting risk management decisions at all levels of the enterprise architecture.[16]

Due to the increasing number of environments, domains, and platforms that potentially will be crossed in executing mission/business processes supporting organizational partnerships, business relationships, and information sharing activities, the federal government will, over time, transition to a more federated approach to information security. The federated approach will be based on a service-oriented architecture (SOA) that will provide a variety of centrally-managed, assured information security services (e.g., authentication and identity management services; integrity services; availability services; authorization and confidentiality services; auditing and monitoring services; non-repudiation services; security administration and policy management services) to organizations. A government-wide security architecture will promote more cost-effective, interoperable, and consistent security capabilities across domains and environments of operation to help organizations better protect their mission/business processes and manage risk.

The FEA concepts for defining needs-driven, performance-based mission/business processes should be applied by organizations, recognizing that being able to work effectively in a cyberspace environment with sophisticated, high-end threats and highly competent adversaries, is a key need and measure of performance. Specific guidance on how to incorporate information security requirements into enterprise architectures is provided in the FEA Security and Privacy Profile (SPP).

[15] Chapter Three provides additional information on integrating information security into the organization's enterprise architecture and managing the risk associated with the operation and use of information systems.

[16] The activities required to incorporate information security into enterprise architectures are most effectively carried out by integrated project teams that bring together key stakeholders within the organization including, but not limited to, information technology planners, enterprise architects, information security professionals, information system owners, and authorizing officials.

2.1.2 Integrating Information Security into the System Development Life Cycle

In addition to using enterprise architectures to guide information security decisions, information security-related activities should also be fully integrated into the System Development Life Cycle (SDLC) for organizational information systems.[17] Integrating information security requirements into the SDLC is the most efficient and cost-effective method of ensuring that the organization's protection strategy is reflected in the information systems and component information technology products needed to support the mission/business processes of the organization. Information security activities take place at every phase in the SDLC.[18] For example, organizations should address information security requirements during the *initiation* and *development/acquisition* phases of the SDLC (e.g., during requirements definition, conceptual design, system development and demonstration).[19] The requirements define the needed security functionality[20] and the assurance that the required functionality is obtained (see related definition of trustworthiness of information systems in Section 2.3). The *implementation* phase of the SDLC provides an opportunity for organizations to determine the overall effectiveness of the security controls that have been employed within information systems prior to the commencement of actual operations. Once approved for operation, information systems move into the *operations/maintenance* phase of the SDLC where continuous monitoring of the implemented security controls and the operational environment helps ensure that mission/business processes are protected on an ongoing basis. During the *disposition* phase of the SDLC, organizations ensure that critical or sensitive information that may cause adverse impacts, if compromised, is verifiably removed from information systems prior to disposal. Appendix D provides additional information on incorporating the steps in the NIST Risk Management Framework (described in Chapter Three) into the phases of the SDLC.

Many of the activities conducted during the SDLC can support or are complementary to the information security activities that are required to be carried out routinely by organizations. Organizations should maximize the use of relevant information (e.g., testing results, system documentation, and other artifacts) generated during the SDLC to satisfy requirements for similar information needed for information security-related purposes. Reuse of information helps to reduce or eliminate unnecessary documentation, duplication of effort, and cost that may result when security activities are conducted independently of routine SDLC processes. Organizations should ensure that there is close cooperation and collaboration among personnel responsible for the design, development, implementation, operation, and disposition of information systems and the information security professionals advising the senior leadership on appropriate security controls needed to adequately mitigate risk and protect critical mission/business processes. Making information security-related requirements and activities an integral part of the SDLC ensures that senior leaders consider the specific risks to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of information systems and take appropriate actions to carry out the organization's security due diligence.

---

[17] There are five phases in the system development life cycle: (i) system initiation; (ii) system development and acquisition; (iii) system implementation; (iv) system operations and maintenance; and (v) system disposition (disposal).

[18] NIST Special Publications 800-64 and 800-100 provide guidance on integrating information security activities into the specific phases of the SDLC.

[19] Information security requirements are defined in FIPS 200, NIST Special Publication 800-53, and other FISMA-related information security standards and guidelines.

[20] Security functionality is the set of management, operational, and technical security controls within an information system implemented by a combination of people, processes, and technologies. Security controls are described in NIST Special Publication 800-53.

2.1.3 Risk Executive Function

Many approaches to managing risk today focus on individual information systems and the authorization decisions associated with those systems without adequate regard to the complex relationships among the mission/business processes carried out by the organization. Authorizing officials may have narrow or localized perspectives in rendering authorization decisions, perhaps without fully understanding or explicitly accepting the risk incurred from such decisions.[21] Organizations need a comprehensive and holistic approach for addressing risk—an approach that provides greater visibility into and understanding of the integrated operations/business flows of the organization. To address the issues related to managing risk and the associated information security capabilities that must be in place to achieve adequate protection, organizations should include management of organizational risks from information systems as part of an overall *risk executive function*. This function is not limited to addressing risks resulting from information systems, although that is the focus of this document. In general, the risk executive function:

- Provides senior leadership input and oversight for all risk management and information security activities across the organization (e.g., security categorizations, common security control identification) to help ensure consistent risk acceptance decisions;
- Ensures that individual authorization decisions by authorizing officials consider all factors necessary for mission and business success organization-wide;
- Provides an organization-wide forum to consider all sources of risk (including aggregated risk from individual information systems) to organizational operations and assets, individuals, other organizations, and the Nation;
- Ensures that information security considerations are integrated into enterprise architectures, programming/planning/budgeting cycles, and acquisition/system development life cycles;
- Promotes cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility;
- Identifies the overall risk posture based on the aggregated risk from each of the information systems and supporting infrastructures for which the organization is responsible;
- Ensures that information security activities (including the identification of deficiencies and gaps) are coordinated with appropriate organizational entities (e.g., enterprise architects, information technology planners, planning/programming/budgeting officials); and
- Ensures that the shared responsibility for supporting organizational mission/business functions using external providers of information and services receives the needed visibility and is elevated to the appropriate decision-making authorities.

Organizations have flexibility in how the risk executive function is implemented. The risk executive function presumes neither a specific organizational structure nor formal responsibility assigned to any one individual or group within the organization. Whether the head of the organization chooses to retain the risk executive function or to delegate the function to another organizational official (e.g., the Chief Information Officer) or group (e.g., an executive leadership council), the organization head retains ultimate responsibility and accountability for adequately addressing risks to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of information systems.

[21] The original responsibility of authorizing officials published in FIPS 200 and NIST Special Publication 800-37 (authorization with regard to risks to the organization, to its assets, and to individuals) was extended in NIST Special Publication 800-53 (i.e., security control RA-2) to address risks to other organizations and the Nation.

A risk executive function helps ensure that information security considerations for individual information systems, to include the specific authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its mission/business processes. The risk executive function does not make authorization decisions; rather, the intent is to provide *visibility* into the decisions of authorizing officials and a holistic view of risk to the organization beyond that risk associated with the operation and use of individual information systems. While authorizing officials are by definition, senior leaders within the organization with mission, business, operational, and budgetary responsibilities, it is possible or likely that their authorization decisions may affect, either directly or indirectly, other parts of the organization. It is also possible that multiple authorizing officials may be responsible for information systems which collectively support a single organizational mission or business process. A risk executive function facilitates the sharing of security-related and risk-related information among authorizing officials and other senior leaders within the organization to help these officials consider all types of risks that may affect mission and business success and the overall interests of the organization at large.[22]

In addition to the aforementioned internal authorization decisions, there is also increasing reliance on external providers to provide important information system/security services and information that the organization depends on to carry out its mission/business processes. A risk executive function ensures that the shared responsibility for supporting organizational mission/business processes using external providers receives the needed visibility and is elevated to the appropriate decision-making authorities. The additional potential risk assumed by the organization through the use of external providers of services and information can be brought forward by the risk executive function and considered along with other organizational risks. Figure 3 illustrates the relationships among authorizing officials, the information systems that support organizational mission/business processes, and the risk executive function.

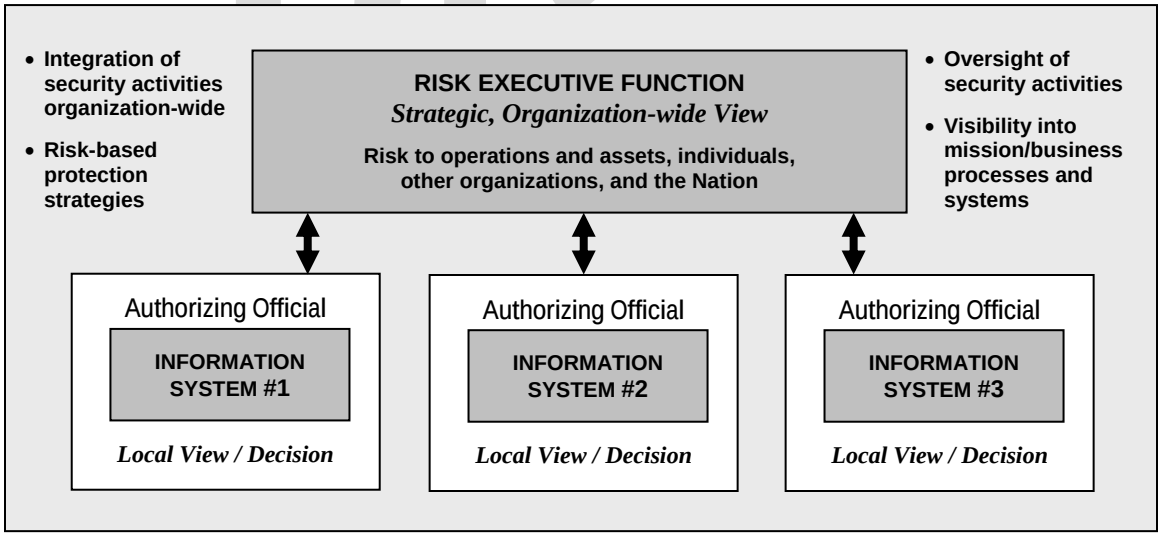

FIGURE 3. RISK EXECUTIVE FUNCTION

[22] For example, the selection of common security controls for the organization may be conducted as an organization-wide activity with the resulting information regarding assignments of responsibility for common control development, implementation, and assessment shared among appropriate organizational personnel.

2.2 RISK-BASED PROTECTION STRATEGIES

To help protect organizations from the adverse effects of ongoing, serious, and increasingly sophisticated *threats* to information systems, organizations should employ a risk-based protection strategy. Risk-based protection strategies are characterized by identifying, understanding, mitigating as appropriate, and explicitly accepting the residual risks associated with the operation and use of information systems. Risk-based protection strategies require authorizing officials to:

- Determine, with input from the risk executive function and senior agency information security officer, the appropriate balance between the risks from and the benefits of using information systems to carry out organizational mission/business processes;
- Approve the selection of security controls for information systems and the supporting infrastructure necessary to achieve this balance;
- Take responsibility for the information security solutions agreed upon and implemented within the information systems supporting the organization's mission/business processes;
- Acknowledge, understand, and explicitly accept the risks to organizational operations and assets, individuals, other organizations, and the Nation that result from the operation and use of information systems;
- Be accountable for the results of information security-related decisions; and
- Monitor the continued acceptability of organizational risk from information systems over time.

Risk-based protection strategies focus on managing risks from information systems based on real-world conditions and making the management decisions explicit—an essential requirement for establishing and maintaining trust among organizations (as further discussed in Section 2.4). A primary consideration of any risk-based protection strategy is to effectively integrate risks from the operation and use of information systems into existing organizational processes dealing with other types of organizational risks (e.g., program and investment risks). This integrated approach moves the management of information system-related risks from an isolated process to an integral part of an overall process for managing the totality of risks organization-wide.[23]

Risk-based protection strategies are necessary to help ensure that organizations are adequately protected against the growing sophistication of threats to information systems. The serious nature of the threats, along with the dynamic environment in which modern organizations operate, demand flexible, scalable, and mobile defenses that can be tailored to rapidly changing conditions including the emergence of new threats, vulnerabilities, and technologies. Risk-based protection strategies support the overall goals and objectives of organizations, can be tightly coupled to enterprise architectures, and can operate effectively within system development life cycles. By empowering senior leaders to make explicit risk management decisions, these strategies also provide the flexibility necessary for the selection and employment of appropriate security controls for organizational information systems to achieve commonsense, cost-effective information security solutions.

[23] NIST Special Publication 800-65 provides guidance on integrating information security into the capital planning and investment control process and incorporating security into organizational programming and budgeting processes.

2.3 TRUSTWORTHINESS OF INFORMATION SYSTEMS

Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system. Trustworthy information systems are systems that are worthy of being trusted to operate within defined levels of *risk* despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Two factors affecting the trustworthiness of an information system include:

- *Security functionality* (i.e., the security-related features or functions employed within an information system or the infrastructure supporting the system); and
- *Security assurance* (i.e., the grounds for confidence that the security functionality, when employed within an information system or its supporting infrastructure, is effective in its application).

