NIST Special Publication 800-30
Revision 1

Guide for Conducting Risk Assessments

National Institute of Standards and Technology
U.S. Department of Commerce

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

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

INITIAL PUBLIC DRAFT

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

September 2011

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary for Standards and Technology and 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 national security-related 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 publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such 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 Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Nothing in this publication should be taken to contradict the 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. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Special Publication 800-30, 85 pages

(September 2011)

CODEN: NSPUE2

Public comment period: September 19 through November 4, 2011

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

In accordance with the provisions of FISMA,[1] the Secretary of Commerce shall, on the basis of standards and guidelines developed by NIST, prescribe standards and guidelines pertaining to federal information systems. The Secretary shall make standards compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of federal information systems. Standards prescribed shall include information security standards that provide minimum information security requirements and are otherwise necessary to improve the security of federal information and information systems.

- Federal Information Processing Standards (FIPS) are approved by the Secretary of Commerce and issued by NIST in accordance with FISMA. FIPS are compulsory and binding for federal agencies.[2] FISMA requires that federal agencies comply with these standards, and therefore, agencies may not waive their use.
- Special Publications (SPs) are developed and issued by NIST as recommendations and guidance documents. For other than national security programs and systems, federal agencies must follow those NIST Special Publications mandated in a Federal Information Processing Standard. FIPS 200 mandates the use of Special Publication 800-53, as amended. In addition, OMB policies (including OMB Reporting Instructions for FISMA and Agency Privacy Management) state that for other than national security programs and systems, federal agencies must follow certain specific NIST Special Publications.[3]
- Other security-related publications, including interagency reports (NISTIRs) and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when specified by OMB.
- Compliance schedules for NIST security standards and guidelines are established by OMB in policies, directives, or memoranda (e.g., annual FISMA Reporting Guidance).[4]

[1] The E-Government Act (P.L. 107-347) recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

[2] The term *agency* is used in this publication in lieu of the more general term *organization* only in those circumstances where its usage is directly related to other source documents such as federal legislation or policy.

[3] While federal agencies are required to follow certain specific NIST Special Publications in accordance with OMB policy, there is flexibility in how agencies apply the guidance. Federal agencies apply the security concepts and principles articulated in the NIST Special Publications in accordance with and in the context of the agency's missions, business functions, and environment of operation. Consequently, the application of NIST guidance by federal 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. Given the high priority of information sharing and transparency within the federal government, agencies also consider reciprocity in developing their information security solutions. When assessing federal agency compliance with NIST Special Publications, Inspectors General, evaluators, auditors, and assessors consider the intent of the security concepts and principles articulated within the specific guidance document and how the agency applied the guidance in the context of its mission/business responsibilities, operational environment, and unique organizational conditions.

[4] Unless otherwise stated, all references to NIST publications in this document (i.e., Federal Information Processing Standards and Special Publications) are to the most recent version of the publication.

Acknowledgements

This publication was developed by the *Joint Task Force Transformation Initiative* Interagency Working Group with representatives from the Civil, Defense, and Intelligence Communities in an ongoing effort to produce a unified information security framework for the federal government. The National Institute of Standards and Technology wishes to acknowledge and thank the senior leaders from the Departments of Commerce and Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and the members of the interagency technical working group whose dedicated efforts contributed significantly to the publication. The senior leaders, interagency working group members, and their organizational affiliations include:

U.S. Department of Defense

Teresa M. Takai
Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (Acting)

Gus Guissanie
Deputy Assistant Secretary of Defense (Acting)

Dominic Cussatt
Senior Policy Advisor

Barbara Fleming
Senior Policy Advisor

Office of the Director of National Intelligence

Adolpho Tarasiuk Jr.
Assistant Director of National Intelligence and Intelligence Community Chief Information Officer

Charlene P. Leubecker
Deputy Intelligence Community Chief Information Officer

Mark J. Morrison
Director, Intelligence Community Information Assurance

Roger Caslow
Chief, Risk Management and Information Security Programs Division

National Institute of Standards and Technology

Cita M. Furlani
Director, Information Technology Laboratory

William C. Barker
Cyber Security Advisor, Information Technology Laboratory

Donna Dodson
Chief, Computer Security Division

Ron Ross
FISMA Implementation Project Leader

Committee on National Security Systems

Teresa M. Takai
Acting Chair, CNSS

Eustace D. King
CNSS Subcommittee Co-Chair

Kevin Deeley
CNSS Subcommittee Co-Chair

Lance Dubsky
CNSS Subcommittee Co-Chair

Joint Task Force Transformation Initiative Interagency Working Group

Ron Ross *NIST, JTF Leader*	Gary Stoneburner *Johns Hopkins APL*	Jennifer Fabius *The MITRE Corporation*	Kelley Dempsey *NIST*
Deborah Bodeau *The MITRE Corporation*	David R. Comings *Tenacity Solutions, Inc.*	Peter Gouldmann *Department of State*	Arnold Johnson *NIST*
Peter Williams *Booz Allen Hamilton*	Karen Quigg *The MITRE Corporation*	Christina Sames *TASC*	Christian Enloe *NIST*

In addition to the above acknowledgments, a special note of thanks goes to Peggy Himes and Elizabeth Lennon of NIST for their superb technical editing and administrative support. The authors also gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, both nationally and internationally, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

DEVELOPING COMMON INFORMATION SECURITY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by 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 publications are complementary with the standards and guidelines employed for the protection of national security systems. In addition to its comprehensive public review and vetting process, NIST is collaborating 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. A common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their contractors, more uniform and consistent ways to manage the risk to organizational operations and assets, individuals, other organizations, and the Nation that results from the operation and use of information systems. A common foundation for information security will also provide a strong basis for reciprocal acceptance of security authorization decisions and facilitate information sharing. NIST is also 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).

Notes to Reviewers

NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, is the fifth in the series of risk management and information security guidelines being developed by the Joint Task Force, a joint partnership among the Department of Defense, the Intelligence Community, NIST, and the Committee on National Security Systems. The partnership, under the leadership of the Secretary of Defense, the Director of National Intelligence, and the Secretary of Commerce, continues to collaborate on the development of a unified information security framework for the federal government to address the challenges of protecting federal information and information systems as well as the Nation's critical information infrastructure.

In today's world of complex and sophisticated threats, risk assessments are an essential tool for organizations to employ as part of a comprehensive risk management program. Risk assessments can help organizations:

- Determine the most appropriate risk responses to ongoing cyber attacks or threats from man-made or natural disasters;
- Guide investment strategies and decisions for the most effective cyber defenses to help protect organizational operations (including missions, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and
- Maintain ongoing situational awareness with regard to the security state of organizational information systems and the environments in which the systems operate.

This publication changes the focus of Special Publication 800-30, originally published as a risk management guideline. NIST Special Publication 800-39 has now replaced Special Publication 800-30 as the authoritative source of comprehensive risk management guidance. The update to Special Publication 800-30 focuses exclusively on risk assessments, one of the four steps in the risk management process. The risk assessment guidance in Special Publication 800-30 has been significantly expanded to include more in-depth information on a wide variety of risk factors essential to determining information security risk (e.g., threat sources and events, vulnerabilities and predisposing conditions, impact, and likelihood of threat occurrence). A three-step process is described including key activities to prepare for risk assessments, activities to successfully conduct risk assessments, and approaches to maintain the currency of assessment results.

In addition to providing a comprehensive process for assessing information security risk, the publication also describes how to apply the process at the three tiers in the risk management hierarchy—the *organization* level, *mission/business process* level, and *information system* level. To facilitate ease of use for individuals or groups conducting risk assessments within organizations, a set of exemplary templates, tables, and assessment scales for common risk factors is also provided. The templates, tables, and assessment scales give maximum flexibility in designing risk assessments based on the express purpose, scope, assumptions, and constraints established by organizations.

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 meet the needs of our customers.

-- RON ROSS
FISMA IMPLEMENTATION PROJECT LEADER
JOINT TASK FORCE LEADER

Table of Contents

Prologue

"*... Through the process of risk management, leaders must consider risk to U.S. 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

CAUTIONARY NOTE

SCOPE AND APPLICABILITY OF RISK ASSESSMENTS

Risk assessments are required for effective risk management and to inform decision making at all three tiers in the risk management hierarchy including the organization level, mission/business process level, and information system level. Furthermore, risk assessments are enduring and should be conducted throughout the system development life cycle, from pre-system acquisition (i.e., material solution analysis and technology development), through system acquisition (i.e., engineering/manufacturing development and production/deployment), and on into sustainment (i.e., operations/support). There are no specific requirements with regard to: (i) the formality, rigor, or level of detail risk assessments; (ii) the methodologies, tools, and techniques used to conduct such risk assessments; or (iii) the format and content of assessment results and any associated reporting mechanisms. Therefore, organizations have maximum flexibility on how risk assessments are conducted and employed and are encouraged to apply the guidance in this document in the manner that most effectively and cost-effectively provides the information necessary for informed risk management decisions. Organizations are also cautioned that risk assessments are often not precise instruments of measurement and reflect: (i) the limitations of specific assessment methodologies, tools, and techniques employed; (ii) the subjectivity, quality, and trustworthiness of the data used; (iii) the interpretation of assessment results; and (iv) the skills and expertise of those individuals or groups conducting the assessments. Since cost, timeliness, and ease of use are a few of the many important factors in the application of risk assessments, organizations should attempt to reduce the complexity of risk assessments and maximize the reuse of assessment results by sharing risk-related information across their enterprises, whenever possible.

CHAPTER ONE

INTRODUCTION

THE NEED FOR RISK ASSESSMENTS TO SUPPORT ENTERPRISE-WIDE RISK MANAGEMENT

Organizations[5] in the public and private sectors depend on *information systems*[6] to successfully carry out their missions and business functions. Information systems can include very diverse entities ranging from office networks, financial and personnel systems to very specialized systems (e.g., weapons systems, telecommunications systems, industrial/process control systems, and environmental control systems). Information systems are subject to serious *threats* that can have adverse effects on organizational operations (i.e., missions, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation by exploiting both known and unknown vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems. Threats to information and information systems can include purposeful attacks, environmental disruptions, and human/machine errors and result in great harm to the national and economic security interests of the United States. Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations.