Security functionality can be obtained by employing within the information systems and supporting infrastructure of the organization, a combination of management, operational, and technical security controls from NIST Special Publication 800-53.[24] Technical security controls include, for example: physical and logical access control mechanisms; identification and authentication mechanisms; auditing/accountability mechanisms; encryption mechanisms; and system and communications protection mechanisms. Management and operational security controls are typically deployed within the organizational infrastructure that supports the information systems and include, for example: intrusion detection and protection capabilities; contingency planning capabilities; physical and environmental protection capabilities; awareness and training capabilities; and personnel security capabilities.

Security assurance can be obtained by: (i) the actions taken by developers and implementers[25] of security controls with regard to the design, development, implementation, and operation of those controls; and (ii) the actions taken by assessors 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 information systems and supporting infrastructure. Security assurance requirements for developers, implementers, and assessors are addressed in NIST Special Publication 800-53. Developers and implementers can increase the assurance in security controls by employing well-defined security policy models, structured, disciplined, and rigorous hardware and software development techniques, and sound system/security engineering principles. Assurance is also based on the assessment of evidence produced during the initiation, acquisition/development, implementation, and operations/maintenance phases of the SDLC.[26] For example, developmental evidence may include the techniques and methods used to design and develop security functionality. Operational evidence may include flaw reporting and remediation, the results of security incident reporting, and the results of ongoing monitoring of security controls. Independent assessments by qualified assessors may include analyses of the evidence as well as testing, inspections, and audits.[27]

[24] The employment of appropriate security controls for information systems and the supporting infrastructure is guided by the first three steps in the *Risk Management Framework* (i.e., categorization, selection, and implementation).

[25] In this context, a developer/implementer is an individual or group of individuals responsible for the design, development, implementation, or operation of security controls for an information system or supporting infrastructure.

[26] NIST Special Publication 800-64 provides guidance on security considerations in the SDLC.

[27] NIST Special Publication 800-53A provides guidance on assessing security controls in federal information systems.

Understanding trustworthiness and the linkage to the Risk Management Framework, is important to ensuring that information systems are able to provide an appropriate degree of protection against a loss of confidentiality, integrity, or availability. Information systems with greater trustworthiness (i.e., systems having essential security functionality and appropriate levels of assurance) are expected to exhibit a lower rate of latent design and implementation flaws and a higher degree of penetration resistance against a wide range of adversaries with varying degrees of sophistication in the attacks employed. The susceptibility of mission/business processes to threats, the operational environment, and the maximum acceptable level of risk to organizational operations and assets, individuals, other organizations, or the Nation, guide the degree of trustworthiness needed.

2.4 ESTABLISHING TRUST RELATIONSHIPS AMONG ORGANIZATIONS

Organizations are becoming increasingly reliant on information system services[28] and information provided by external providers as well as partnerships established to carry out important mission and business processes. The need for *trust relationships* among organizations arises both from the partnerships established to share information and conduct business and from an organization's use of external providers of information and information system services.[29] In many cases, while external providers bring greater productivity and cost efficiencies to the organization, they may also bring greater risk. This risk must be appropriately managed given the mission and business goals and objectives of the organization.

Relationships among cooperating organizations are established and maintained in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency and intra-agency agreements, lines of business arrangements), licensing agreements, and/or supply chain[30] exchanges (i.e., supply chain collaborations or partnerships). The growing dependence on external service providers and partnerships with domestic and international public and private sector participants presents new challenges for organizations, especially in the area of information security. These challenges include:

- Defining the types of services/information to be provided to the organization or the types of information to be shared/exchanged in partnering arrangements;
- Describing how the services/information are to be protected in accordance with the security requirements of the organization;
- Obtaining the relevant information from external providers and from business partners needed to support and maintain trust (including visibility into risk decisions to understand the participating/cooperating organization's risk management strategies and risk tolerance); and
- Determining if the risk to organizational operations and assets, individuals, other organizations, or the Nation resulting from the use of the services or information or the participation in the partnership, is at an acceptable level.

[28] External information system services are services that are implemented outside of the system's traditional authorization boundary (i.e., services that are used by, but not a part of, the organizational information system).

[29] Trust relationships are scalable and can represent simple (bilateral) relationships between two partners or more complex many-to many relationships among many diverse partners. Trust relationships can be inter-organizational or intra-organizational in nature.

[30] Supply chain refers to the distribution channel of a product from its sourcing to its delivery to the end consumer. Trust relationships for the supply chain are discussed in Section 2.5.

The assurance (i.e., grounds for confidence) that the organizational risk is at an acceptable level depends on the trust relationships established among organizations.[31] The degree of trust that an organization places in external service providers or mission/business partners can vary widely ranging from those who are highly trusted (e.g., business partners in a joint venture that share a common business model and common goals) to those who are less trusted and may represent greater sources of risk (e.g., business partners in one endeavor who are also competitors or adversaries). The specifics of establishing and maintaining trust can differ from organization to organization based on mission/business requirements, the participants involved in the trust relationship, the criticality/sensitivity of the information being shared or the types of services being rendered, and the risk to the organization participating in the relationship. Trust among participating/cooperating partners can be established either formally[32] or informally by:

- Identifying the goals and objectives for the provision of services/information or information sharing;
- Agreeing upon the risk from the operation and use of information systems associated with the provision of services/information or information sharing;
- Agreeing upon the degree of trustworthiness (i.e., the security functionality and assurance) needed for the information systems processing, storing, or transmitting shared information or providing services/information in order to adequately mitigate the identified risk;
- Determining if the information systems providing services/information or involved in information sharing activities are worthy of being trusted; and
- Providing ongoing monitoring and management oversight to ensure that the trust relationship is maintained.[33]

Using the elements of trust described above, trust relationships can be formed authoritatively or through negotiation. In the authoritative approach, an organization with appropriate authority establishes the essential conditions for trust. The authoritative organization initially: (i) identifies the goals and objectives for the provision of services/information or the participation in information sharing activities; (ii) determines the risk associated with the provision of such services/information or the information sharing activities; (iii) establishes the degree of trustworthiness of the information systems providing the services/information or supporting the information sharing operations; and (iv) determines how compliance to the trust requirements is demonstrated and measured. Once established, the trust relationship can continue as long as the information system trustworthiness remains unchanged and the organizational risk remains acceptable.[34]

[31] External providers or mission/business partners can be public or private sector entities, domestic or international.

[32] Trust relationships can be formally established, for example, by documenting the trust element information in contracts, service level agreements, statements of work, memoranda of agreement, or interconnection security agreements.

[33] Maintenance of trust relationships includes an ongoing determination that the information systems of external service providers and participating/cooperating partners continue to operate within agreed-upon levels of risk despite changing threats and technologies, environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation.

[34] The authoritative organization explicitly accepts the risks to be incurred by the use of the services/information from external providers or from the sharing of information among partners and is accountable for the risk management decisions imposed by the organization.

When a single authoritative organization does not exist over the organizations desiring to share information or to use services/information from external providers, or when such an organization might exist but is not willing or able to accept the risks to be incurred or to be accountable for risk management decisions, an alternative approach for developing trust relationships may be in order. The alternative, negotiated approach establishes trust through agreements among potential partners and relies on *negotiating* the provisions for the elements of trust among those partners. In developing negotiated trust relationships, there must be explicit agreement on all elements of trust including the identification of goals and objectives for the provision of services/information or information sharing, the associated risk in conducting those activities, the trustworthiness for information systems involved in the partnership, how trustworthiness is to be demonstrated and measured, and how the trust relationship is to be maintained over time. The objective is to achieve a sufficient *understanding* of the partner's information security programs and information systems in order to establish and maintain an environment conducive to information sharing or to obtaining services/information.

Trust relationships depend on the specific *actions* taken by the participating/cooperating partners to provide appropriate security controls for the information systems supporting the partnerships and the *evidence* needed to demonstrate that the controls have been implemented as intended. This evidence can include, for example, security plans (including risk assessments), security assessment reports, plans of action and milestones, or any other information that the organization can produce to demonstrate the trustworthiness of its information systems.[35] Since the mission and business goals and objectives, security plans, risk mitigation strategies, and risk tolerance of participating/cooperating partners can vary widely based on the inherent flexibility in applying the Risk Management Framework, establishing trust relationships provides the visibility and understanding necessary to have confidence in the information sharing activities or the external services/information provided. Figure 4 illustrates the types of evidence that can be used to support the establishment of trust relationships among partners.

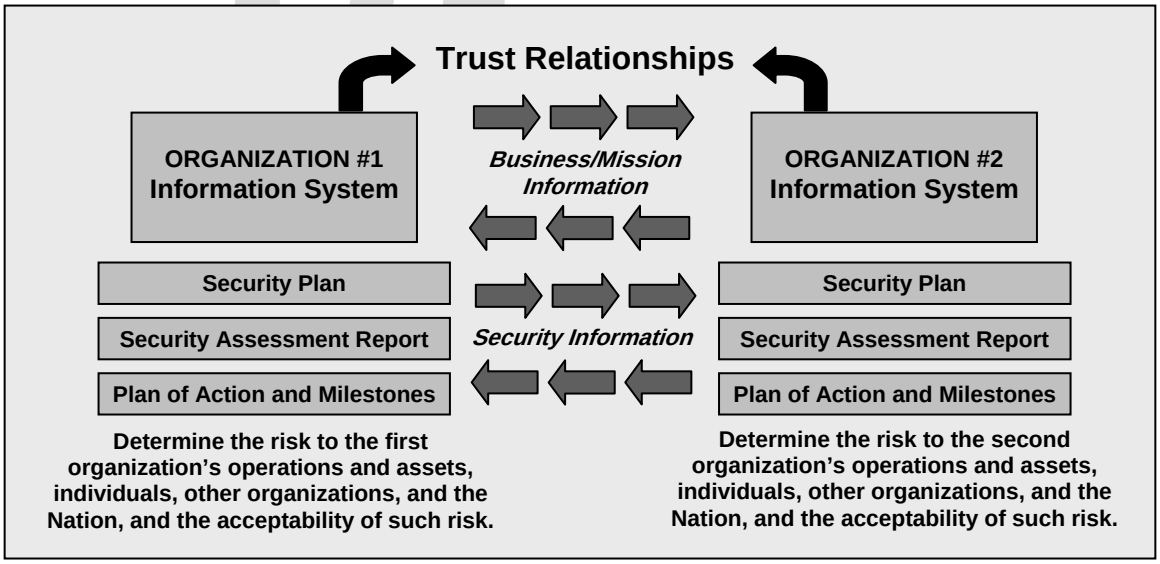

FIGURE 4: BUILDING TRUST RELATIONSHIPS AMONG PARTNERS

[35] Additional information supporting trust relationships can be found in information system Interconnection Security Agreements (ISA) which include technology security services established by participating/cooperating partners. NIST Special Publications 800-35 and 800-47 provide guidance on technology security services and the interconnection of information systems, respectively.

There are also situations in which trust may be *assumed* based on special relationships that have been previously established (e.g., federal agencies cooperating in a long-standing interagency initiative, customer using the services of a known provider with well-established credentials). The elements of trust described above that would normally be used to build a negotiated trust relationship are assumed based on the knowledge of the participants in the partnership and the credentials of the providers. In certain circumstances where there is an overwhelming or compelling need to carry out a critical mission or business function perhaps in a time-sensitive manner (e.g., sharing highly sensitive information to avert a potential terrorist attack that may adversely impact individuals or property), trust relationships may assume a lower priority in deference to achieving immediate mission/business success.

With regard to trust relationships, organizations should also consider whether the participating or cooperating organizations are governed by different laws and regulations and whether they have different parent organizations. For the former, differences in governing laws, regulations, or policies might impact how well organizations are able to trust each other. For the latter, if there is a common parent at the top of the organizational tree (e.g., President of the United States and two cabinet-level departments), then there is always a means of resolving conflict. However, if two organizations attempting to establish a trust relationship have no common parent (e.g., a United States cabinet department and its foreign counterpart), then that may impact trust as well. In the situations described above, risk-based decisions should guide the types of trust relationships that are acceptable to the organizations involved.

Trust in external providers or participating/cooperating partners is directly related to the trustworthiness of the information systems of the providers/partners. In practice, authorizing officials have varying degrees of information about the trustworthiness of such information systems. In some cases, the degree of trust is based on the amount of direct control the authorizing official is able to exert on the prospective provider/partner with regard to the trustworthiness of the information systems involved, including the employment of appropriate security controls necessary for the protection of the information or service and the evidence brought forth as to the effectiveness of those controls. The degree of control, in most cases, is established by the terms and conditions of the contracts, service-level agreements, or interagency agreements with the providers or partners and can range from extensive control (e.g., negotiating specific contracts or agreements that specify detailed information security requirements for the providers/partners) to very limited control (e.g., using contracts or service-level agreements to obtain commodity services such as commercial telecommunications services).[36] In other cases, trust is derived from other factors that convince authorizing officials that the requisite security controls have in fact, been employed and that a credible determination of effectiveness exists.

Trust relationships can be very complicated due to the number of entities participating in the consumer-provider or partner relationship and the type of relationship among the parties. External providers or partners may also outsource services to other external entities, making the trust relationships even more complicated and difficult to manage. Depending on the nature of the services provided or the information shared, it may be unwise for the organization to wholly trust the provider or partner. This less than complete trust in the service provider or partner is due

[36] The provision of services by external providers may result in some services without explicit agreements between the organization and the external entities responsible for providing the services. Whenever explicit agreements are feasible and practical (e.g., through contracts, service-level agreements, interagency agreements), the organization should develop such agreements and require the use of appropriate security controls. When the organization is not in a position to require explicit agreements with external providers, the organization should make explicit any assumptions about the service capabilities with regard to security.

not to any inherent untrustworthiness on the part of the other organization, but to the intrinsic level of risk in using the services or the information. Where a sufficient degree of trust cannot be established in the services, information, providers, or partners, organizations should employ compensating controls or explicitly accept a greater degree of risk.

Ultimately, the responsibility for adequately mitigating risks from the use of external service providers or from the involvement in mission/business partnerships remains with authorizing officials with oversight by the organization's risk executive function. Authorizing officials should ensure that appropriate trust relationships are established with external providers and mission/business partners. For external providers and partners, a trust relationship requires that organizations establish and retain grounds for confidence that each participating provider or partner provides adequate protection for the services rendered or information shared.

Explicit statements of the risk to an organization's operations and assets, individuals, other organizations, and the Nation that are understood and accepted by authorizing officials (reflecting an organization's risk tolerance) are the foundation of risk-based protection and essential for establishing trust relationships among organizations.

2.5 MANAGING RISK FROM SUPPLY CHAINS

A supply chain is a system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.[37] Domestic and international supply chains are becoming increasingly important to the national and economic security interests of the United States because of the growing dependence on products and services produced or maintained in worldwide markets. Uncertainty in the supply chain and the growing sophistication and diversity of international cyber threats increase the potential for a range of adverse effects on organizational operations and assets, individuals, other organizations, and the Nation. Global commercial supply chains provide adversaries with opportunities to manipulate information technology products that are routinely used by public and private sector organizations (e.g., federal agencies, contractors) in the information systems that support U.S. critical infrastructure applications. Malicious activity at any point in the supply chain poses downstream risks to the mission/business processes that are supported by those information systems. These risks include:

- The introduction of exploitable vulnerabilities into information systems when products containing malicious code and other malware are integrated into the systems;
- Inability/difficulty in determining the trustworthiness of information systems that depend upon commercial information technology products to provide many of the security controls necessary to ensure adequate security; and
- Inability/difficulty in determining the trustworthiness of information systems service providers (e.g., installation, operations, and maintenance) that provide many of the security controls necessary to ensure adequate security.

[37] Products and services in the domestic and international supply chain include, for example, hardware, software, and firmware components for information systems, data management services, telecommunications service providers, and Internet service providers.

To mitigate risk from the supply chain, a comprehensive information security strategy should be considered that employs a strategic, organization-wide *defense-in-breadth* approach. A defense-in-breadth approach helps to protect information systems (including the information technology products that compose those systems) throughout the SDLC (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk. In particular, organizations should, whenever possible:

- Know the provenance of the information technology products and services provided by vendors and suppliers;
- Use a diverse set of vendors and suppliers to minimize the adverse effects from particular bad actors in the supply chain;
- Seek transparency in the information technology product design and development processes employed by vendors and suppliers;
- Minimize the time between decisions to purchase information technology products/services and the actual delivery date of the products/services to reduce windows of opportunity for malicious activity by adversaries;
- Use standard configurations of information technology products and systems to reduce the probability of malicious code insertion;
- Protect purchasing information to include the buyer's identity;
- Implement trusted distribution processes for information technology products and services;
- Perform on-site testing of newly acquired information technology products prior to widespread deployment to reduce the probability of unauthorized, covert modifications;
- Use information technology components provided by trusted vendors and suppliers;
- Reduce the insider threat during information system upgrades or when replacing information technology components by using different system administrators at different points in the layered defenses of organizations; and
- Strictly control access to information systems for external maintenance and service providers to reduce the probability for malicious activity.

To facilitate the implementation of supply chain risk mitigation, organizational officials should work closely with acquisition management to incorporate risk mitigation activities into the acquisition process. Coordination among program managers, security officers, and acquisition officials early in the acquisition process will allow the organization to take advantage of the knowledge and tools available within the acquisition community to meet the strategic goals and objectives of the organization, satisfy mission and business requirements, and comply with federal legislation, policies, directives, and regulations. A common understanding of global supply chain risk and associated risk mitigations can leverage skills and experience from both disciplines to expedite the acquisition process and avoid unnecessary delays.

To more effectively integrate global supply chain risk mitigation into the acquisition process, senior leaders should ensure that organizational officials (e.g., program managers, mission owners, information system owners) communicate information security and risk mitigation needs to acquisition officials. Request for Proposals (RFPs) and contracts are developed by acquisition officials based upon needs and requirements specified by program managers, information system

owners, or other organizational officials. Failure to recognize supply chain risks and to specify appropriate risk mitigation measures can result in deficiencies in RFPs and contracts raising opportunities for threat agents to exploit vulnerabilities in the development of information technology products and the delivery of services. To address this problem, organizations should consider using common (boiler-plate) language in RFPs and contracts that would more clearly define the information security and risk mitigation needs of organizations relative to supply chain risk and involve information security officials in the preparation and approval of RFPs. The following requirements for vendors and suppliers can help reduce supply chain risks:

- Requirements for information security within vendor/supplier information systems and networks that are used to acquire or develop information technology products for or provide services to organizations;[38]
- Requirements for information security within the information technology products that are delivered to organizations;
- Requirements for consequence management (e.g., requiring vendors and suppliers to respond to and recover from information security incidents so that the incidents do not adversely affect information technology products and services delivered to organizations);
- Requirements for vendor and supplier penalties for mismanagement resulting in incidents that cause damage to an organization's information, information systems, or networks; and
- Requirements for vendors and suppliers to push information security requirements to subcontractors (in perpetuity) and to require accountability through prime contractors.

While it may be difficult to follow all of the above risk mitigation recommendations for supply chain-related activities, organizations should implement as many of the recommendations as practicable based on organizational assessments of risk and the criticality and sensitivity of the information systems affected (including FIPS 199 impact levels). Organizational officials should also take responsibility and be accountable for the results from risk-based decisions to use information systems, system components, and services subjected to supply chain risks.

To mitigate risk from the global supply chain, a comprehensive information security strategy should be considered that employs a strategic, organization-wide defense-in-breadth approach.

2.6 STRATEGIC PLANNING CONSIDERATIONS

To strengthen an organization's information security defenses in light of the growing intensity and sophistication of cyber threats and to effectively manage risks arising from the operation and use of information systems, senior leaders should consider additional security measures that go beyond the traditional security controls employed by the organization. These additional security measures should be implemented in accordance with an organizational assessment of risk that includes consideration of the criticality/sensitivity of the information systems affected. Strategic

[38] Information security requirements for vendors and suppliers can be specified using, for example: ISO 9001 (quality management practices); ISO 28000 (security management in the supply chain); ISO 27000-series standards, FIPS, NIST Special Publications (network and information system security); ISO 17025 (laboratory testing); and vendor service level agreement requirements for commercial partners and subcontractors.

planning considerations should be an integral part of an overall protection strategy and complement the security controls deployed in organizational information systems and supporting infrastructure.

2.6.1 Consolidation, Simplification, and Optimization of Information Systems

Organizations are acquiring larger and more complex information systems that can become significant targets for adversaries. Information system complexity can increase mission and business risk. Greater complexity can result in increased opportunities for exploitation by threat agents and may also amplify the impact of errors and omissions. Large and complex information systems can represent single points of failure affecting significant segments of the organization or the U.S. critical infrastructure and thereby, potentially increasing risk to the Nation. For example, an electric utility's failure to trim trees over power lines coupled with a computer software error in an energy management system caused the great blackout of 2003 that occurred throughout parts of the Northeastern and Midwestern United States, and Ontario, Canada.[39]

Organizations can manage complexity and the potential for single points of failure by applying the principles and concepts articulated in the Federal Enterprise Architecture (FEA), employing sound information systems engineering methods and techniques, and applying good security practices such as those defined in the NIST security standards and guidelines. The FEA promotes a shared, standards-based infrastructure which, in turn, facilitates consolidation, simplification, and optimization of the information technology infrastructure across the federal government. Through the FEA implementation, complexity can be reduced by introducing simpler, more consolidated information technology solutions that are easier to understand and therefore, easier to protect. Optimization of information technology resources may also help to identify single points of failure as well as opportunities for redundancy to support continuity of operations during local, state, and national emergencies or crises.

In a full FEA implementation, assured information security services can be centralized and made available to organizations government-wide. In addition, the discipline applied in defining the various components of the enterprise architecture (including the derivative segment and solution architectures), provides an opportunity to select and allocate the appropriate security controls for an organization's information systems in a more structured and targeted manner. A well-designed, well-engineered, carefully implemented, and well-managed information technology infrastructure (and the information systems operating within that infrastructure) can greatly reduce risk to organizational operations and assets, individuals, other organizations, and the Nation.

2.6.2 Information Technology Use Restrictions

The use of certain information technologies, including some technologies that are commonly employed in organizational information systems, may introduce significant vulnerabilities into those systems that have the potential to increase risk beyond an acceptable level. In those situations, an alternate strategy is needed. Organizations should carefully assess the risks that would result from the use of such technologies in their information systems. If organizations cannot achieve the needed level of trustworthiness in the information systems necessary to adequately reduce or mitigate the risk brought about by the introduction of those technologies, use restrictions may be needed. Information system use restrictions provide an alternative method to reduce or mitigate risk when, for example: (i) security controls cannot be implemented

[39] Federal Energy Regulatory Commission (FERC) assisted the US Department of Energy in determining the root causes of the blackout that occurred on August 14-15, 2003.

within the technology or resource constraints of the organization; or (ii) security controls lack reasonable expectation of effectiveness against identified threats. Careful consideration should be given to restricting how information technologies that introduce unacceptable risks are used by the organization to carry out its mission/business processes. Restrictions on the use of information systems are sometimes the only prudent or practical course of action to enable mission accomplishment in the face of determined and sophisticated adversaries.[40]

The determination to restrict information technology or information system use should be made by the appropriate organizational officials responsible for managing organizational risk. These officials typically include, for example, mission and business owners, information system owners, authorizing officials, senior agency information security officers, chief information officers, and officials participating in the risk executive function. Examples of use restrictions include: (i) limiting either the information an information system can process, store, or transmit or the manner in which mission/business processes are automated (e.g., restricting the use of hypertext markup language (HTML) technology in email applications); (ii) prohibiting external information system access to critical organizational information by removing selected system components from the network (i.e., air gapping); and (iii) prohibiting critical/sensitive information on information system components to which the public has access.

2.6.3 Application of a Balanced Set of Security Controls

Organizations should employ a balanced set of security controls using a defense-in-depth strategy.[41] Deploying pervasive defenses across the organization includes management, operational, and technical security controls in the following areas: access control; identification and authentication; auditing and accountability; system and communications protection; planning; risk assessment; personnel security; physical and environmental protection; system and information integrity; system and services acquisition; awareness and training; configuration management; contingency planning; incident response; maintenance; media protection; and certification, accreditation, and security assessments. The objective is to provide multiple layers of protection, reducing the number of information system vulnerabilities and increasing the effort adversaries would need to expend to cause harm to organizational operations and assets, individuals, other organizations, or the Nation. While the layered protections of a defense-in-depth strategy are generally helpful, they are of particular importance when using technical controls obtained through the global supply chain. Because of supply chain risks and the potential for malicious activity, there may be less assurance that the technical security controls implemented in information technology products are resilient in the face of serious threats, thus reducing the trustworthiness of the information systems where those products are employed. A reduction in the level of confidence in the technical security controls may result in a greater reliance on management and operational controls that are less vulnerable to supply chain risks.

[40] Use restrictions are similar in concept to business process re-engineering concepts that are discussed in Section 2.6.7. The difference is one of degree where with use restrictions, the mission/business process remains essentially the same and decisions are made concerning what technologies will be allowed within that process and how the technologies will be used. With process re-engineering, potentially more extensive changes to the process are considered.

[41] In the context of this publication, the term *balanced* security controls implies the selection of a broad-based set of safeguards and countermeasures for organizational information systems and supporting infrastructure that includes management, operational, and technical considerations and that are deployed using a defense-in-depth strategy. NIST Special Publication 800-53 provides a complete catalog of security controls for information systems that includes these types of management, operational, and technical controls.