Risk assessment is one of the key components of an organizational risk management process as described in NIST Special Publication 800-39. Risk assessments identify, prioritize, and estimate risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems. The purpose of the risk assessment component is to identify: (i) threats to organizations or threats directed through organizations against other organizations or the Nation; (ii) vulnerabilities internal and external to organizations; (iii) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. The end result is a determination of risk (i.e., the degree of harm and likelihood of harm occurring). Risk assessments can be conducted at all three tiers in the risk management hierarchy—including Tier 1 (organization level), Tier 2 (mission/business process level), and Tier 3 (information system level).[7] At Tier 1 and Tier 2, risk assessments are used to evaluate, for example, systemic information security-related risks associated with organizational governance and management activities, mission/business processes or enterprise architecture, and funding of information security programs. At Tier 3, risk assessments are used to effectively support the implementation of the *Risk Management Framework* (i.e., security categorization, security control selection, security control implementation, security control assessment, information system authorization, and monitoring).[8]

[5] 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.

[6] An *information system* is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes the environment in which the information system operates (i.e., people, processes, technologies, facilities, and cyberspace).

[7] The risk management hierarchy is described in NIST Special Publication 800-39 and is discussed in greater detail in Chapter 2.

[8] The Risk Management Framework is described in NIST Special Publication 800-37.

1.1 PURPOSE AND APPLICABILITY

The purpose of Special Publication 800-30 is to provide guidance for conducting risk assessments of federal information systems and organizations. Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process—providing senior leaders/executives with the information needed to determine appropriate courses of action to take in response to identified risks. In particular, this document provides practitioners with practical guidance for carrying out each of the three steps in the *risk assessment process* (i.e., prepare for the assessment, conduct the assessment, and maintain the assessment) and how risk assessments and other organizational risk management processes complement and inform each other. Special Publication 800-30 also provides guidance on identifying risk factors to monitor on an ongoing basis, so that organizations can determine whether levels of risk have increased to unacceptable levels (i.e., exceeding organizational risk tolerance) and different courses of action should be taken.

This publication satisfies the requirements of FISMA and meets or exceeds the information security requirements established for executive agencies[9] by the Office of Management and Budget (OMB) in Circular A-130, Appendix III, *Security of Federal Automated Information Resources.* The guidelines in this publication are 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 have been broadly developed from a technical perspective to complement similar guidelines for national security systems and may be used for such systems with the approval of appropriate federal officials exercising policy authority over such systems. State, local, and tribal governments, as well as private sector organizations are encouraged to consider using these guidelines, as appropriate.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse group of risk management professionals including:

- Individuals with oversight responsibilities for risk management (e.g., heads of agencies, chief executive officers, chief operating officers);
- Individuals with responsibilities for conducting organizational missions/business functions (e.g., mission/business owners, information owners/stewards, authorizing officials);
- Individuals with responsibilities for acquiring information technology products, services, or information systems (e.g., acquisition officials, procurement officers, contracting officers);
- Individuals with information system/security design, development and implementation responsibilities (e.g., program managers, enterprise architects, information security architects, information system/security engineers; information systems integrators);
- Individuals with information security oversight, management, and operational responsibilities (e.g., chief information officers, senior information security officers,[10] information security managers, information system owners, common control providers); and

[9] An *executive agency* is: (i) an executive department specified in 5 U.S.C., Section 101; (ii) a military department specified in 5 U.S.C., Section 102; (iii) an independent establishment as defined in 5 U.S.C., Section 104(1); and (iv) a wholly owned government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. In this publication, the term *executive agency* is synonymous with the term *federal agency*.

[10] At the *agency* level, this position is known as the Senior Agency Information Security Officer. Organizations may also refer to this position as the *Chief Information Security Officer*.

- Individuals with information security/risk assessment and monitoring responsibilities (e.g., system evaluators, penetration testers, security control assessors, risk assessors, independent verifiers/validators, inspectors general, auditors).

1.3 RELATED PUBLICATIONS

The risk assessment approach described in this publication is supported by a series of security standards and guidelines necessary for managing information security risk. In particular, the Special Publications developed by the Joint Task Force Transformation Initiative supporting the unified information security framework for the federal government include:

- Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*;[11]
- Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*;
- Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*; and
- Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*.

The concepts and principles contained in this publication are intended to implement, for federal information systems and organizations, risk assessment processes and approaches that are similar to the processes and approaches described in International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) standards. Extending the concepts and principles of international standards for the federal government and its contractors and promoting the reuse of risk assessment results, reduces the burden on organizations that must conform to ISO/IEC and NIST standards.

1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes: (i) the risk management process and how risk assessments are an integral part of that process; (ii) the basic terminology used in conducting risk assessments; and (iii) how risk assessments can be applied across the organization's risk management tiers (i.e., organization level, mission/business process level, and information system level).
- **Chapter Three** describes the process of assessing information security risk including: (i) a high-level overview of the risk assessment process; (ii) the activities necessary to prepare for risk assessments; (iii) the activities necessary to conduct effective risk assessments; and (iv) the activities necessary to maintain the results of risk assessments on an ongoing basis.
- **Supporting appendices** provide additional risk assessment information on a variety of topics including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) threat sources; (v) threat events; (vi) vulnerabilities and predisposing conditions; (vii) likelihood of threat event occurrence; (viii) impact; (ix) risk and uncertainty; (x) prioritization of risks; and (xi) a summary of risk assessment tasks.

[11] Special Publication 800-39 supersedes Special Publication 800-30 as the primary source for guidance on information security risk management.

CHAPTER TWO

THE FUNDAMENTALS

BASIC CONCEPTS ASSOCIATED WITH RISK ASSESSMENTS

This chapter describes the fundamental concepts associated with assessing information security risk within an organization including: (i) a high-level overview of the risk management process and the role risk assessments play in that process; (ii) the basic concepts used in conducting risk assessments; and (iii) how risk assessments can be applied across the organization's risk management tiers.[12] Risk assessment is a key component of a holistic, organization-wide *risk management process* as defined in NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*. Risk management processes include: (i) establishing the context for risk management activities to be carried out (i.e., risk framing); (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk. Figure 1 illustrates the fundamental steps in the risk management process including the risk assessment step and the information and communications flows necessary to make the process work effectively.

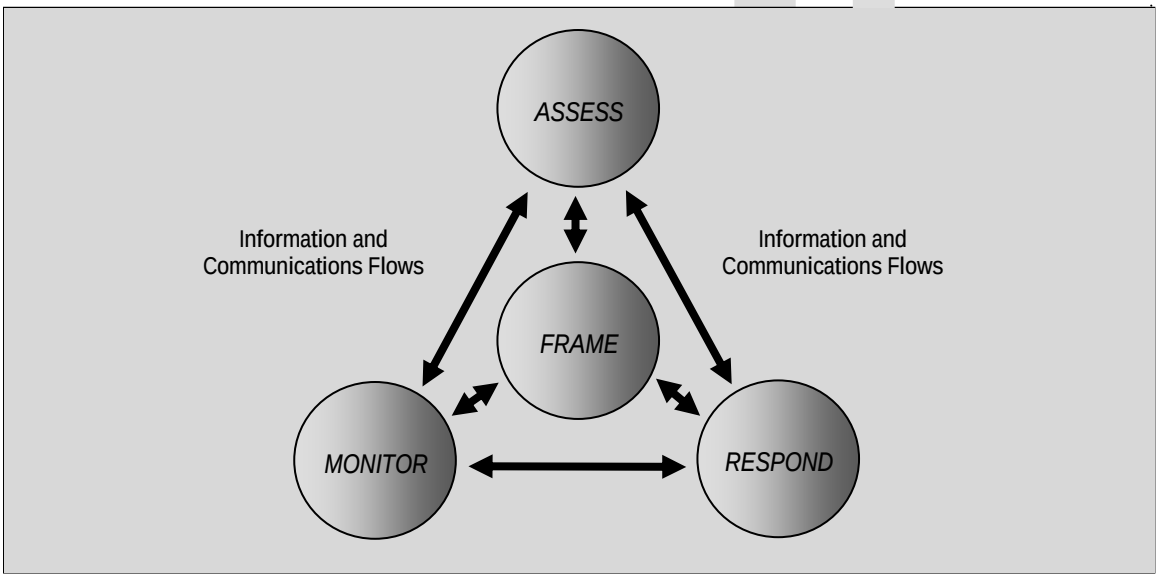

FIGURE 1: RISK ASSESSMENT WITHIN THE RISK MANAGEMENT PROCESS

The first component of risk management addresses how organizations *frame* risk or establish a risk context—that is, describing the environment in which risk-based decisions are made. The purpose of the risk framing component is to produce a *risk management strategy* that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. The risk frame establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations.

[12] NIST Special Publication 800-39 provides guidance on the three tiers in the risk management hierarchy including Tier 1 (organization), Tier 2 (mission/business process), and Tier 3 (information system).

The second component of risk management addresses how organizations *assess* risk within the context of the organizational risk frame. The purpose of the risk assessment component is to identify: (i) threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation; (ii) vulnerabilities internal and external to organizations;[13] (iii) the harm (i.e., adverse impact) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur. The end result is a determination of risk (i.e., the degree of harm and likelihood of harm occurring).

The third component of risk management addresses how organizations *respond* to risk once that risk is determined based on the results of risk assessments. The purpose of the risk response component is to provide a consistent, organization-wide response to risk in accordance with the organizational risk frame by: (i) developing alternative courses of action for responding to risk; (ii) evaluating the alternative courses of action; (iii) determining appropriate courses of action consistent with organizational risk tolerance; and (iv) implementing risk responses based on selected courses of action.

The fourth component of risk management addresses how organizations *monitor* risk over time. The purpose of the risk monitoring component is to: (i) verify that planned risk responses are implemented and information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, standards, and guidelines are satisfied; (ii) determine the ongoing effectiveness of risk response measures following implementation; and (iii) identify risk-impacting changes to organizational information systems and the environments in which the systems operate.[14]

This publication focuses on the risk assessment component of risk management—providing a step-by-step process on how to *prepare* for risk assessments, how to *conduct* risk assessments, and how to *maintain* the currency of risk assessments over time. The risk framing step in the risk management process described above, provides essential information to organizations when preparing for risk assessments. The risk monitoring step in the risk management process also provides important information to organizations when updating their risk assessments. Chapter Three provides a description of the three steps in the risk assessment process incorporating the basic concepts described in this chapter. Well-designed and well-executed risk assessments can be used to effectively analyze and respond to risks from a complex and sophisticated threat space and subsequently monitor those risks over time. Unlike risk assessments that focus exclusively on information systems, the process described in this publication focuses on *mission* and *business* impacts and the associated risk to organizations. Risk assessments can support a wide variety of risk-based decisions by organizational officials across all three tiers in the risk management hierarchy including:

- Determination of organization-level risks, that is, risks that are common to the organization's core missions or business functions, mission/business processes, mission/business segments, common infrastructure/support services, or information systems;

[13] Organizational vulnerabilities are not confined to information systems but can include, for example, vulnerabilities in governance structures, mission/business processes, enterprise architecture, information security architecture, facilities, equipment, system development life cycle processes, supply chain activities, and external service providers.

[14] Environments of operation include, but are not limited to: the threat space; vulnerabilities; missions/business functions; mission/business processes; enterprise and information security architectures; information technologies; personnel; facilities; supply chain relationships; organizational governance/culture; procurement/acquisition processes; organizational policies/procedures; organizational assumptions, constraints, risk tolerance, and priorities/trade-offs).

- Definition of an information security architecture (embedded within enterprise architecture);
- Definition of interconnection requirements for information systems (including systems supporting mission/business processes and common infrastructure/support services;
- Design of security solutions for information systems and environments of operation including selection of security controls, information technology products, suppliers, and contractors to support core missions/business functions or provide common infrastructure/support services;
- Authorization (or denial of authorization) to operate information systems or to use security controls inherited by those systems (i.e., common controls);
- Modification of missions/business functions and/or mission/business processes permanently, or for a specific time frame (e.g., until a newly discovered vulnerability or attack is addressed);
- Implementation of security solutions (e.g., whether specific information technology products or configurations for those products meet established requirements); and
- Operation and maintenance of security solutions (e.g., continuous monitoring strategies and programs, ongoing risk assessments and authorizations).

2.1 RISK ASSESSMENT CONCEPTS

Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. A *risk assessment* is the process of identifying, prioritizing, and estimating information security risks. Assessing information security risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur.

Any assessment of risk typically includes: (i) an explicit *risk model*, defining key terms and assessable risk factors and the relationships among the factors; (ii) an *assessment approach*, specifying the range of values those risk factors can assume during the assessment; and (iii) an *analysis approach*, specifying how values of those factors are functionally combined to evaluate risk. *Risk factors* are characteristics used in risk models as inputs to determining levels of risk in risk assessments. Risk factors are also used extensively in risk communications to highlight the various aspects of problem domains that strongly affect the levels of risk in particular situations, circumstances, or contexts. Typical risk factors include, for example, threat, vulnerability, impact, likelihood, and predisposing condition. Risk factors can be further decomposed into more detailed characteristics (e.g., threats decomposed into threat sources and threat events).[15]

[15] A risk factor can have a single assessable characteristic (e.g., impact severity), in which case the risk factor is identified with the characteristic for purposes of discussion or presentation. Alternately, a risk factor can have multiple characteristics, some of which may be assessable, some of which may not be assessable. Characteristics which are not assessable typically help determine what lower-level characteristics are relevant. For example, a threat source has a (characteristic) threat type (using a taxonomy of threat types, which are nominal rather than assessable). The threat type determines which of the more detailed characteristics are relevant (e.g., a threat source of type *adversary* has associated characteristics of capabilities, intent, and targeting, which are directly assessable characteristics.

A *risk assessment methodology* is a risk assessment process (as described in Chapter Three), together with a risk model, assessment approach, and analysis approach. Risk assessment methodologies are defined by organizations and are a component of the risk management strategy developed during the risk framing step of the risk management process. Organizations can use a single risk assessment methodology or can employ multiple risk assessment methodologies, with the selection of a specific methodology depending on: (i) the criticality and/or sensitivity of the organization's core missions and business functions including the supporting mission/business processes and information systems; (ii) the maturity of the organization's mission/business processes (by enterprise architecture segments); or (iii) the stage of information systems in the system development life cycle. By making explicit the risk model, the assessment approach, and the analysis approach used, and requiring as part of the assessment process, a rationale for the assessed values of risk factors, organizations can increase the *reproducibility* and *repeatability* of their risk assessments.[16]

2.1.1 Risk Models

Risk models define the key terms used in risk assessments including the risk factors to be assessed and the relationships among those factors. These definitions are important for organizations to document prior to conducting risk assessments because the assessments rely upon well-defined attributes of threats, vulnerabilities, and other risk factors to effectively determine risk. Figure 2 illustrates an example of a risk model for adversarial threats including the key risk factors associated with the model and the relationship among the factors. Each of the risk factors is described in greater detail below and used in the risk assessment process in Chapter Three.

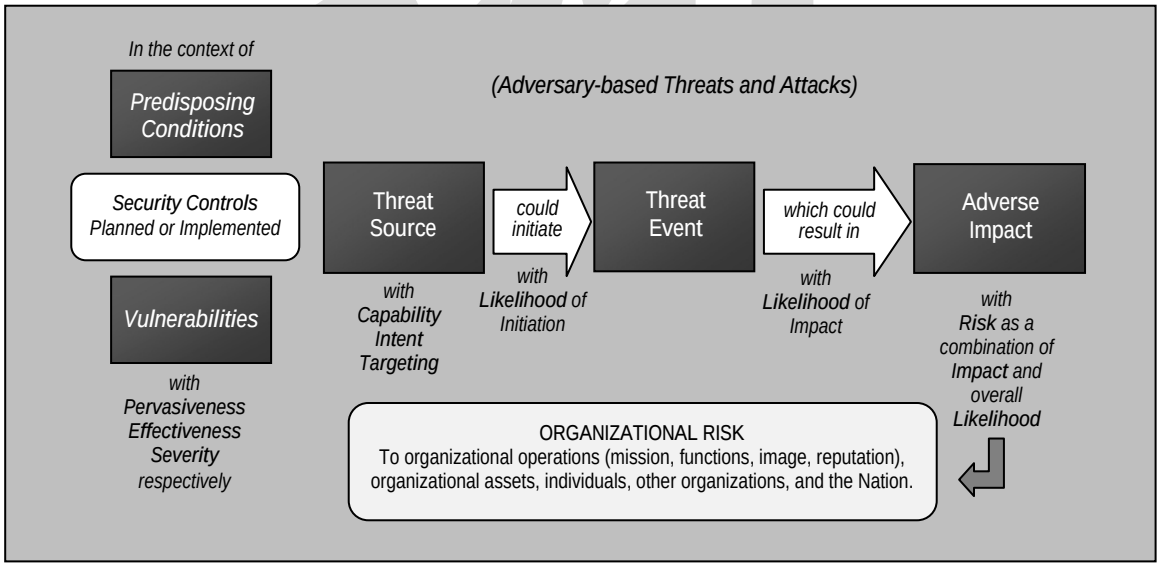

FIGURE 2: RISK MODEL WITH KEY RISK FACTORS FOR ADVERSARIAL THREATS

Threats

A *threat* is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information

[16] *Reproducibility* refers to the ability of different experts to produce the same results from the same data. *Repeatability* refers to the ability to repeat the assessment in the future, in a manner that is consistent with and hence comparable to prior assessments—enabling the organization to identify trends.

system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. There are two aspects to threat considered in this publication: (i) threat sources; and (ii) threat events.

A *threat source* is an actor (causal agent) with the intent and method targeted at the exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability. In general, types of threat sources include: (i) hostile cyber/physical attacks; (ii) human errors of omission or commission; (iii) structural failures of organization-controlled resources (e.g., hardware, software, environmental controls); and (iv) natural and man-made disasters, accidents, and failures beyond the control of the organization.[17] A *threat event* is an event or situation initiated or caused by a threat source that has the potential for causing adverse impact. Threat events for cyber attacks are typically characterized by the tactics, techniques, and procedures (TTPs) employed by adversaries.[18]

Risk models can provide useful distinctions between threat sources and threat events. Various taxonomies of threat sources have been developed.[19] A typical taxonomy of threat sources uses the type of adverse impacts as an organizing principle. Multiple threat sources can initiate or cause the same threat event—for example, a key provisioning server can be taken off-line by a denial-of-service attack, a deliberate act by a malicious system administrator, an administrative error, a hardware fault, or a power failure. Risk models differ in the degree of detail and complexity with which threat events are identified. When threat events are identified with great specificity, *threat scenarios* can be modeled and analyzed.[20]

Vulnerabilities and Predisposing Conditions

A *vulnerability* is an inherent weakness in an information system, security procedures, internal controls, or implementation that could be exploited by a threat source. Most information system vulnerabilities can be identified with security controls either which have not been applied or which, while applied, retain some weakness. However, vulnerabilities need not be identified only within information systems. Viewing information systems in a broader context, vulnerabilities can be found in organizational governance structures (e.g., lack of effective risk management strategies, poor intra-agency communications, inconsistent decisions about relative priorities of core missions and business functions). Vulnerabilities can also be found in external relationships (e.g., dependencies on energy sources, the supply chain, technology, and telecommunications providers), mission/business processes (e.g., poorly defined processes or processes that are not risk-aware), and enterprise and information security architectures (e.g., poor architectural decisions resulting in lack of diversity or resiliency in organizational information systems).[21]

[17] Appendix D provides a taxonomy of threat sources and associated threat characteristics.