2.6.4 Changing Architectural Configurations

Organizations should consider changing the architectural configurations of organizational information systems on regular basis to prevent adversaries from having predictable targets to exploit. Since adversaries typically require detailed knowledge about the information systems that are the subject of their attacks, changing the system configurations frequently can confuse adversaries and make attacks more difficult to carry out. A degradation in specific knowledge about organizational information systems may cause adversaries to change the types of attacks used and increase the probability that the attacks will fail or have other than the intended effects. Adversaries observing unfamiliar information system configurations may be less likely to be able to cover up their presence within the systems and therefore, be subject to increased likelihood of detection. Changing system configurations frequently can be resource intensive and lead to configuration management and control problems. Organizations can balance configuration management and control issues by using virtualization techniques to deceive adversaries regarding the actual physical configuration of organizational information systems.

2.6.5 Detection and Response to Breaches of Information Systems

Organizations should regularly and methodically check information systems for breaches by adversaries. For extremely critical/sensitive information systems (e.g., high-impact systems), organizations should assume that adversaries may have penetrated their defenses at some point and installed malicious code (e.g., worms, viruses, Trojan horses, rootkits). Once inside the information system, intruders can do great damage to the organization by taking control of the system, compromising the confidentiality and integrity of the information processed, stored, and transmitted by the system, transferring large quantities of information to hostile entities, and affecting the overall availability of the system. These malicious activities can go virtually undetected by the organization unless specific detection and response strategies are employed and diligently followed.

Detection strategies should include both network-based and host-based intrusion detection and prevention programs that use signature, anomaly, and/or stateful analysis techniques.[42] The basic response strategies include containment, eradication, recovery, and application of lessons learned.[43] Information systems suspected of being compromised and under the control of a malicious insider cannot be trusted to carry out any further functions, either diagnostic in nature or mission/business-related. While sophisticated intruders will likely be able to mask their activities and make it very difficult to detect them, ongoing detection activities increase the likelihood of eventually uncovering the adversary activity. Whether there is sufficient increase in the likelihood of detection must be considered in conjunction with other protections (such as those described in Section 2.6.6 on protecting critical system components) as a part of the organization's risk management decisions. Organizations obtaining sufficient evidence that a breach to an information system has occurred should assess the extent and severity of the breach and the realistic alternatives for addressing the compromised system given ongoing mission and/or business requirements, availability of resources to initiate repairs, and the degree of difficulty in bringing the system back to a known secure state.

[42] NIST Special Publication 800-94 provides guidance on intrusion detection and prevention systems.

[43] NIST Special Publication 800-83 provides guidance on malware incident prevention and handling.

2.6.6 Protection for Critical Information System Components

Organizations should make a concerted effort to identify critical mission/business processes and the associated information systems needed to support those processes.[44] Critical information system components should also be identified including any functionality in hardware, software, or firmware providing security capabilities or protection measures necessary for achieving adequate mitigation of risk arising from the use of the components. Once identified, organizations should take extraordinary measures to increase the trustworthiness of the critical information system components. Protection strategies should address all phases of the SDLC to increase the security of the information systems and components and make the systems/components less susceptible to subversion at all points in the supply chain.

Considering the criticality of the aforementioned information systems, organizations should consider restoring and reconstituting those information systems to a known secure state on a periodic basis, assuming that highly sophisticated and well-resourced adversaries may have successfully penetrated and taken control of the systems and remained undetected. This proactive response is very time-consuming and resource-intensive but may be justified under certain circumstances. Organizations should obtain the latest available threat information to determine if there is specific and credible evidence that their information systems are being targeted by specific adversaries and take appropriate mitigation actions.

2.6.7 Business Process Reengineering

Successfully managing the risk resulting from the operation and use of information systems may necessitate reengineering of the processes used to carry out missions and business functions. While such reengineering efforts require significant commitment on the part of the organization, they are in line with the concepts incorporated in the OMB Federal Enterprise Architecture initiative—that is, the potential for risk is greatly influenced by decisions made in the definition of mission/business processes. These decisions include the manner and degree to which the organization relies upon information and exposes itself to potential harm through the use of information systems. By purposefully considering risk and security decisions in the mission or business process definitions, there is the distinct potential for significant risk reduction within acceptable operational constraints. Conversely, failure to do so may well result in processes that impose undue risk that cannot be adequately mitigated with available resources. Therefore, avoiding unacceptable risk requires decisions that are realistic with regard to risk tolerance and the trustworthiness of the information systems available within the organization's resources.

[44] Critical information systems are typically those systems assigned a FIPS 199 high-impact security categorization by an organization. Organizations may on occasion, include selected moderate-impact information systems in the group of systems deemed mission critical or mission essential based on operational needs and/or specific and credible threat information received.

CHAPTER THREE

THE PROCESS

APPLYING THE RISK MANAGEMENT FRAMEWORK TO ORGANIZATIONS AND SYSTEMS

This chapter describes the process of applying the Risk Management Framework to organizational information systems and supporting infrastructure to include: (i) categorizing information and information systems with regard to mission and business impacts (**FIPS 199** and **Special Publication 800-60**); (ii) selecting and documenting security controls needed for risk mitigation (**FIPS 200** and **Special Publication 800-53**); (iii) implementing security controls in organizational information systems and supporting infrastructure (**Special Publication 800-70**); (iv) assessing security controls to determine effectiveness (**Special Publication 800-53A**); (v) authorizing information systems and supporting infrastructure and explicitly accepting mission/business risk(**Special Publication 800-37**); and (vi) monitoring of the security state of information systems and operational environments (**Special Publications 800-53A and 800-37**).

3.1 RISK MANAGEMENT FRAMEWORK

The *Risk Management Framework (RMF)* provides organizations with a structured, yet flexible process for managing risk related to the operation and use of information systems. The RMF is used by organizations to determine the appropriate risk mitigation needed to protect the information systems and infrastructure supporting organizational mission/business processes. The risk executive function ensures that an organization-wide focus is maintained during the implementation of the RMF and provides key inputs (e.g., mission/business goals and objectives, security requirements, policy guidance, resource availability, and priorities) and oversight for the organizational entities executing the framework. Implementation of the RMF can rely on the Federal Enterprise Architecture to generate an organization-wide view of the information types that are integral to the information and data flows within the organization across lines of business. The framework can be applied to both new development and legacy information systems[45] and operates iteratively within the phases of the SDLC (see Appendix D). The RMF represents an information security life cycle that facilitates ongoing monitoring and continuous improvement in the security state and overall risk posture of the organization and the associated information systems processing, storing, and transmitting information necessary for mission and business success. An organization using the RMF for its information systems and supporting infrastructure with inputs and oversight from the risk executive function, obtains comprehensive, cost-effective, risk-based information security solutions that are commensurate with the organization's strategic goals and objectives, the importance and value of its mission and business processes, and its overall tolerance for risk.

The RMF incorporates a well-defined set of information security standards and guidelines for federal agencies and support contractors to facilitate and demonstrate compliance with the FISMA legislation. The plug-and-play nature of the RMF allows other communities of interest (e.g., state, local, and tribal governments, private sector entities) to use the framework voluntarily

[45] Since legacy information systems may already have a full complement of security controls deployed, the RMF can be used to determine whether the controls are necessary and sufficient to protect the organization's mission/business processes that are supported by those systems. Applying each of the steps in the framework to a particular legacy system can confirm that the current security categorization, selection of security controls, and determination of overall control effectiveness either meet or exceed the federal information security standards and guidelines and the security requirements of the organization, or are deficient in some manner and require additional actions by the organization (see Appendix D for additional details on applying the RMF to legacy systems).

either with the NIST security standards and guidelines or with industry-specific standards and guidelines. The RMF consists of six steps that are paramount to effective organization-wide management of risk resulting from the operation and use of information systems. The framework addresses the broader issues of managing risk at the organizational level and can also be used in an iterative manner throughout the phases of the SDLC for individual information systems and supporting infrastructure. Figure 5 illustrates the steps in the RMF, the risk executive function, and the NIST information security standards and guidelines associated with each step.[46]

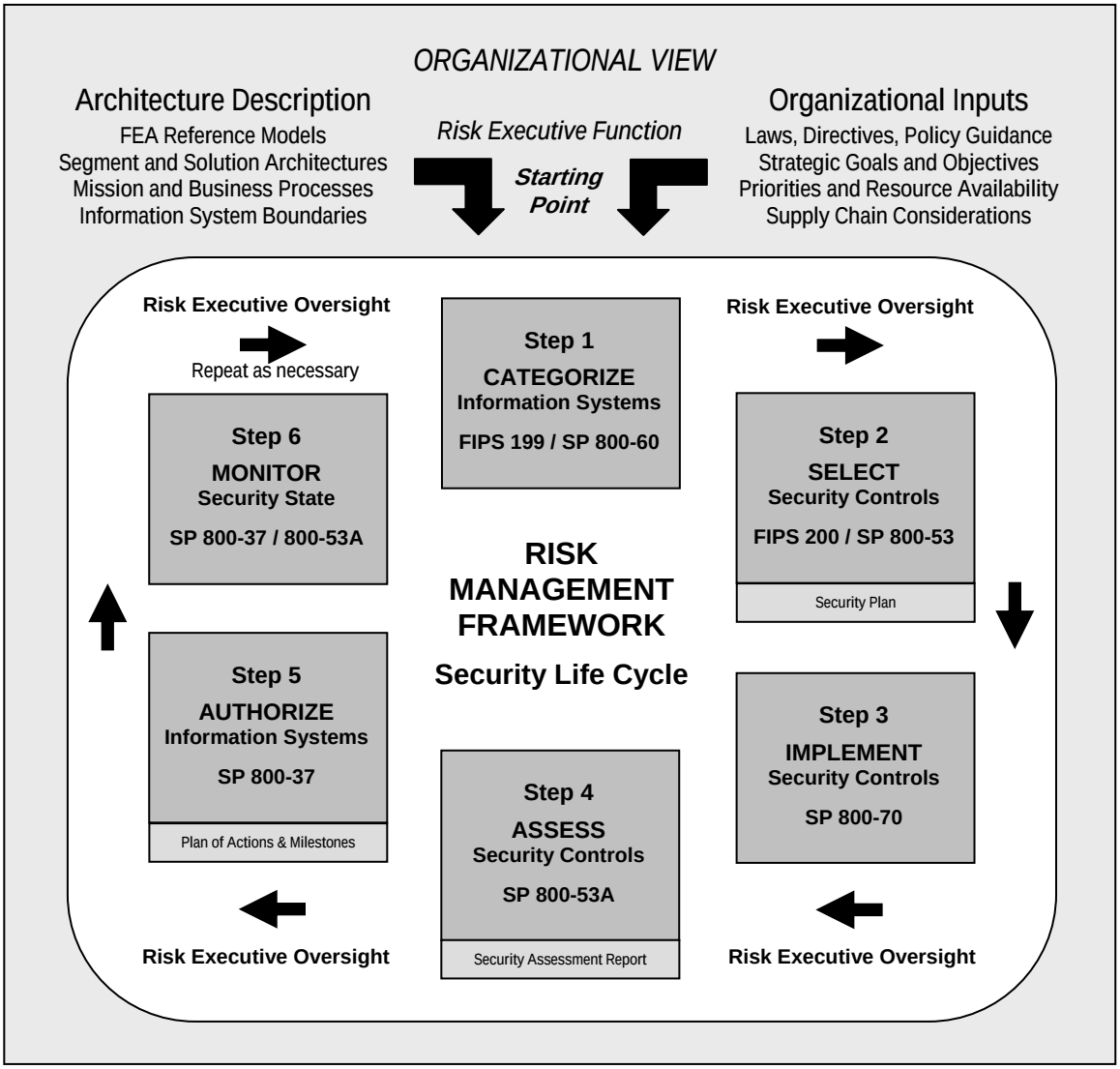

FIGURE 5: RISK MANAGEMENT FRAMEWORK

[46] Original versions of the Risk Management Framework included separate steps for security control *selection* and *supplementation*. The *supplementation* step has been incorporated into the *selection* step to provide a more complete and comprehensive activity for security control selection, and thereby also simplifying the framework. In addition, the *documentation* step has been distributed throughout the RMF and now covers the production of all key documents supporting the management of risk from information systems including security plans, security assessment reports, and plans of action and milestones. It should be noted that the new representation of the RMF does not change any of the previously defined activities occurring during the execution of the framework. Therefore, while the current version of the RMF supersedes all previous versions, organizations may, as part of a transition to the new version of the RMF, continue to reference previous versions in planning and conducting current risk management activities.

3.2 CATEGORIZING INFORMATION AND INFORMATION SYSTEMS

The first step in building an effective organization-wide information security program is to conduct a thorough analysis of the organization's mission and business processes informed by the organization's enterprise architecture, identifying the types of information that will be processed, stored, and transmitted by the information systems supporting those processes. This impact analysis, or *security categorization*, uses the *mission-based* and *management and support* information types from NIST Special Publication 800-60 to assign appropriate FIPS 199 impact levels for the security objectives of confidentiality, integrity, and availability.[47] The security categorization process draws upon the organization's enterprise architecture and thus provides traceability from the FEA reference models through the segment and solution architectures to the individual information systems within the organization.[48] As organizations determine the specific allocation of information resources for the identified mission/business processes, the FIPS 199 security categorizations for the individual information types can be extended to the respective information systems supporting those processes, aggregating the impact levels for the information types to determine overall impact levels for the systems.[49] Information system impact levels are subsequently used to select initial sets of baseline security controls from NIST Special Publication 800-53 (described in Section 3.3). The end result produces an organization-wide view of the criticality/sensitivity of the information systems supporting mission/business processes and potential (worst case) impact to organizational operations and assets, individuals, other organizations, and the Nation[50] should the information systems be compromised.

Organizations should conduct FIPS 199 security categorizations of information types and associated information systems as an organization-wide activity with the participation and involvement of senior leaders and other key officials within the organization (e.g., mission and business owners, information system owners, information owners, enterprise architects, information technology planners, information security managers, information system security officers, chief information officers, senior agency information security officers, authorizing officials, and officials executing or participating in the risk executive function) and others external to the organization when needed and appropriate. Conducting the security categorization process as an organization-wide exercise helps ensure that the process accurately reflects the criticality, sensitivity, and priority of the information and information systems that are supporting organizational mission/business processes and is consistent with the organization's enterprise architecture.

Senior leadership oversight in the security categorization process is essential so that the subsequent steps in the RMF can be carried out in an effective manner. An error in the initial categorization process can result in either an over-specification or under-specification of the security controls for the information systems involved. Over-specification of security controls

[47] NIST Special Publication 800-60 associates *services for citizens* and the *mode of delivery* with mission-based information types and *support delivery of services* and *management of government resources* with management and support information types.

[48] The security categorization process is also integrated into the SDLC with the results affecting the requirements definition, design, and development of organizational information systems (for both new development efforts and upgrades to legacy systems).

[49] Implicit in the security categorization decision is the explicit determination of the information system boundary which establishes the scope of the security accreditation (i.e., authorization to operate).

[50] In accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, NIST Special Publication 800-53 (Security Control RA-2, *Security Categorization*) extends the language in FIPS 199 to include consideration of potential national-level impacts and impacts to other organizations.

means that the organization is expending more effort and resources on information security than is actually necessary and potentially taking resources away from other mission/business areas with greater protection needs. Under-specification of security controls means that selected mission/business processes may be at greater risk due to potentially insufficient protection measures allocated for the information systems supporting those processes. FIPS 199 security categorizations should be reviewed on an ongoing basis to help ensure that mission/business impact assessments reflect the current organizational priorities and operational environments.

- **Key Milestone:** *Has the organization determined the criticality/sensitivity of the information and information systems needed to effectively carry out its mission/business processes and the potential adverse effects on organizational operations and assets, individuals, other organizations, and the Nation if the information and systems are not adequately protected and ultimately compromised?*

3.3 SELECTING SECURITY CONTROLS

After the security categorization process is completed, appropriate security controls can be specified for each information system to implement the organization's protection strategy.[51] The selection of security controls for an organization's mission/business processes and the information systems supporting those processes is a risk mitigation activity that requires the involvement of senior leaders. The security control selection process described in NIST Special Publication 800-53 consists of three activities:

- Selection of *baseline* security controls for each information system from NIST Special Publication 800-53 in accordance with the FIPS 199 impact levels determined during the security categorization process and the minimum security requirements defined in FIPS 200;
- Application of security control *tailoring guidance* for the information systems to allow organizations to adjust the initial security control baselines with respect to specific mission and business processes, organizational requirements, and environments of operation; and
- Supplementation of tailored baseline security controls with *additional controls* based on an assessment of risk and local conditions including specific and credible threat information, organization-specific security requirements, cost-benefit analyses, and special circumstances.

Senior leadership involvement in the security control selection process is necessary in order to provide an organization-wide perspective on: (i) the selection of common security controls and the assignment of responsibility for the development, implementation, and assessment of those controls; (ii) the tailoring of security control baselines (including the application of scoping guidance, use of compensating controls, and control parameterization); and (iii) the selection of supplemental controls. An organization-wide view is essential in the security control selection process to ensure that adequate risk mitigation is achieved for all mission/business processes and the information systems and organizational infrastructure supporting those processes. Senior leadership involvement in the security control selection process is essential to ensure that there is "buy in" to the risk mitigation decisions taken, as the senior leaders are accountable for the resulting risk that will be incurred by the organization.

[51] Security controls should be reflected in the FEA solution architectures and should be traceable to security requirements allocated to mission/business processes defined in the FEA segment architectures. Certain security controls (e.g., common security controls) may be provided by cross federal information security initiatives, supporting infrastructure, other shared security services or solutions, or cross agency, segment, or bureau initiatives.

The following sections describe the key responsibilities for implementing an effective security control selection process including approaches for addressing common security controls, security control tailoring/supplementation, and security control documentation in associated security plans.[52]

3.3.1 Common Security Controls

Security controls are typically characterized as system-specific, common, or hybrid (combination of system-specific and common). System-specific controls are typically under the direct control of individual information system owners and their associated authorizing officials. Common security controls are safeguards and countermeasures that serve the organization as a whole and are typically deployed as part of the infrastructure of the organization.[53] Common controls are determined by the organization and can include, for example, physical and environmental protection controls, personnel security controls, contingency planning controls, or security awareness and training controls.[54] The organization is responsible for:

- Identifying which security controls are to be considered common controls;
- Assigning responsibility for common controls to appropriate organizational entities;
- Developing, implementing, and assessing the effectiveness of common controls; and
- Ensuring that the appropriate information systems organization-wide can inherit the protection measures provided by the common controls.

The identification of common security controls should be an organization-wide activity considering the totality of the organization's mission/business processes and the information systems supporting those processes. For each of the security control baselines defined in Special Publication 800-53 (low, moderate, and high impact), organizations should determine which security controls in each of the baselines are to be designated as common controls. The organization assigns *responsibility* for the development, implementation, and assessment of the selected common controls to specific organizational entities. The ultimate objective of the organization is to have *accountability* for every security control supporting the organization-wide protection strategy.

Since common security controls can provide protection for multiple information systems at different FIPS 199 impact levels, it is important for organizations to consider the most appropriate and cost-effective impact level for the common controls being deployed to best accommodate the information systems using the controls. If the organization chooses to implement common controls at an impact level that falls below the highest impact levels required for individual information systems, then the system owners and authorizing officials for those systems should take appropriate actions to supplement those controls as required for any protection deficits that result at the system level.

[52] Security requirements and the associated security controls employed to satisfy those requirements should also be documented in the organization's segment and solution architectures, thus providing requirements traceability and integration of information security into the enterprise architecture.

[53] While common security control considerations are described in the tailoring guidance section in NIST Special Publication 800-53, the topic is discussed separately in this publication because of the overarching requirement to have common control selection conducted as an organization-wide activity.

[54] Common security controls can also include technical controls such as access control mechanisms, identification and authentication mechanisms, auditing mechanisms, or systems and communications protection mechanisms that are deployed in standard information system configurations at multiple sites.

3.3.2 Security Control Tailoring Guidance

Organizations have the flexibility to *tailor* the security control baselines in accordance with the terms and conditions set forth in NIST Special Publication 800-53. Tailoring guidance facilitates customization of security controls and control baselines to more closely meet the protection needs of organizations. Tailoring activities include: (i) the application of appropriate scoping guidance to the initial security control baselines; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in security controls, where allowed. Tailoring guidance helps to ensure that the security controls selected for protecting the organization's mission/business processes and the information systems/infrastructure supporting those processes are appropriate and in line with the organization-wide protection strategy.

Scoping guidance provides organizations with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines from NIST Special Publication 800-53. Scoping guidance addresses environments of operation, mission and operational considerations, policy and regulatory considerations, physical infrastructure, public access, technology, scalability, common security controls, and control downgrading. The application of scoping guidance can affect the number and types of security controls that are ultimately selected for organizational information systems and supporting infrastructure.

With the diverse nature of information systems, organizations may find it necessary, on occasion, to specify and employ compensating security controls. Compensating security controls are the management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended security controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for mission/business processes and the information systems/infrastructure supporting those processes. Compensating controls may be employed by an organization only under the following conditions:

- The organization selects the compensating controls from NIST Special Publication 800-53 or, if appropriate compensating controls are not available in the security control catalog, the organization develops/adopts suitable compensating controls;
- The organization provides a complete and convincing rationale[55] for how the compensating controls selected provide an equivalent level of protection for the mission/business processes and the information systems/infrastructure supporting those processes and why the related baseline security controls could not be employed; and
- The organization assesses and explicitly accepts the risks associated with employing the compensating controls.

Security controls containing organization-defined parameters (i.e., assignment and/or selection operations) give organizations the flexibility to define selected portions of the controls to support specific organizational requirements or objectives. After the application of the scoping guidance and the selection of compensating security controls, organizations should review the list of security controls for assignment and selection operations and determine appropriate organization-defined values for the identified parameters. Where specified in NIST Special Publication 800-53, minimum and maximum values for organization-defined parameters should be adhered to unless more restrictive values are prescribed by applicable laws, Executive Orders, directives, policies, standards, or regulations or are indicated by an organizational assessment of risk.

[55] Throughout the Risk Management Framework, the meaning for terms such as complete, convincing, and sound when applied to *rationale* is determined with regard to the FIP 199 potential impacts that can occur, with higher potential impact requiring more thorough and rigorous rationale than lower potential impact.

3.3.3 Security Control Supplementation

Organizations also have the flexibility to *supplement* the tailored security control baselines in accordance with the terms and conditions set forth in NIST Special Publication 800-53. Organizations should use Special Publications 800-30 and 800-53 to determine the need for additional security controls for information systems in order to provide adequate protection for organizational mission/business processes.[56] The tailored baselines represent, for particular security categories of information systems (derived from the FIPS 199 impact analyses and modified appropriately for local conditions), the starting points for determining the levels of *security due diligence* to be demonstrated by organizations. The final determination of the security controls necessary to provide adequate security is a function of an organizational assessment of risk and the resulting trustworthiness required for the information systems used in carrying out the organization's mission/business processes to sufficiently mitigate this risk. In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in information systems or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, or regulations. Risk assessments at this stage in the security control selection process provide important inputs to determine the sufficiency of the security controls in the tailored baselines—that is, the security controls needed to adequately protect organizational operations and assets, individuals, other organizations, and the Nation.[57] Figure 6 summarizes the security control selection process applied at the organizational level.

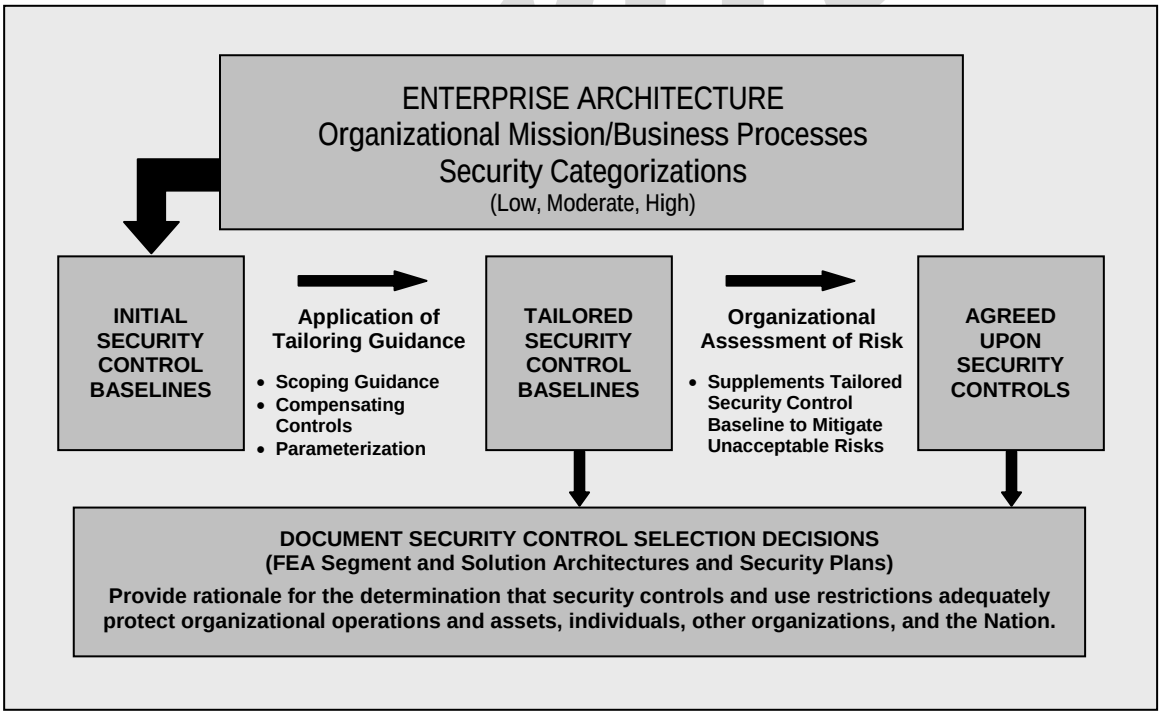

FIGURE 6: SECURITY CONTROL SELECTION PROCESS

[56] Organizations are encouraged to make maximum use of NIST Special Publication 800-53 to supplement security controls in the tailored baselines. To assist in this process, the security control catalog contains numerous controls and control enhancements that are found only in higher-impact baselines or are not included in any of the baselines.