[18] Understanding adversary-based threat events gives organizations insights into the capabilities associated with certain threat sources. In addition, having greater knowledge about who is carrying out the attacks gives organizations a better understanding of what adversaries desire to gain by the attacks. Knowing the intent and targeting aspects of a potential attacks helps organizations narrow the set of threat events that are most relevant to consider.

[19] For example, the Software Engineering Institute provides a listing of threat sources in its publication, *A Taxonomy of Operational Security Risks*, December 2010.

[20] A *threat scenario* is set of discrete threat events, attributed to a specific threat source or multiple threat sources, partially ordered in time, that result in adverse effects.

[21] NIST Special Publication 800-39 provides guidance on vulnerabilities at all three tiers in the risk management hierarchy and the potential adverse impact that can occur if threats exploit such vulnerabilities.

In addition to the vulnerabilities described above, organizations also consider predisposing conditions. A *predisposing condition* is a condition that exists within an organization, a mission or business process, enterprise architecture, information system, or environment of operation, which affects (i.e., increases or decreases) the likelihood that threat events, once initiated, result in adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Predisposing conditions include, for example, the location of a facility in a hurricane- or flood-prone region (increasing the likelihood of exposure to hurricanes or floods) or a stand-alone information system with no external network connectivity (decreasing the likelihood of exposure to a network-based cyber attack). Vulnerabilities resulting from predisposing conditions that cannot be easily corrected could include, for example, gaps in contingency plans or weaknesses/deficiencies in information system backup and failover mechanisms. In all cases, these types of vulnerabilities create a predisposition toward threat events having adverse impacts on organizations. Vulnerabilities (including those attributed to predisposing conditions) are part of the overall security state of organizational information systems and environments of operation which can affect the likelihood of a threat event's occurrence.

Likelihood

The *likelihood of occurrence* of a threat event initiated or caused by a threat source, combines an estimate of the likelihood of initiation or occurrence of the threat event, with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts). For adversarial threats, an assessment of likelihood of initiation is typically based on: (i) adversary *intent*; (ii) adversary *capability*; and (iii) adversary *targeting*. Particular concern is given to the advanced persistent threat (APT).[22] For other than adversarial threat events, the likelihood of occurrence can be estimated using historical evidence, empirical data, or other factors. Note that the likelihood that a threat event will be initiated or will occur is assessed with respect to a specific time frame (e.g., the next six months, the next year, or the period until a specified milestone is reached). If a threat event is almost certain to be initiated or occur in the (specified or implicit) time frame, the assessment of risk may take into consideration the estimated frequency of the event. The likelihood of threat occurrence can also be based on the state of the organization, its mission/business processes, enterprise and information security architectures, or information systems and environments of operation (taking into consideration the presence and effectiveness of deployed safeguards and countermeasures (i.e., security controls) to protect against unauthorized or undesirable behavior, detect and limit damage, and/or maintain or restore mission/business capabilities).

Impact

The level of *impact* from a threat event is the magnitude of harm that can be expected to result from the unauthorized disclosure, modification, disruption, destruction, or loss of information and/or denial of service. Such adverse impact, and hence harm, can be experienced by a variety of organizational and non-organizational stakeholders including, for example, heads of agencies, mission and business owners, information owners/stewards, mission/business process owners, information system owners, or individuals/groups in the public or private sectors relying on the organization—in essence, anyone with a vested interest in the organization's operations, assets, or

[22] The *advanced persistent threat* is an adversary with sophisticated levels of expertise/significant resources, allowing it through the use of multiple attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future. Moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.

individuals, including other organizations in partnership with the organization, or the Nation (for critical infrastructure-related considerations).[23]

As noted above, *risk* is the combination of the likelihood of a threat event's occurrence and its potential adverse impact. This definition accommodates many types of adverse impacts at all tiers in the risk management hierarchy described in NIST Special Publication 800-39 (e.g., damage to image or reputation of the organization or financial loss at Tier 1; inability to successfully execute a specific mission/business process at Tier 2; or the resources expended in responding to an information system incident at Tier 3). It also accommodates relationships among impacts (e.g., loss of current or future mission/business effectiveness due to the loss of data confidentiality; loss of confidence in critical information due to loss of data or system integrity; or unavailability or degradation of information or information systems). This broad definition also allows risk to be represented as a single value or as a vector in which different types of impacts are assessed separately. For purposes of risk communication, risk is generally aggregated according to the types of adverse impacts (and possibly the time frames in which those impacts are likely to be experienced).

With regard to the aggregation of risk, there are several issues that organizations may consider. In general, for individual discrete risks (e.g., the risk associated with a single information system supporting a well-defined mission/business process), the worst-case impact establishes an upper bound for the overall risk to organizational operations and assets.[24] In more complex situations involving multiple information systems and multiple mission/business processes with specified relationships and dependencies among those systems and processes, organizations may need to consider risk aggregation. Risk aggregation, conducted primarily at Tier 1 and occasionally at Tier 2, addresses the overall risk to organizational operations and assets, given the risk attributed to each of the discrete risks. There may be situations when organizations desire to assess risk at the organization level when multiple risks materialize concurrently or near the same time. When two or more risks materialize at or near the same time, there is the possibility that the amount of overall risk incurred is beyond the risk capacity of the organization, and therefore the overall impact to organizational operations and assets (i.e., mission/business impact) goes beyond that which was originally assessed for each specific risk.

When assessing risk for potential aggregation issues, organizations consider the relationship among various discrete risks. For example is there a cause and effect relationship so that if one risk materializes, another risk is more likely (or less likely) to materialize? If there is a direct or inverse relationship among discrete risks, then the risks can be coupled (in a qualitative sense) or correlated (in a quantitative sense) either in a positive or negative manner. Risk coupling or correlation (i.e., finding relationships among risks that increase or decrease the likelihood of any specific risk materializing) can be done at Tiers 1, 2, or 3.

[23] The term *organizational assets* can have a very wide scope of applicability to include for example, high-impact programs, physical plant, mission-critical information systems, personnel, equipment, or a logically related group of systems. More broadly, organizational assets represent any resource or set of resources which the organization values, including intangible assets such as image or reputation.

[24] Security categorizations conducted in accordance with FIPS Publication 199 provide examples of *worst-case* impact analyses (using the high-water mark concept). This type of impact analysis provides an upper bound for risk when applied to discrete situations within organizations.

2.1.2 Assessment Approaches

Risk, and its contributing factors, can be assessed in a variety of ways, including quantitatively, qualitatively, or semi-quantitatively.[25] Each risk assessment approach considered by organizations has advantages and disadvantages. A preferred approach (or situation-specific set of approaches) can be selected based on organizational culture and, in particular, attitudes toward the concepts of uncertainty and risk communication. *Quantitative* assessments typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers—where the meanings and proportionality of values are maintained inside and outside the context of the assessment. This type of assessment most effectively supports cost-benefit analyses of alternative risk responses or courses of action. However, the meaning of the quantitative results may not always be clear and may require a qualitative interpretation. For example, organizations may ask if the numbers obtained in the risk assessments are good or bad or if the differences in the obtained values are meaningful or insignificant. Additionally, the rigor of quantification is significantly lessened when subjective determinations are buried within the quantitative assessments, or when significant uncertainty surrounds the determination of values. The benefits of quantitative assessments (in terms of the rigor, repeatability, and reproducibility of assessment results) can, in some cases, be outweighed by the costs (in terms of the expert time and effort and the possible deployment and use of tools required to make such assessments).

In contrast to quantitative assessments, *qualitative* assessments typically employ a set of methods, principles, or rules for assessing risk based on non-numerical categories or levels (e.g., very low, low, moderate, high, very high). This type of assessment supports to a much higher degree, risk communication in conveying assessment results to decision makers. However, the range of values in qualitative assessments is comparatively small in most cases, making the relative prioritization or comparison within the set of reported risks difficult. Additionally, unless each value is very clearly defined or is characterized by meaningful examples, different experts relying on their individual experiences could produce significantly different assessment results. The repeatability and reproducibility of qualitative assessments are increased by the annotation of assessed values (e.g., this value is high because of the following factors) and by using tables or other well-defined functions to combine qualitative values.

Finally, *semi-quantitative* assessments typically employ a set of methods, principles, or rules for assessing risk that uses bins, scales, or representative numbers whose values and meanings are not maintained in other contexts. This type of assessment can provide the benefits of quantitative and qualitative assessments. The bins (e.g., 0-15, 16-35, 35-70, 71-85, 86-100) or scales (e.g., 1-10) translate easily into qualitative terms that support risk communications for decision makers (e.g., a score of 95 can be interpreted as very high), while also allowing relative comparisons between values in different bins or even within the same bin (e.g., the difference between risks scored 70 and 71 respectively is relatively insignificant, while the difference between risks scored 35 and 70 is relatively significant). The role of expert judgment in assigning values is more evident than in a purely quantitative approach. Moreover, if the scales or sets of bins provide sufficient granularity, relative prioritization among results is better supported than in a purely qualitative approach. As in a quantitative approach, rigor is significantly lessened when subjective determinations are buried within assessments, or when significant uncertainty surrounds a determination of value. As with the non-numeric categories or levels used in a well-founded qualitative approach, each bin or range of values needs to be clearly defined and/or characterized by meaningful examples.

[25] The definitions for *quantitative*, *qualitative*, and *semi-quantitative* assessments are obtained from the Department of Homeland Security (DHS) publication, *DHS Risk Lexicon.*

2.1.3 Analysis Approaches

Analysis approaches differ with respect to the orientation or starting point of the risk assessment, level of detail in the assessment, and how risks due to similar threat scenarios are treated. An analysis approach can be: (i) *threat-oriented*, starting with the identification of threat sources and threat events; (ii) *asset/impact-oriented*, starting with the identification of high-value assets or highly adverse impacts;[26] or (iii) *vulnerability-oriented*, starting with a set of predisposing conditions or exploitable weaknesses/deficiencies in organizational information systems or the environments in which the systems operate. Each orientation can potentially fail to notice (and hence determine) risks. Therefore, identification of risks from a second orientation (e.g., graph-based analysis, rigorous analysis) can improve the rigor and effectiveness of the analysis.