[57] If the security controls that can feasibly be implemented do not result in the desired level of risk mitigation, then the organization must either explicitly accept this situation or reconsider the mission/business process definitions in order to reduce the inherent susceptibility to threats.

Based on strategic goals and objectives and organizational assessments of risk, organizations should provide specific policy guidance on the types of tailoring and supplementation activities that are permissible and appropriate for the information systems supporting the organization. Tailoring and supplementation decisions with respect to the selection of security controls for organizational mission/business processes and for the information systems/infrastructure supporting those processes can potentially impact large segments of the organization and affect the overall security state and risk posture. Therefore, individual tailoring decisions (including decisions on the scoping of security controls, the use of compensating controls, or the assignment of specific security control parameters) and decisions to add supplemental controls should have appropriate visibility and oversight by the senior leadership including the risk executive function within the organization. Tailoring and supplementation decisions should be documented in security plans (see Section 3.3.4 for additional details on documenting security controls for organizational information systems and supporting infrastructure).

Organizations should strive for a high degree of requirements traceability from the organizational mission/business processes identified during the development of the enterprise architecture to the security controls selected for the information systems/infrastructure supporting those processes. Requirements traceability helps to ensure that organizations are providing adequate protection and appropriate risk mitigation for organizational operations and assets, individuals, other organizations (in partnership with or collaborating with the organization), and the Nation. The results of the security control selection process should also be integrated into the SDLC of the individual information systems to help ensure that the required security capabilities are part of the design and development activities associated with organizational information systems (for both new development efforts and upgrades to legacy systems).

- **Key Milestone:** *Has the organization selected an appropriate set of security controls to adequately mitigate the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of its information systems?*

3.3.4 Security Control Documentation

Documenting an organization's protection strategy begins with the enterprise architecture description and the results of the security categorization process for the information and information systems supporting organizational mission/business processes. The security controls allocated to individual information systems and to the supporting infrastructure are documented in the respective *security plans* as described in NIST Special Publication 800-18. Security plans provide an overview of the security requirements for the information systems and supporting infrastructure within an organization and describe the security controls in place or planned for meeting those requirements. The plans also describe the rationale for security categorization, tailoring, and supplementation activities, how individual controls are implemented within specific operational environments, and any use restrictions to be enforced on information systems due to high-risk situations. Security plans provide a description of the *risk mitigations* that are deemed necessary reflecting the information system *trustworthiness* required to help ensure mission and business success. Security plans are important because the plans document the decisions taken during the security control selection process and the rationale for those decisions. Security plans are approved by appropriate authorizing officials within the organization and provide one of the key documents in security accreditation packages that are instrumental in authorization decisions.

Organizations should ensure that security plans are created for all information systems supporting organizational mission/business processes covering all system-specific security controls and the system-specific portions of hybrid controls. Organizations should also ensure that common security controls and the non system-specific (or common) portions of hybrid controls are documented in security plans (or equivalent documents) similar to the plans created for individual information systems.[58] Security plans ensure that designated organizational officials (e.g., human resource officials, physical and personnel security officials, information system owners, chief information officers) are assigned responsibility for the development, implementation, and assessment of the agreed-upon security controls. Security plans are approved by appropriate officials within the organization who are accountable for the results of the risk management decisions documented in the plans. Security plans for individual information systems are approved by the respective authorizing officials for those systems. Security plans (or equivalent documents) for common controls are approved by appropriate organizational officials with oversight authority for those entities within the organization assigned responsibility for the development, implementation, and assessment of those controls.[59]

The organization-wide approach for security control documentation helps to ensure that risks to organizational mission/business processes are adequately mitigated and that all security controls required by the organization, whether system-specific, hybrid, or common, are either contained within some security plan or documented in some other manner by the organization. Complete coverage of security controls in appropriate security plans facilitates more comprehensive information security, promotes increased accountability, provides an effective vehicle to better manage the risks resulting from the operation and use of information systems, and is required to adequately support the security certification of systems as part of the accreditation process.

- **Key Milestone:** *Has the organization documented its protection strategy providing a sound rationale for the risk mitigation decisions associated with the selection of security controls to be implemented by the organization?*

3.4 IMPLEMENTING SECURITY CONTROLS

The implementation of security controls[60] to protect the organization's mission/business processes is tightly coupled to the enterprise architecture and integrated into the SDLC. Security controls that are documented in approved security plans are allocated to specific information systems (i.e., system-specific controls and the system-specific portions of hybrid controls are allocated to particular system components) and to the supporting infrastructure (i.e., common controls and the non system-specific portions of hybrid controls are allocated to the information

[58] Organization may choose to document common security controls in the information system security plans that inherit the protection measures provided by those controls. Organizations using this approach for documenting common controls should ensure that the necessary responsibility for control development, implementation, and assessment is clearly defined, and there is appropriate accountability by the responsible parties, organization-wide.

[59] Common security controls may also be provided by external providers (e.g., services provided by OMB Lines of Business). The external providers may be public or private sector entities (see Section 2.4 for trust relationships with external providers). Organizations should obtain the appropriate assurances that common security controls from external providers have been developed, implemented, and assessed for effectiveness.

[60] In the RMF, *implementation* is used in a broad sense to encompass all of the activities necessary to translate the security controls identified in the security plan into an effective implementation.

system environments of operation including facilities). This process requires a determination by knowledgeable individuals within the organization (e.g., system architects, systems/security engineers, system administrators, physical security experts, personnel specialists) as to which personnel, processes, hardware, software, firmware, facilities, or environmental components within the defined information system boundary are providing specific security functionality (e.g., access control, identification and authentication, auditing and accountability, physical security, personnel security, system and communications protection, incident response, contingency planning). There should be close coordination and collaboration among organizational personnel to ensure that the needed security functions are allocated to the appropriate information systems and supporting infrastructure. For common security controls, the organization should allocate the controls to entities, either internal or external to the organization, responsible for development, implementation, and assessment. For all security controls (management, operational, and technical), the implementation should meet the trustworthiness requirements identified by the organization to provide the desired functionality and assurance (see information system trustworthiness in Section 2.3).[61]

Allocation of security controls to the appropriate components within information systems or to the supporting infrastructure is a critically important activity that can affect the security state and risk posture of the organization. Allocation decisions should be consistent with the enterprise architecture to help ensure that the needed protection measures are provided in the information systems and supporting infrastructure to successfully carry out the organization's mission and business processes. Allocation decisions also affect assessments of security controls, informing assessors of information system and infrastructure components providing specific security capabilities. Information concerning the allocation of security controls and any additional derived requirements for the controls to meet control objectives (e.g., meeting trustworthiness needs), should be documented in security plans for organizational information systems and the supporting infrastructure and approved by the appropriate authorizing officials.

Certain security controls employed within organizational information systems require that security configuration settings be established during implementation. Organizations are required to define mandatory configuration settings for all information technology products that are used within organizational information systems and also to comply with any configuration settings-related legislation, directives, and policy requirements. Mandatory security configuration settings should be enforced across the organization including all information systems that are supporting organizational mission/business processes. NIST Special Publication 800-53 identifies specific security controls where security configuration settings may be required.[62] There are several efforts under way to standardize the security configuration settings for information technology products and to use automated tools to determine if the required settings are in effect and providing the functionality required by the associated security controls.[63]

[61] Trustworthiness is measured by determining whether the security controls selected by the organization and employed within organizational information systems are effective in their application and meet specified functionality, quality, and assurance requirements from NIST Special Publication 800-53. NIST Special Publication 800-53A provides guidance on assessing security controls to determine effectiveness and to provide a measure of information system trustworthiness.

[62] NIST Special Publication 800-70 provides guidance on security configuration settings for information technology products employed in organizational information systems.

[63] To facilitate more cost-effective and comprehensive security with regard to configuration settings for information technology products, NIST has initiated the Information Security Automation Program (ISAP) and Security Content Automation Protocol (SCAP). The primary purpose of the SCAP is to improve the automated application, verification, and reporting of commercial information technology product-specific security configuration settings, thereby reducing vulnerabilities when products are not configured properly.

- **Key Milestone:** *Has the organization effectively implemented its organization-wide protection strategy including the agreed-upon security controls for the information and information systems supporting its mission/business processes?*

3.5 ASSESSING SECURITY CONTROLS

After the organization completes the implementation of the security controls documented in approved security plans for the organizational information systems and supporting infrastructure, the controls should be assessed for effectiveness using the assessment procedures in NIST Special Publication 800-53A. Assessments determine the extent to which the security controls are in fact implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information systems supporting the organization's mission/business processes. Understanding the collective effectiveness of the security controls implemented in the organization's information systems and supporting infrastructure is essential in determining the overall risk to organizational operations and assets, individuals, other organizations, and the Nation. Assessments provide a compilation of the evidence necessary to establish the required assurances that intended security functionality in the security controls selected and implemented by the organization, is present with the requisite level of quality—that is, the information systems and supporting infrastructure possess the required and agreed-upon level of trustworthiness. These assessments, therefore, promote a better understanding of risks from information systems and create more complete, reliable, and trustworthy information to support information-sharing activities, accreditation decisions,[64] and compliance to federal legislation, directives, regulations, and policies.

Organizations should develop an organization-wide strategy for assessing the security controls within organizational information systems and the supporting infrastructure. System-specific security controls and the system-specific portions of hybrid controls implemented within the organization's information systems are assessed with the findings documented in *security assessment reports*. Common security controls and the non system-specific (or common) portions of hybrid controls assigned to responsible entities within the organization (or external to the organization) are also assessed with the findings documented in separate security assessment reports. The information in the security assessment reports provides critical inputs to the organization-wide *plans of action and milestones (POA&M)* documents generated for the individual information systems and the supporting infrastructure.[65] For assessments of common security controls, the evidence regarding control effectiveness should be conveyed to all information system owners and authorizing officials that depend on those controls (through inheritance) for the protection of organizational mission/business processes.

Security control assessments are typically conducted by information system developers, system integrators, certification agents, information system owners, auditors, Inspectors General, and the

[64] NIST Special Publication 800-37 provides guidance on information system accreditation (i.e., authorization) decisions and the acceptance of mission/business risk. The publication also provides guidance on the security certification process, a process that determines the effectiveness of security controls in organizational information systems in support of the accreditation process.

[65] Preliminary POA&Ms are drafted by information system owners upon completion of security control assessments and receipt of security assessment reports. POA&Ms are updated and finalized after the review and approval by authorizing officials.

information security staffs of organizations. These assessors or assessment teams bring together available information about the information system and supporting infrastructure such as the results from product assessments, if available, and conduct additional assessments using a variety of methods and techniques. Assessments are used to develop and compile the evidence needed to determine how effective the security controls employed in information systems and the supporting infrastructure are likely to be in mitigating risks. The results from assessments conducted using assessment procedures from NIST Special Publication 800-53A, contribute to compiling the necessary evidence to determine the effectiveness of security controls in accordance with the assurance requirements in NIST Special Publication 800-53.

3.5.1 Reuse of Assessment Results

Organizations should take advantage of existing assessment information to facilitate more cost-effective assessments. The reuse of assessment results from previously accepted or approved assessments of information systems and supporting infrastructure should be considered in the body of evidence for determining overall security control effectiveness.[66] When considering the reuse of assessment results from previous assessments, organizations should assess the credibility of the evidence obtained, the appropriateness of previous analysis, and the applicability of the evidence to present conditions within the organization.[67] It may be necessary to supplement the previous assessment results under consideration for reuse with additional assessment activities to fully address the organization's assessment objectives. For example, if independent, third-party evaluation of information technology products employed within an organization did not test particular configuration settings used by the organization to help protect its information systems, then the organization may need to supplement the original test results with additional testing to cover the configuration settings for the current information systems environment.

The collective results of security control assessments provide important indicators regarding the overall security state and risk posture of the organization. It is important that assessment results from individual information systems and the supporting infrastructure be reviewed by appropriate organizational officials and made available to interested parties organization-wide. Assessment results from common security controls can potentially affect a significant number of information systems that depend upon the protection capabilities provided by those controls. Deficiencies in common controls can adversely impact the organization's mission/business processes supported by the information systems inheriting the protection capabilities from the common controls. Depending on the nature of the deficiencies, the affected information systems may need to implement compensating controls. Mission/business process owners, information system owners, and authorizing officials of the affected systems need to be aware of the assessment results.

Sharing assessment results provides organizations with an opportunity to discover systemic weaknesses or deficiencies in security controls (e.g., weaknesses or deficiencies in the security controls in one information system may also appear in other information systems) and to provide organization-wide solutions to correct the identified weaknesses and deficiencies. And finally, managing security control assessments at the organizational level facilitates an effective prioritization and allocation of resources in determining the effectiveness of intended controls.