Graph-based analyses (e.g., functional dependency network analysis, attack tree analysis for adversarial threats, fault tree analysis for other types of threats) provide a way to use highly specific threat events to generate threat scenarios. Graph-based analyses can also provide ways to account for situations in which one event can change the likelihood of occurrence for another event. Attack and fault tree analyses, in particular, can generate multiple threat scenarios that are nearly alike, for purposes of determining the levels of risk. With automated modeling and simulation, large numbers of threat scenarios (e.g., attack and/or fault trees, traversals of functional dependency networks) can be generated. Thus, graph-based analysis approaches include ways to define a cut set[27] or reasonable subset of all possible threat scenarios.

A rigorous analysis approach provides an effective way to account for the many-to-many relationships between: (i) threat sources and threat events (i.e., a single threat event can be caused by multiple threat sources and a single threat source can cause multiple threat events); (ii) threat events and vulnerabilities (i.e., a single threat event can exploit multiple vulnerabilities and a single vulnerability can be exploited by multiple threat events); and (iii) threat events and impacts/assets (i.e., a single threat event can affect multiple assets or have multiple impacts, and a single asset can be affected by multiple threat events). A rigorous analysis approach also provides a way to account for whether, in the time frame for which risks are assessed, a specific adverse impact could occur (or a specific asset could be harmed) at most once, or perhaps repeatedly, depending on the nature of the impacts and on how organizations (including mission/business processes or information systems) recover from such adverse impacts.

Organizations can differ in the risk models, assessment approaches, and analysis approaches that they prefer for a variety of reasons. For example, cultural issues[28] can predispose organizations to employ risk models which assume a constant value for one or more possible risk factors, so that some factors that are present in other organizations' models are not represented. Culture can also predispose organizations to employ risk models that require detailed analyses using quantitative assessments (e.g., nuclear safety). Alternately, organizations may prefer qualitative or semi-quantitative assessment approaches. In addition to differences among organizations, differences can also exist within organizations. For example, organizations can use coarse or high-level risk models early in the system development life cycle to select security controls, and subsequently,

[26] A *Business Impact Analysis* (BIA) identifies high-value assets and adverse impacts with respect to the loss of integrity or availability. DHS Federal Continuity Directive 2 provides guidance on BIAs at the organization and mission/business process levels of the risk management hierarchy, respectively. NIST Special Publication 800-34 provides guidance on BIAs at the information system level of the risk management hierarchy.

[27] The term *cut set* is derived from the fact that the search tree or graph traversals are cut or pruned, limiting the number of viable choices.

[28] NIST Special Publication 800-39 describes how organizational culture affects risk management.

more detailed models to assess risk to given missions or business functions. Organizational risk frames[29] determine which risk models, assessment approaches, and analysis approaches to use under varying circumstances. Figure 3 illustrates the fundamental components in organizational risk frames (from the risk management process defined in NIST Special Publication 800-39) and the relationships among those components.

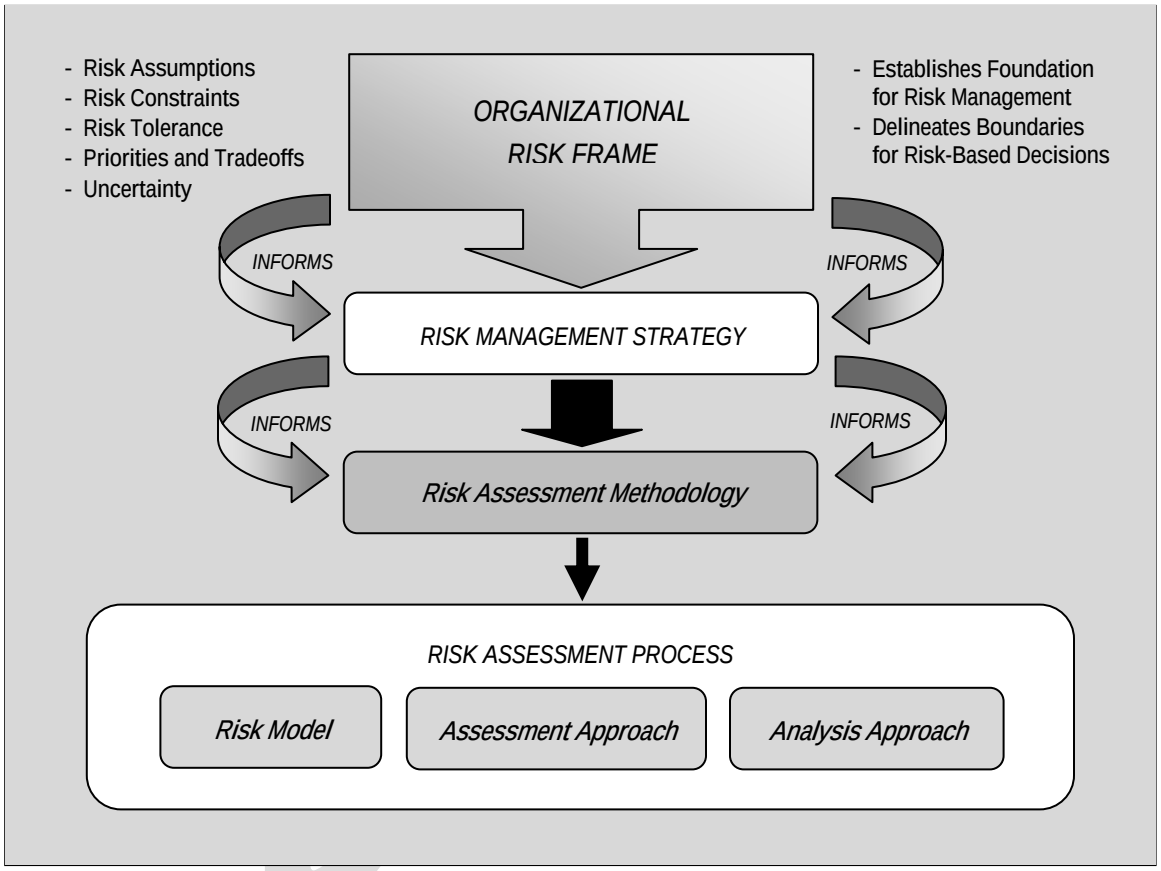

FIGURE 3: RELATIONSHIP AMONG RISK FRAMING COMPONENTS

[29] NIST Special Publication 800-39 defines an organization's risk frame as the set of assumptions, constraints, risk tolerances, priorities, and trade-offs that underpin the organization's risk management strategy—establishing a solid foundation for managing risk and bounding its risk-based decisions.

2.2 APPLICATION OF RISK ASSESSMENTS

As stated previously, risk assessments can be conducted at all three tiers in the risk management hierarchy—*organization level*, *mission/business process level*, and *information system level*. Figure 4 illustrates the risk management hierarchy defined in NIST Special Publication 800-39, which provides multiple risk perspectives from the strategic level to the tactical level. Traditional risk assessments generally focus at the Tier 3 tactical level (i.e., information system level) and as a result, tend to overlook other significant risk factors that may be more appropriately assessed at the Tier 1 or Tier 2 strategic levels.

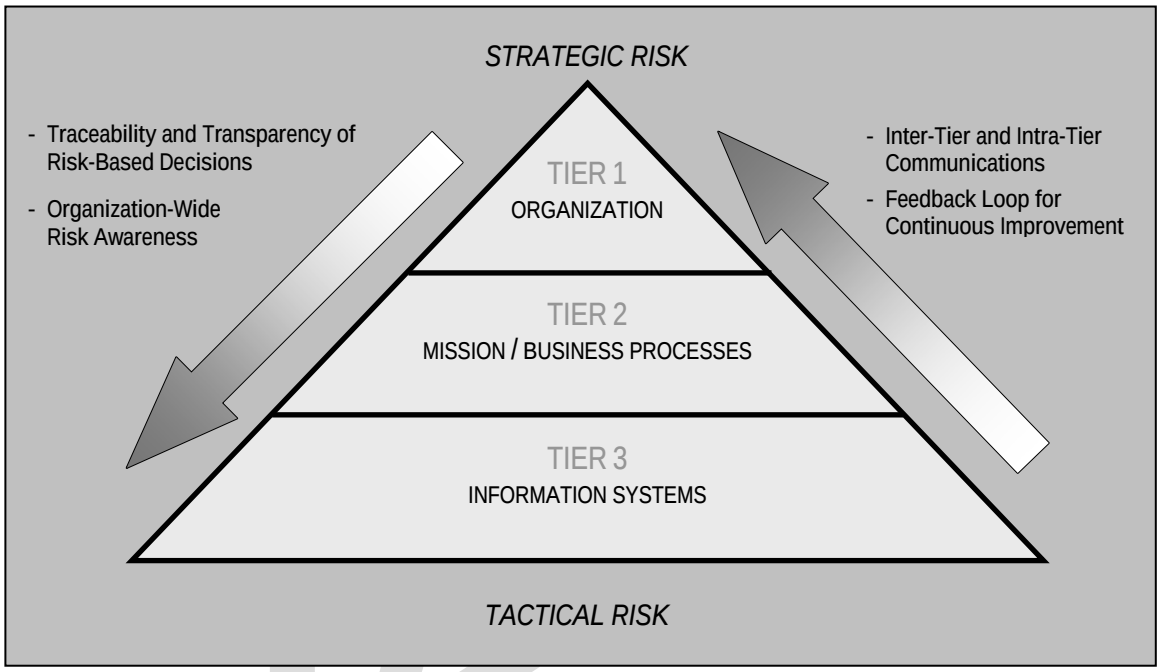

FIGURE 4: RISK MANAGEMENT HIERARCHY

Risk assessments support organizational risk response decisions at the different tiers of the risk management hierarchy. At Tier 1, risk assessments can affect, for example: (i) organization-wide information security programs, policies, procedures, and guidance; (ii) the types of appropriate risk responses (i.e., risk acceptance, avoidance, mitigation, sharing, or transfer); (iii) investment decisions for information technologies/systems; (iv) procurements; (v) minimum organization-wide security controls; (vi) conformance to enterprise/security architectures; and (vii) monitoring strategies and ongoing authorizations of information systems and common controls. At Tier 2, risk assessments can affect, for example: (i) enterprise architecture/security architecture design decisions; (ii) the selection of common controls; (iii) the selection of suppliers, services, and contractors to support core missions and business functions; (iv) the development of risk-aware mission/business processes; and (v) the interpretation of organizational security policies with respect to mission/business processes and operating environments. Finally, at Tier 3, risk assessments can affect, for example: (i) design decisions (including the selection, tailoring, and supplementation of security controls and the selection of information technology products for organizational information systems); (ii) implementation decisions (including whether specific information technology products or product configurations meet security control requirements); and (iii) operational decisions (including the requisite level of monitoring activity, the frequency of ongoing information system authorizations, and system maintenance decisions).

Risk assessments can also inform other risk management activities across the three tiers that are not security-related. For example, at Tier 1, risk assessments can provide useful inputs to: (i) operational risk determinations (including business continuity for organizational missions and business functions); (ii) organizational risk determinations (including financial risk, compliance risk, regulatory risk, reputation risk, and cumulative acquisition risk across large-scale projects); and (iii) multiple-impact risk (including supply chain risk and risk involving partnerships). At Tier 2, risk assessments can provide the same useful inputs to operational, organizational, and multiple-impact risks, specific to mission/business processes. At Tier 3, risk assessments can affect cost, schedule, and performance risks associated with information systems.

It is important to note that information security risk contributes to non-security risks at each tier. Thus, the results of a risk assessment at a given tier serve as inputs to, and are aligned with, non-security risk management activities at that tier. In addition, the results of risk assessments at lower tiers serve as inputs to risk assessments at higher tiers. Risks arise on different time scales, and risk response decisions can take effect in different timeframes. Therefore, risks are managed in different timeframes. In general, the risk management process moves most slowly at Tier 1 and most quickly at Tier 3. However, while Tier 1 decisions are often embodied in policy, which changes slowly, Tier 1 risks can lead to situations in which new vulnerabilities or cyber attacks are discovered and the implementation of an organization-wide mandate for mitigation requires immediate action.

2.2.1 Risk Assessments at the Organizational Tier

At Tier 1, risk assessments support organizational strategies, policies, guidance, and processes for managing risk. Risk assessments conducted at Tier 1 focus on organizational operations, assets, and individuals—comprehensive across mission/business lines. Organization-wide assessments of risk can be based solely on the assumptions, constraints, risk tolerances, priorities, and trade-offs established in the risk framing step (i.e., derived primarily from Tier 1 activities). However, more realistic and meaningful organization-wide risk assessments are based on assessments conducted across multiple mission/business lines (i.e., derived primarily from Tier 2 activities). The ability of organizations to use Tier 2 risk assessments as inputs to Tier 1 risk assessments is shaped by such considerations as: (i) the similarity of organizational missions/business functions; and (ii) the degree of autonomy that organizational entities or subcomponents have with respect to parent organizations. Centralized organizations with similar missions/business functions which take a common approach to all types of risk may choose to consolidate risk-related information into a comprehensive risk *dashboard*. Conversely, expert analysis may be needed to normalize the results from Tier 2 risk assessments in decentralized organizations with varied missions/business functions. Finally, risk assessments at Tier 1 take into consideration the identification of mission-essential functions from the organization's Continuity of Operations (COOP) plan when determining the contribution of Tier 2 risks. Risk assessment results at Tier 1 are communicated to organizational entities at Tier 2 and Tier 3.

2.2.2 Risk Assessments at the Mission/Business Process Tier

At Tier 2, risk assessments support the determination of mission/business process protection and resiliency requirements, and the allocation of those requirements to the enterprise architecture as part of mission/business segments (that support mission/business processes). This allocation is accomplished through an information security architecture embedded within the enterprise architecture. Tier 2 risk assessments also inform and guide decisions on whether, how, and when to use information systems for specific mission/business processes, in particular for alternative mission/business processing in the face of compromised information systems. Risk management and associated risk assessment activities at Tier 2 are closely aligned with the development of

Business Continuity Plans (BCPs). Tier 2 risk assessments focus on mission/business segments, which typically include multiple information systems, with varying degrees of criticality and/or sensitivity with regard to core organizational missions/business functions.[30] Risk assessment results at Tier 2 are communicated to and shared with organizational entities at Tier 3 to help inform and guide the allocation of security controls to information systems and the environments in which those systems operate. Tier 2 risk assessments also provide ongoing assessments of the security posture of organizational mission/business processes. Risk assessment results at Tier 2 are communicated to organizational entities at Tier 1 and Tier 3.

2.2.3 Risk Assessments at the Information System Tier

At Tier 3, the system development life cycle determines the purpose and defines the scope of risk assessments. Initial risk assessments evaluate the anticipated vulnerabilities and predisposing conditions affecting the confidentiality, integrity, and availability of organizational information systems in the context of the planned operational environment. Initial risk assessments conclude with recommendations for appropriate security controls—permitting mission/business owners to make the final decisions about the security controls necessary based on the security categorization and threat environment. Risk assessments are also conducted to assess information systems at later phases in the life cycle and update Risk Assessment Reports (RARs) from earlier phases. These reports for as-built or as-deployed information systems typically include descriptions of known vulnerabilities in the systems, an assessment of the risk posed by each, and corrective actions that can be taken to mitigate the risks. The reports also include an assessment of the overall risk to the organization and the information contained in the information systems by operating the systems as evaluated. Risk assessment results at Tier 3 are communicated to organizational entities at Tier 1 and Tier 2.

Risk assessments can also be conducted at each step in the Risk Management Framework (RMF), as defined in NIST Special Publication 800-37. The RMF, in its system life cycle approach, operates primarily at Tier 3 in the risk management hierarchy with some application at Tier 2, for example, in the selection of common controls. Risk assessments can be tailored to each step in the RMF as reflected in the purpose and scope of the assessments described in Section 3.1. The benefit of risk assessments conducted as part of the RMF can be realized from both initial assessments and from updated assessments, as described below.

Security Categorization

Organizations can use initial risk assessments to inform the worst-case impact analysis required to categorize organizational information and information systems as a preparatory step to security control selection.[31] Worst-case impact analyses from risk assessments can be used to define an upper bound on risk to organizational operations and assets, individuals, other organizations, and the Nation (i.e., for discrete risks without consideration for potential of risk aggregation).

Security Control Selection

Organizations can use risk assessments to inform and guide the selection of security controls for organizational information systems and environments of operation. Initial risk assessments can help organizations: (i) select appropriate baseline security controls; (ii) apply appropriate tailoring

[30] The criticality of information systems to organizational missions/business function may be identified in Business Impact Analyses.

[31] FIPS Publication 199 and CNSS Instruction 1253 provide guidance on security categorization of organizational information and information systems for the non national security and national security systems, respectively.

guidance to adjust the controls based on specific mission/business requirements, assumptions, constraints, priorities, trade-offs, or other organization-defined conditions; and (iii) supplement the controls based on specific and credible threat information. Threat data from risk assessments can provide critical information on adversary capabilities, intent, and targeting which may affect the decisions by organizations regarding the selection of additional security controls including the associated costs and benefits. Organizations also consider risk assessment results when selecting common controls (typically a Tier 2 activity) that provide one or more potential single points of failure because of security capabilities inherited by multiple information systems. Updated risk assessments can be used by organizations to modify current security control selections based on the most recent threat and vulnerability data available.

Security Control Implementation

Organizations can use the results from initial risk assessments to determine the most effective implementation of selected security controls (e.g., there may be potential inherent vulnerabilities associated with one type of security control implementation versus another). Certain information technology products, system components, or architectural configurations may be more susceptible to certain types of threat sources and are subsequently addressed during control development and implementation. In addition, the strength of security mechanisms employed by organizations can reflect threat data from risk assessments, thereby significantly increasing the overall resilience of organizational information systems. Individual configuration settings for information technology products and system components can also eliminate attack vectors determined during the analysis of threat events documented in the most current risk assessments. Initial risk assessments can also be employed to help inform decisions regarding the cost, benefit, and/or risk trade-offs in using one technology over another or how security controls are effectively implemented in particular environments of operation (e.g., when certain technologies are unavailable and compensating controls must be used). Updated risk assessments can be used to help determine if current security control deployments remain effective given changes to the threat space over time.

Security Control Assessments

Organizations can use the results from security control assessments (documented in security assessment reports) to identify any residual vulnerabilities in organizational information systems and/or the environments in which those systems operate. Partial/full failure of deployed security controls or the complete absence of planned controls represents potential vulnerabilities that can be exploited by threat sources. Organizations can use the results from initial or updated risk assessments to help determine the severity of such vulnerabilities which in turn, can guide and inform organizational risk responses (e.g., prioritizing vulnerabilities, sequencing risk response activities, establishing milestones for corrective actions). Risk assessments can also be used by organizations to determine the type of security assessments conducted during various phases of the system development life cycle, the frequency of assessments, the level of rigor applied during the assessments, the assessment methods used, and the number of objects assessed.

Security Authorization

Organizations can use the results of initial risk assessments and the results from updated risk assessments conducted during the previous steps in the RMF to provide important risk-related information to authorizing officials. The risk responses carried out by organizations based on the risk assessments conducted, result in known security states of organizational information systems and environments of operation. The residual risks determined from the risk assessments provide useful information needed by authorizing officials to make credible risk-based decisions on whether to operate those systems in the current security state or take actions to provide additional

safeguards or countermeasures—thereby reducing risk to organizational operations and assets, individuals, other organizations, or the Nation.