[66] Previously accepted or approved assessments include those assessments of common security controls that are managed by the organization and support multiple information systems.

[67] For example, it should be noted that information technology product assessments are based upon the assumption that the products are properly configured when installed in particular information systems in specific operational environments. If not properly configured, the products may not perform in the manner verified during the assessment.

3.5.2 Additional Security Control Documentation

Additional documentation for the organization-wide protection strategy is developed by the organization after the agreed-upon and approved security controls are implemented and assessed. *Security assessment reports* provide detailed information on the observed deficiencies in security controls (including system-specific, hybrid, and common controls) employed within information systems and the supporting infrastructure and are used to determine the effectiveness of the controls in mitigating risks. *Plans of action and milestones* provide documentation on the organization's strategy to address deficiencies and weaknesses in the deployed security controls (including system-specific, hybrid, and common controls) in a disciplined and structured manner in accordance with organizational priorities and available resources. These documents, along with the security plans and organizational assessments of risk, compose the key artifacts used by authorizing officials and officials participating in the risk executive function, in assessing the security state of the information systems supporting the mission/business processes within the organization.

- **Key Milestone:** *Has the organization assessed its organization-wide protection strategy including a determination of the effectiveness of the security controls employed within its information systems and supporting infrastructure?*

3.6 AUTHORIZING ORGANIZATIONAL INFORMATION SYSTEMS

After the organization completes the assessment of security controls in organizational information systems and supporting infrastructure, the information system authorization process begins following the guidance in NIST Special Publication 800-37. Authorization decisions are based on a determination, understanding, and explicit acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems. The authorization decision is one of the most important decisions made by an authorizing official. With the move toward risk-based protection, authorizing officials, more than ever before, must take ownership of the potential risks to the organization's mission/business processes due to the use of the information systems supporting those processes. Authorizing officials must weigh the near-term operational capability being gained by the mission/business process dependence on information and information systems with the potential loss of operational capability due to the susceptibility to the threats that result from this dependence. While there is significant flexibility in developing the appropriate security controls for managing organizational risk, there is also great responsibility and accountability for the decisions made by authorizing officials in exercising this flexibility to specify acceptable security solutions. The results from security control assessments discussed in the previous section provide authorizing officials with essential information for developing an understanding of the current security state of the organization's information systems and supporting infrastructure. This security state is an essential element for understanding the current risk posture of the organization with regard to its susceptibility to threats. In explicitly understanding and accepting the risk resulting from authorization decisions, authorizing officials assume the responsibility and accountability for these decisions.

By employing the risk executive function, organizations will have a comprehensive strategy for bringing together the individual authorization decisions for organizational information systems and supporting infrastructure to address the overall risk posture of the organization. The complex nature of organizations and the many-to-many relationships among missions/business processes

and the information systems supporting those processes, demand a risk-based approach that considers the organization's strategic goals and objectives, priorities, and stakeholder interests. In addition to authorization decisions that are focused on individual information systems, organizations should ensure that common security controls identified by the organization and assigned to appropriate organizational entities for development, implementation, and assessment, go through a similar authorization process. The organization can use the risk executive function to bring all of the authorization results together to obtain a more accurate picture of the organization's overall security state and the ultimate risk to organizational operations and assets, individuals, other organizations, and the Nation based on the collective operation and use of its information systems. The risk executive function promotes a comprehensive, organization-wide view of risk, balancing the risks from information systems with the other types of risks that organizations must address in order to successfully carry out mission/business processes.

Authorization decisions should also consider organizational risks brought about by the use of external providers of services and information (e.g., outsourcing, service-oriented architectures, software as a service, lines of business) in customer/provider relationships and peer-to-peer relationships. Such relationships require the establishment of trust among organizations. The trust relationships are based on the trustworthiness of the information systems providing the services or information to include the evidence brought forth by external providers demonstrating that functionality and assurance claims are being met. The degree of trustworthiness of the information systems employed by external providers should be factored into the authorization decisions and explicit acceptance of risk by authorization officials. In instances where the appropriate level of trustworthiness is not met to reduce risk to an acceptable level, authorization officials should work with program managers, information system owners, and security managers to implement additional compensating security controls.

Authorization decisions by senior leaders can no longer be made in isolation and instead need to be made with regard to organization-wide mission/business process considerations. In addition, authorization decisions must be reexamined periodically as risks change (for example, due to new interconnections or implementation of new applications). Making information security a part of the risk executive function helps ensure that the strategic goals and objectives of the organization are always taken into account when considering the individual authorization (risk acceptance) decisions for organizational information systems and the supporting infrastructure. Whether an individual authorization decision is made from a mission/business process (or organizational) perspective or from the perspective of a single information system, the authorization decisions are interrelated. It is essential that the risk executive function ensures this interrelationship is adequately reflected in the individual authorization decisions, and that the risk executive function works with authorizing officials to inform them of potential new risks which would impact their initial authorization decisions.

- **Key Milestone:** *Has the organization determined and explicitly accepted the risks to its operations (i.e., mission, functions, image, reputation) and assets, individuals, other organizations (partnering or interacting with the organization), and the Nation, based on its risk mitigation decisions and implemented organization-wide protection strategy?*

Figure 7 illustrates the application of the RMF to the organization, showing the role of the risk executive function in providing oversight, monitoring, and risk management of the organization's information security activities.[68]

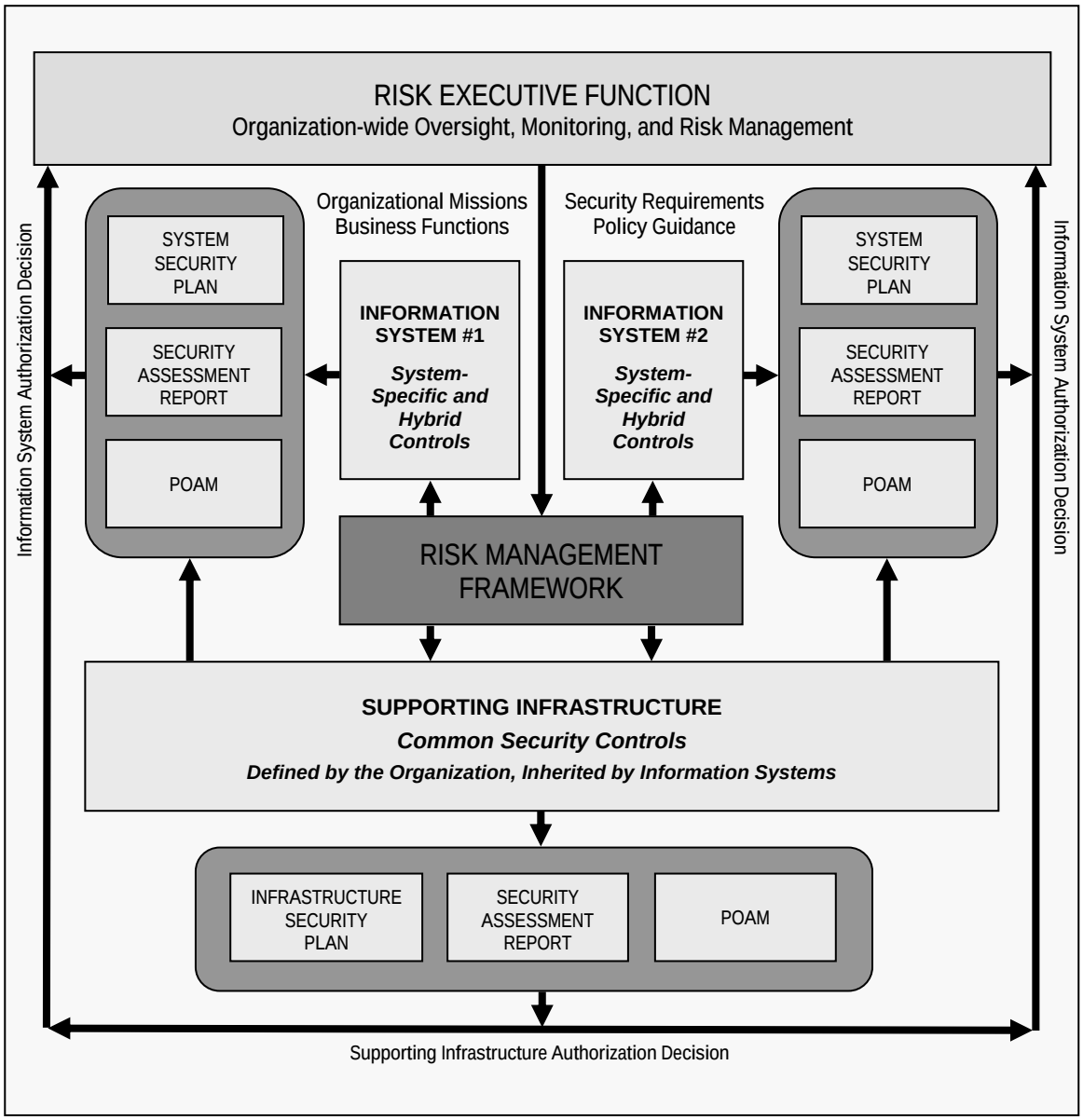

FIGURE 7: EXTENDING THE RISK MANAGEMENT FRAMEWORK TO ORGANIZATIONS

By producing only the essential information necessary for senior leaders to make credible, risk-based decisions with regard to the operation and use of information systems, coordinating those decisions across the organization, and introducing automated support tools in the implementation of information security programs, organizations can more efficiently and cost-effectively manage the risks arising from the operation and use of information systems.

[68] Organizations may choose to employ multiple security plans to document the common security controls associated with the supporting infrastructure depending on the number of entities assigned responsibility for those controls.

3.7 MONITORING THE SECURITY STATE OF THE ORGANIZATION

Conducting thorough point-in-time assessments of security controls in organizational information systems and supporting infrastructure is a necessary but not a sufficient condition to demonstrate security due diligence and to manage risk. Effective information security programs should also include comprehensive continuous monitoring programs to maintain on-going, up-to-date knowledge by senior leaders of the organization's security state and risk posture and to initiate appropriate responses as needed when changes occur. Continuous monitoring programs achieve these objectives by:

- Determining if the security controls in organizational information systems and supporting infrastructure continue to be effective over time in light of the inevitable changes that occur in the systems as well as the environment in which the systems operate; and
- Causing the necessary steps of the RMF to be engaged to adequately address these changes to include, for example, re-categorizing information and information systems and responding to any changes in the FIPS 199 impact levels of the systems by appropriately adjusting security controls, and reauthorizing the systems, when required.

A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status information to appropriate organizational officials. This information is used to maintain a current understanding of the security state and risk posture of the organization and to facilitate appropriate risk mitigation actions. The information is also used to make credible, risk-based decisions regarding the continued operation of the organization's information systems and the continued use of common controls in the supporting infrastructure, and the explicit acceptance of risk that results from those decisions. Continuous monitoring programs provide organizations with an effective tool for producing ongoing updates to security plans, security assessment reports, and plans of action and milestone documents.

Organizations can use NIST Special Publications 800-37 and 800-53A to develop rigorous and comprehensive continuous monitoring programs. Effective organization-wide monitoring programs include:

- Employing strict configuration management and control processes for organizational information systems;
- Documenting changes to the organization's information systems and supporting infrastructure (including the environments of operation for those information systems);
- Conducting security impact analyses of the changes to organizational information systems and supporting infrastructure;
- Developing strategies for selecting and assessing subsets of security controls implemented in organizational information systems and supporting infrastructure that address the priority and frequency of those assessments;
- Conducting assessments of agreed-upon subsets (and holistic assessments over an agreed-upon time period) of security controls in accordance with the priorities and frequency established by the organization; and
- Reporting the security status of both information systems and the supporting infrastructure to appropriate organizational officials on a regular basis.

Organizations should use the current risk assessment, results of previous security control assessments, and operational requirements in guiding the selection of controls to be monitored and the frequency of the monitoring process. Priority for control monitoring should be given to the security controls that have the greatest volatility (i.e., greatest potential for change) after implementation, the controls that have the potential to affect the greatest number of information systems (e.g., common security controls), and the controls that have been identified in the organization's plans of action and milestones for the information systems and supporting infrastructure. Security control volatility is a measure of how frequently a control is likely to change over time. For example, security policies and implementing procedures in a particular organization are less likely to change from one year to the next and thus would be a security control with lower volatility. Access control mechanisms or other technical controls that are subject to the direct effects or side effects of frequent changes in hardware, software, and/or firmware components of information systems would therefore be security controls with higher volatility. Organizations should apply greater resources to security controls deemed to be of higher volatility as there is typically a higher return on investment for assessing security controls of this type. Security controls identified in the plans of action and milestones should also be a priority in the continuous monitoring process, due to the fact that these controls have been deemed to be ineffective to some degree (or nonexistent, in the worst case).