Security Control Monitoring

Organizations can update risk assessments on an ongoing basis by monitoring at an organization-defined frequency: (i) the *effectiveness* of security controls; (ii) *changes* to information systems and environments of operation; and (iii) *compliance* to federal legislation, regulations, directives, policies, standards, and guidance. The results from ongoing monitoring can provide information on new vulnerabilities which can be addressed through the risk assessment process in the same manner as described above. This illustrates the importance of employing risk assessments on an ongoing basis throughout the life cycle of the information systems that support core organizational missions/business functions.

2.2.4 Risk Communications and Information Sharing

In addition to preparing, conducting, and maintaining risk assessments, the manner and form in which risks are communicated across organizations is an expression of organizational culture. To be effective, communication of information security risks and related information needs to be consistent with other forms of risk communication within organizations. Similarly, the extent and form of risk-related information sharing is an expression of organizational culture, as well as legal, regulatory, and contractual constraints. To maximize the benefit of risk assessments, organizations should establish policies, procedures, and implementing mechanisms (including, for example, Security Content Automation Protocols),[32] to ensure that appropriate information produced during risk assessments is effectively communicated and shared across all three tiers in the Risk Management Hierarchy to reinforce the importance of risk communication and information sharing within organizations. The input tables in Appendices D, E, F, G, H, and I (i.e., for threat sources, threat events, vulnerabilities and predisposing conditions, likelihood, impact, and risk) provide recommendations for inter-tier risk communication/sharing.

STRATEGIC VIEW OF RISK ASSESSMENTS

Risk assessments should not be viewed simply as one-time activities that provide total information for decision makers to guide and inform potential responses to risks from relevant threat sources. Rather, risk assessments should be viewed as important tools in the arsenal of risk management tools that are available to organizations and employed on an ongoing basis throughout the system development life cycle—with the frequency of the assessments and the resources applied during the assessments, commensurate with the expressly defined purpose and scope of the assessments. Risk assessments are about developing information for decision makers that can be effectively used to support credible risk-based decisions throughout the life cycle of the information systems supporting the core missions and business functions of organizations. In the end, risk assessment address the potential adverse affects to organizational operations (including missions, functions, image and reputation), critical assets, individuals, other organizations in partnering relationships, and the economic and national security interests of the United States, that arise from the operation and use of organizational information systems and the information processed, stored, and transmitted by those systems.

[32] NIST Special Publication 800-70 provides guidance on the Security Content Automation Protocol (SCAP) program. In addition to the automated testing, evaluation, and assessment characteristics associated with SCAP, the protocols also establish common naming conventions for information security activities which promote enhanced communication and information sharing of risk-related information internally within organizations and externally among organizations.

CHAPTER THREE

THE PROCESS

CONDUCTING RISK ASSESSMENTS WITHIN ORGANIZATIONS

This chapter describes the process of assessing information security risk including: (i) a high-level overview of the risk assessment process; (ii) the activities necessary to prepare for risk assessments; (iii) the activities necessary to conduct effective risk assessments; and (iv) the activities necessary to maintain the results of risk assessments on an ongoing basis. The risk assessment process[33] is divided into three general steps: (i) *prepare*; (ii) *conduct*; and (iii) *maintain*.[34] Each step is further divided into a set of tasks that organizations carry out to complete the step. For each task, supplemental guidance provides additional information for organizations and individuals conducting risk assessments. Risk tables and exemplary assessment scales are listed in appropriate tasks and cross-referenced to more detailed information in the supporting appendices. Figure 5 illustrates the basic steps in the risk assessment process and the tasks associated with the steps.

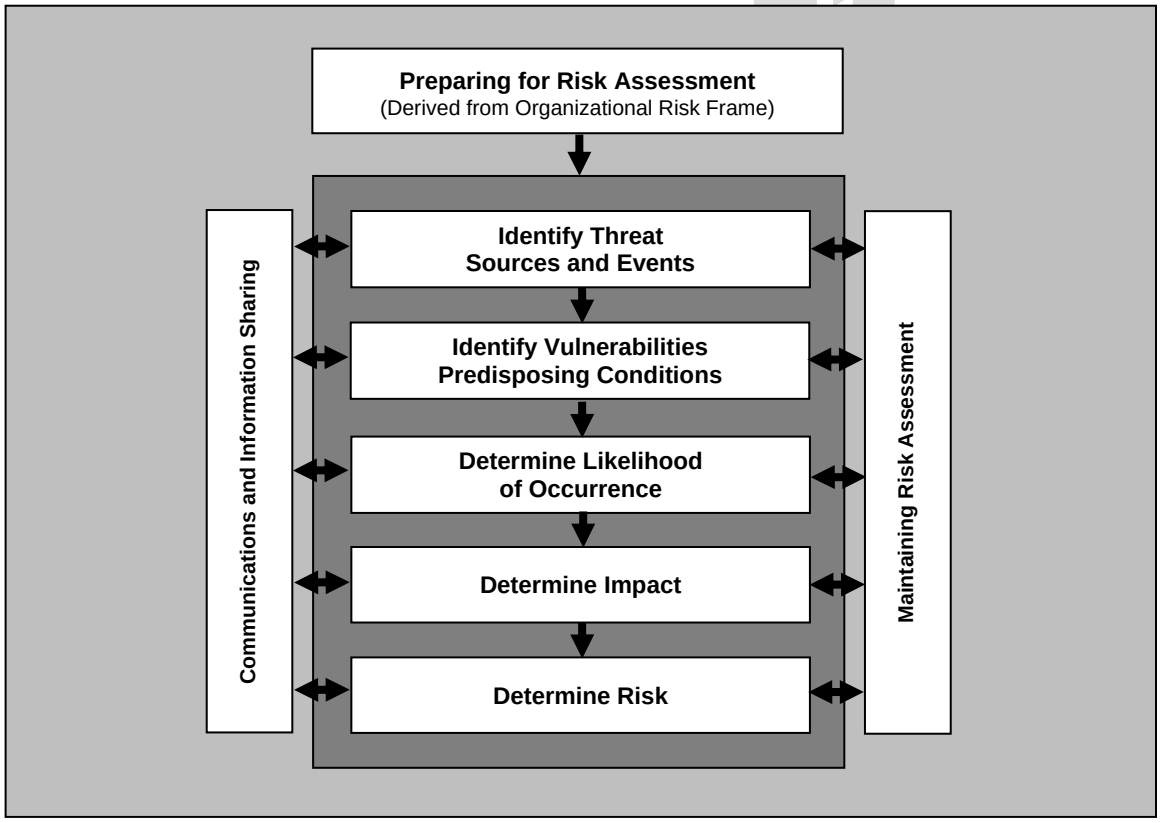

FIGURE 5: RISK ASSESSMENT PROCESS

[33] The intent of process description in Chapter Three (and summarized in Figure 5) is to provide a common expression of the essential elements of an effective risk assessment process. It is not intended to prescribe a specific procedure for accomplishing risk assessments or limit organizational flexibility in conducting those assessments. Other procedures can be implemented if organizations choose to do so, provided the intent of the process description is achieved.

[34] The three-step risk assessment process described in this publication is consistent with the general risk assessment process described in NIST Special Publication 800-39. The additional steps and tasks result from the need to provide more detailed guidance to effectively carry out the specific activities associated with risk assessments.

3.1 PREPARING FOR THE RISK ASSESSMENT

The first step in the risk assessment process is to *prepare* for the assessment. The objective of this step is to establish a context for the risk assessment. This context is established and informed by the risk management strategy of the organization, developed during the risk framing step of the risk management process. The strategy includes, for example, information regarding policies and requirements for conducting risk assessments, specific assessment methodologies to be employed, procedures for selecting risk factors to be considered, scope of the assessments, rigor of analyses, degree of formality, and requirements that facilitate consistent and repeatable risk determinations across the organization. Preparing for risk assessments includes the following specific tasks:

- Identifying the purpose, scope, assumptions, and constraints associated with the assessment;
- Identifying the sources of information to be used as inputs to the assessment; and
- Defining or refining the risk model.

STEP 1: PREPARE FOR THE ASSESSMENT

IDENTIFY PURPOSE

TASK 1-1: Identify the purpose of the risk assessment in terms of the information the assessment is intended to produce and the decisions the assessment is intended to support.

Supplemental Guidance: The purpose of the risk assessment is explicitly stated in sufficient detail in order to fully inform and guide the conduct of the assessment to ensure that the purpose is achieved. The purpose of the risk assessment is influenced by whether the assessment is: (i) an initial assessment; or (ii) an updated assessment initiated from the risk response or risk monitoring steps in the risk management process. For an initial assessment, the purpose can include, for example: (i) establishing a baseline assessment of risk; or (ii) identifying threats and vulnerabilities, impacts to organizational operations and assets, individuals, other organizations, and the Nation, and other risk factors to be monitored or tracked over time as part of risk monitoring. For a reassessment initiated from the risk response step, the purpose can include, for example, recommending (or providing a comparative analysis of) alternative risk response courses of action. Alternatively, for a reassessment initiated from the risk monitoring step, the purpose can include, for example, updating the risk assessment based on: (i) ongoing determinations of the effectiveness of security controls in organizational information systems or environments of operation; (ii) changes to organizational information systems or environments of operation (e.g., changes to hardware, firmware, software; changes to system-specific, hybrid, or common controls,; changes to mission/business processes, common infrastructure and support services, threats, vulnerabilities, or facilities); and (iii) results from compliance verification activities.

IDENTIFY SCOPE

TASK 1-2: Identify the scope of the risk assessment in terms of organizational applicability, time frame supported, and architectural/technology considerations.

Supplemental Guidance: The scope of the risk assessment determines the boundary of the assessment and can include one or more tiers in the risk management hierarchy as described in NIST Special Publication 800-39. Risk assessment scope affects the range of information available to make risk-based decisions and is determined by the organizational official requesting the assessment. Establishing the scope of risk assessments helps organizations determine: (i) what tiers are addressed in risk assessments; (ii) what parts of organizations are affected by risk assessments and how are they affected; (iii) what decisions risk assessment results support; (iv) how long risk assessment results are relevant; and (v) what influences the need to update risk assessments.