Since organizations conduct business in dynamic environments of operation with constantly changing threats, vulnerabilities, and technologies, authorization decisions and the risk acceptance associated with those decisions, need to be revisited on a regular basis. Risk-based protection approaches are redefining how organizations conduct certification and accreditation processes and the results produced from those processes. The ability for organizations to update authorization decisions in near real-time to get an accurate picture of the current security state of an organization's information systems and supporting infrastructure is paramount to effectively managing risk. The employment of automated support tools to allow authorizing officials and other senior leaders within the organization to obtain frequent security status information by examining the security plans for information systems, updated risk assessments, security assessment reports, and the plans of action and milestone documents, is critical to understanding and explicitly accepting risk on a day-to-day basis. The risk executive function should help facilitate this process across the organization and help ensure that all of the above activities occur with an organizational perspective that focuses on *outcomes* and the risk to the organization's mission/business processes (see Figure 7 in Section 3.6).

In summary, organizations must make informed judgments regarding the application of limited assessment resources when conducting continuous monitoring activities to ensure that the expenditures are consistent with the organization's mission requirements, security categorizations in accordance with FIPS 199, and assessment requirements articulated in federal legislation, policy, directives, and regulations. As risk management becomes more dynamic in nature, relying to a greater degree on the continuous monitoring aspects of the process, the ability for organizations to update key security documents frequently based on the assessment results obtained from monitoring processes and to take timely risk mitigation actions becomes a critical aspect of organizational information security programs.

- **Key Milestone:** *Is the organization effectively monitoring the implementation of its organization-wide protection strategy on a regular basis, including an ongoing assessment of the security state of the information systems supporting its mission/business processes?*

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, REGULATIONS, MEMORANDA, STANDARDS, AND GUIDELINES[69]

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. Paperwork Reduction Act (P.L. 104-13), May 1995.
4. USA PATRIOT Act (P.L. 107-56), October 2001.
5. Privacy Act of 1974 (P.L. 93-579), December 1974.

POLICIES, DIRECTIVES, INSTRUCTIONS, REGULATIONS, AND MEMORANDA

6. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
7. Office of Management and Budget, Federal Enterprise Architecture (FEA) Program Management Office, FEA Consolidated Reference Model Document, October 2007.
8. Office of Management and Budget, Federal Enterprise Architecture (FEA) Program Management Office, FEA Practice Guidance, November 2007.
9. Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, June 2006.

STANDARDS

10. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
11. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

GUIDELINES

12. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
13. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002. (Note: This document is currently under revision and will be reissued as Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*.)
14. National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

[69] The status of and most current versions of NIST publications including FIPS and Special Publications in the 800-series (draft and final) can be found at http://csrc.nist.gov/publications.

15. National Institute of Standards and Technology Special Publication 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007.
16. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Final Public Draft), December 2007.
17. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
18. National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.
19. National Institute of Standards and Technology Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004.
20. National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, May 2005.
21. National Institute of Standards and Technology Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005.
22. National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007.
23. National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-39. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

Accreditation [FIPS 200, NIST SP 800-37]	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Accreditation Boundary [NIST SP 800-37]	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.
Accrediting Authority	See Authorizing Official.
Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Agency	See Executive Agency.
Aggregated Risk	Risks from information systems that are collected, analyzed and assimilated through the Risk Executive Function for senior management's review and used in determining the overall risk to organizational operations, organizational assets, individuals, other organizations, or the Nation.
Authentication [FIPS 200]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.
Authorize Processing	See Accreditation.
Authorizing Official [FIPS 200, NIST SP 800-37]	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.

Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).
Boundary Protection Device	A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) monitors and controls communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications. Boundary protection devices include such components as proxies, gateways, routers, firewalls, guards, and encrypted tunnels.
Certification [FIPS 200, NIST SP 800-37]	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, 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.
Certification Agent [NIST SP 800-37]	The individual, group, or organization responsible for conducting a security certification.
Chief Information Officer [PL 104-106, Sec. 5125(b)]	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Classified National Security Information [E.O. 13292]	Information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
Common Security Control [NIST SP 800-37]	Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.

Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control [CNSS Inst. 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Countermeasures [CNSS Inst. 4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Defense-in Breadth	A comprehensive information security strategy for protecting information systems over the system life cycle (i.e., product and/or system design and development, manufacturing, packaging, assembly, system integration, distribution, operations, maintenance, and retirement).
Defense-in-Depth [CNSS Inst. 4009, Adapted]	Information security strategy integrating people, processes, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of information systems.
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
External Information System (or Component)	An information system or component of an information system that is outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service	An information system service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system).
External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges (i.e., supply chain collaborations or partnerships).

Federal Enterprise Architecture [FEA Program Management Office]	A business-based framework for governmentwide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
Global Supply Chain	A system of organizations, people, activities, information, and resources, international in scope, involved in moving a product or service from supplier/producer to consumer.
High-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
Hybrid Security Control	Security control that has the properties of both a common security control and a system-specific security control (i.e., one part of the control is deemed to be common, while another part of the control is deemed to be system-specific).
Incident [FIPS 200]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Industrial Control System	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.
Information [FIPS 199]	An instance of an information type.
Information Owner [CNSS Inst. 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy [CNSS Inst. 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information System [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [Note: Information systems consist of people, processes, and technology.]
Information System Owner (or Program Manager) [CNSS Inst. 4009, Adapted]	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Officer [CNSS Inst. 4009, Adapted]	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program.
Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Inheritance	A situation in which an information system or an application receives protection from security controls (or portions of security controls) that are implemented by other entities either internal or external to the organization where the system or application resides.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Line of Business	The following OMB-defined process areas common to virtually all federal agencies: Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and IT Infrastructure.
Low-Impact System [FIPS 200]	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.

Malicious Code [CNSS Inst. 4009] [NIST SP 800-61]	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Management Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Media [FIPS 200]	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Media Sanitization [NIST SP 800-88]	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Moderate-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.
National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Non-repudiation [CNSS Inst. 4009 Adapted]	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Operational Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
Organization [FIPS 200]	A federal agency or, as appropriate, any of its operational elements.

Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact [FIPS 199 Adapted]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Risk [FIPS 200 Adapted]	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation or use of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment [NIST SP 800-30, Adapted]	The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation or use of an information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in-place security controls.
Risk Management [FIPS 200 Adapted]	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation or use of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Safeguards [CNSS Inst. 4009, Adapted]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Scoping Guidance	Provides organizations with specific policy/regulatory-related, technology-related, physical infrastructure-related, operational/environmental-related, public access-related, scalability-related, common security control-related, and security objective-related considerations on the applicability and implementation of individual security controls in the control baseline.

Security Category [FIPS 199 Adapted]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Baseline [FIPS 200]	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.
Security Functions	The hardware, software, and firmware of the information system responsible for supporting and enforcing the system security policy and supporting the isolation of code and data on which the protection is based.
Security Impact Analysis [NIST SP 800-37]	The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.
Security Incident	See Incident.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Perimeter	See Accreditation Boundary.
Security Plan	See System Security Plan.
Security Requirements [FIPS 200]	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
Supply Chain	A system of organizations, people, activities, information, and resources involved in moving a product or service from supplier/producer to consumer.
System	See Information System.
System-specific Security Control [NIST SP 800-37]	A security control for an information system that has not been designated as a common security control.
System Security Plan [NIST SP 800-18, Rev 1]	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Tailoring	The process by which a security control baseline selected in accordance with the FIPS 199 security categorization of the information system is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls, where allowed.
Tailored Security Control Baseline	Set of security controls resulting from the application of the tailoring guidance to the security control baseline.
Technical Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
Trusted Distribution	Method for distributing hardware, software, and firmware components that protects those components from modification during distribution.
Trustworthiness	A characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system.
User [CNSS Inst. 4009]	Individual or (system) process authorized to access an information system.

Vulnerability [CNSS Inst. 4009, Adapted]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CI/KR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
DCID	Director of Central Intelligence Directive
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOD	Department of Defense
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
RMF	Risk Management Framework
SDLC	System Development Life Cycle
SECDEF	Secretary of Defense
SPP	Security and Privacy Profile
SSP	Sector-Specific Plan
SP	Special Publication

APPENDIX D

MANAGING RISKS WITHIN LIFE CYCLE PROCESSES

APPLYING THE RISK MANAGEMENT FRAMEWORK WITHIN THE SDLC

Managing the risks from information systems includes addressing the causes of vulnerabilities that arise during the design, development, implementation, operation, and disposition of those systems. This should be accomplished in the context of the routine SDLC processes employed by organizations. Information security considerations should be addressed by organizations as early as possible in the SDLC to ensure the most cost-effective implementation of the security controls needed to adequately mitigate risk from the operation and use of information systems. Each phase of the SDLC includes a minimum set of information security-related activities required to effectively incorporate security capabilities into information systems.[70] The steps in the NIST Risk Management Framework (RMF) are addressed within the security activities described for the SDLC. The RMF can be applied to both new development systems and legacy systems. Table D-1 illustrates the security activities and RMF steps that are applied at each phase of the SDLC.

TABLE D-1. SECURITY ACTIVITIES AND RMF STEPS INTEGRATED INTO THE SDLC PROCESS

SDLC PHASE	Security Activities and RMF Steps
Initiation	*Needs Determination—RMF Step 1 (Categorize)* *Preliminary Risk Assessment— RMF Step 1 (Categorize)* *Security Categorization— RMF Step 1 (Categorize)*
Development and Acquisition	*Requirements Analysis— RMF Step 1 (Categorize)* *Risk Assessments— RMF Steps 1-2, 4, 6 (Categorize, Select, Assess, Monitor)* *Cost Considerations and Reporting* *Security Planning* *- Security Control Selection— RMF Step 2 (Select)* *- Security Control Documentation—RMF Step 2 (Select)* *Security Control Development—RMF Step 3 (Implement)* *Developmental Security Test and Evaluation—RMF Step 3 (Implement)* *Other Planning Components*
Implementation	*Inspection and Acceptance* *System Integration—RMF Step 3 (Implement)* *Security Certification—RMF Step 4 (Assess)* *Security Accreditation—RMF Step 5 (Authorize)*
Operations and Maintenance	*Configuration Management and Control—RMF Step 6 (Monitor)* *Continuous Monitoring—RMF Step 6 (Monitor)*
Disposition	*Information Preservation—RMF Step 6 (Monitor)* *Media Sanitization—RMF Step 6 (Monitor)* *Hardware and Software Disposal—RMF Step 6 (Monitor)*

[70] NIST Special Publication 800-64 presents a framework for incorporating information security into all phases of the SDLC to ensure the selection, acquisition, and use of appropriate and cost-effective security controls.

Although the RMF steps in Table D-1 are arrayed in a linear manner with respect to the phases in the SDLC, the actual implementation is iterative. For example, during the continuous monitoring step in the RMF, new vulnerabilities might be discovered by organizations that require additional risk mitigation actions in the form of reassessing the original security categorizations of the information and information systems supporting the organization's mission/business processes. A change in information system impact levels would result in the requirement to develop new security controls. The iterative nature of the RMF is reflected in the SDLC correspondingly by transitioning from the operations and maintenance phase of the SDLC back to the initiation phase and subsequently to the development and acquisition phase. Both the RMF and the SDLC offer sufficient flexibility to respond to changing conditions that can potentially affect the security of information systems and ultimately to manage the risks to organizational operations and assets, individuals, other organizations, and the Nation.

In many cases, organizations will be applying information security to legacy information systems that have been in operation for some extended period of time with a set of security controls already in place. Some legacy systems may have excellent security plans that provide comprehensive documentation of the risk management decisions that have been made, to include identifying the security controls currently employed. However, other systems may have little, if any, documentation available. For legacy information systems, although the system is in the operations and maintenance phase of the SDLC, the RMF still applies and can be thought of as a potential system upgrade that represents a full life cycle process from requirements identification and development/acquisition to implementation of the upgrade and back into operations and maintenance. The first two steps in the RMF are executed and culminate in the development of an agreed-upon set of security controls for the information system.

At this point in the process, the agreed-upon security controls are compared to the actual controls that have been employed in the legacy system to determine if there are any discrepancies or shortfalls. The delta factor, or difference between the actual security controls employed in the legacy information system versus the controls necessary to adequately protect organizational mission/business processes supported by the system, provides the necessary information to initiate appropriate upgrades. If a security plan exists, it is updated with the additional security controls and/or control enhancements identified during the execution of the initial steps in the RMF. If a security plan does not exist, a plan is created, documenting the agreed-upon security controls. Next, the necessary acquisitions and development activities are carried out to implement these controls. Once the additional security controls have been implemented, completing the third step in the RMF, the final three steps can be initiated resulting in the assessment of the security controls, the authorization decision, and continuous monitoring of the legacy system.

For both new development and legacy information systems, cost, schedule, and performance issues are the primary consideration for organizational officials concerned with carrying out critical mission/business processes. If information security requirements have been given a high priority by senior leaders and integrated into the SDLC process, the appropriate security controls needed to protect organizational operations and assets, individuals, other organizations, or the Nation will have been included in the performance requirements for the information systems. Authorization decisions rendered for information systems include all relevant considerations in managing risk to ensure that the organization can effectively carry out its mission/business processes.