Organizational Applicability

Organizational applicability describes which parts of the organization or sub-organizations are affected by the risk assessment and the risk-based decisions resulting from the assessment (including the parts of the organization/sub-organizations responsible for implementing the activities and tasks related to the decisions). For example, the risk assessment can inform decisions regarding information systems supporting a particular organizational mission/business function or mission/business process. This can include decisions regarding the selection, tailoring, or supplementation of security controls for specific information systems or the selection of common controls. Alternatively, the risk assessment can inform decisions regarding a set of closely related missions/business functions or mission/business processes. The scope of the risk assessment can include not only the missions/business functions, mission/business

processes, common infrastructure, or shared services on which the organization currently depends, but also those which the organization might use under specific operational conditions.

Effectiveness Time Frame

Organizations determine how long the results of particular risk assessments can be used to legitimately inform risk-based decisions. The time frame is usually related to the purpose of the assessment. For example, a risk assessment to inform Tier 1 policy-related decisions needs to be relevant for an extended period of time since the governance process for policy changes can be time-consuming in many organizations. A risk assessment conducted to inform a Tier 3 decision on the use of a compensating security control for an information system may be relevant only until the next release of the information technology product providing the required security capability. Organizations determine the useful life of risk assessment results and under what conditions the current assessment results become ineffective or irrelevant. Risk monitoring can be used to help determine effectiveness time frames for risk assessments.

Architectural/Technology Considerations

Organizations determine the types of system architectures, information systems, and environments of operation to which risk assessments and the resulting risk-based decisions apply. For example, a risk assessment can be used to inform decisions regarding command and control systems in fixed, land-based facilities. A risk assessment can also be used to inform decisions regarding industrial/process control systems supporting nuclear power plant operations, a service-oriented architecture supporting a just-in-time logistics operation, or mobile/wireless technologies supporting first responders.

IDENTIFY ASSUMPTIONS AND CONSTRAINTS

TASK 1-3: Identify the specific assumptions and constraints under which the risk assessment is conducted.

Supplemental Guidance: Organizations provide direction for the assumptions and constraints that guide and inform risk assessments. By making assumptions explicit and providing realistic constraints, there is greater clarity in the risk model selected for the risk assessment, increased reproducibility/repeatability of assessment results, and an increased opportunity for reciprocity among organizations. Organizations identify assumptions and provide guidance in several areas including, for example: (i) threat sources; (ii) threat events; (iii) vulnerabilities/predisposing conditions; (iv) impacts; and (v) assessment and analytic approaches. Organizations identify constraints in several areas including, for example: (i) resources available for the risk assessment; (ii) skills and expertise required for the risk assessment; and (iii) operational considerations related to mission/business activities. Assessments of threats and impacts, for example, can range from worst-case projections to best-case projections or anything in between those endpoints. Organizations also consider the uncertainty with regard to any assumptions made or any other information related to or used in risk assessments. Uncertainty in assumptions can affect organizational risk tolerance. For example, assumptions based on a lack of specific and/or credible information may reduce an organization's risk tolerance because of the inherent uncertainty influencing the assumptions. The following sections provide some representative examples of areas where assumptions/constraints for risk assessments are needed and appropriate.

Threat Sources

Organizations determine which types of threat sources are to be considered during risk assessments. Risk assessments can address all types of threat sources, a single broad threat source (e.g., adversarial), or a specific threat source (e.g., trusted insider). Table D-2 provides a sample taxonomy of threat sources that can be considered by organizations in identifying assumptions for risk assessments. See Task 2-1 for additional guidance on identifying threat sources.

Threat Events

Organizations determine the level of detail in describing threat events that are to be considered during risk assessments. Descriptions of threat events can be expressed in highly general terms (e.g., phishing, distributed denial-of-service), in more descriptive terms using tactics, techniques, and procedures, or highly specific terms (e.g., the names of specific information systems, technologies, organizations, roles, or locations). In addition, organizations consider: (i) what representative set of threat events can serve as a starting point for the identification of the specific threat events in the risk assessment; and (ii) what degree of confirmation is needed for threat events to be considered relevant for purposes of the risk assessment. For example, organizations may consider only those threat events that have been observed (either internally or by organizations that are peers/partners) or all possible threat events. Table E-2 and Table E-3 provide representative examples of adversarial and non-adversarial threat events. See Task 2-2 for additional guidance on identifying threat events.

Vulnerabilities and Predisposing Conditions

Organizations determine the types of vulnerabilities that are to be considered during risk assessments and the level of detail provided in the vulnerability descriptions. Vulnerabilities can be associated with organizational information systems (e.g., hardware, software, firmware, internal controls, and security procedures) or the environments in which those systems operate (e.g., organizational governance, external relationships, mission/business processes, enterprise

architectures, information security architectures). Organizations also determine the types of predisposing conditions that are to be considered during risk assessments. Table F-4 provides representative examples of such predisposing conditions. See Task 2-3 for additional guidance on identifying vulnerabilities and predisposing conditions.

Impacts

Organizations determine potential adverse impacts in terms of organizational operations (i.e., missions, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. Organizations address impacts at a level of detail that includes, for example, specific mission/business processes or information resources (e.g., information, personnel, equipment, funds, and information technology). Organizations may include information from Business Impact Analyses with regard to providing impact information for risk assessments. Table H-2 provides representative examples of types of impacts (i.e., harm) that can be considered by organizations. See Task 2-4 for additional guidance on identifying potential adverse impacts.

Risk Tolerance and Uncertainty

Organizations determine the levels of risk, types of risk, and degree of risk uncertainty that are acceptable. Of particular concern is how organizations analyze and determine risks when a high degree of uncertainty exists. This is especially important when organizations consider advanced persistent threats since assessments of the likelihood of threat event occurrence can have a great degree of uncertainty. Organizations can take a variety of approaches to determine likelihood, ranging from assuming the worst-case likelihood (certain to happen sometime in the foreseeable future) to assuming that if an event has not been observed, it is unlikely to happen. Organizations also determine what levels of risk (combination of likelihood and impact) indicate that no further analysis of any risk factors is needed.

Analytic Approach

Organizations determine the degree of detail or in what form, threats are analyzed including the level of granularity to describe threat events or threat scenarios. Different analysis approaches are possible, including, for example, event/TTP coverage analysis, attack tree/threat scenario analysis, and layers of protection analysis. Different analysis approaches can lead to different levels of detail in characterizing the adverse events for which likelihoods are determined. For example, an adverse event could be characterized in several ways (with increasing levels of detail): (i) a threat event (for which the likelihood is determined by taking the maximum overall threat sources; (ii) a pairing of a threat event and a threat source; or (iii) a detailed threat scenario/attack tree. In general, organizations can be expected to require more detail for highly critical mission/business functions, common infrastructures, or shared services on which multiple missions or business functions depend (as common points of failure), and information systems with high criticality or sensitivity. Mission/business owners may amplify this guidance for risk *hot spots* (information systems, services, or critical infrastructure components of particular concern) in mission/business segments.

IDENTIFY INFORMATION SOURCES

TASK 1-4: Identify the sources of threat, vulnerability, and impact information to be used in the risk assessment.

Supplemental Guidance: Sources of threat information as described in Tables D-1, E-1, F-1, G-1, H-1, and I-1) can be either internal or external to organizations. Internal sources can provide insights into specific threats to organizations and can include, for example, incident reports, security logs, trouble tickets, and monitoring results. Mission/business owners are encouraged to identify not only common infrastructure and/or support services they depend on, but also those they might use under specific operational circumstances. External sources of threat information can include cross-community organizations (e.g., US Computer Emergency Readiness Team [US-CERT]), sector partners (e.g., Defense Industrial Base [DIB] using the DoD-Defense Industrial Base Collaborative Information Sharing Environment [DCISE], Information Sharing and Analysis Centers [ISACs] for critical infrastructure sectors), research and nongovernmental organizations (e.g. Carnegie Mellon University, Software Engineering Institute-CERT), and security service providers). Organizations using external sources, consider the timeliness, specificity, and relevance of threat information. Similar to sources of threat information, sources of vulnerability information can also be either internal or external to organizations. Internal sources can provide insights into specific vulnerabilities to organizations and can include, for example, security assessment reports, vulnerability assessment reports, risk assessment reports, incident reports, security logs, trouble tickets, and monitoring results. External sources of vulnerability information are similar to those sources identified above for threat information. Sources of impact information can include, for example, mission/business impact analyses and asset inventories, and FIPS Publication 199 security categorizations.

DEFINE RISK MODEL

TASK 1-5: Define (or refine) the risk model to be used in the risk assessment.

Supplemental Guidance: Organizations define one or more risk models for use in conducting risk assessments (see Section 2.1.1). To facilitate reciprocity of risk assessment results, organization-specific risk models include (or can be translated into) the risk factors defined in the appendices. For each assessable risk factor, the appendices include three

assessment scales with correspondingly different representations. Organizations typically define (or select and tailor from the appendices), the assessment scales to be used in their risk assessments, annotating with common anchoring examples for specific values and defining break points between bins for semi-quantitative approaches. In addition, mission/business owners can provide further annotations with mission/business-specific examples.

Summary of Key Activities – Preparing for Risk Assessments

- Identify the ***purpose*** of the risk assessment.
- Identify the ***scope*** of the risk assessment.
- Identify the ***assumptions*** and ***constraints*** under which the risk assessment is conducted.
- Identify ***sources*** of threat, vulnerability, and impact information to be used in the risk assessment.
- Define or refine the ***risk model*** to be used in the risk assessment.

3.2 CONDUCTING THE RISK ASSESSMENT

The second step in the risk assessment process is to *conduct* the assessment. The objective of this step is to produce a list of information security risks that can be prioritized by risk level and used to inform risk response decisions. To accomplish this objective, organizations analyze threats and vulnerabilities, impacts and likelihood, and the uncertainty associated with the risk assessment process. This step also includes the gathering of essential information as a part of each task and is conducted in accordance with the assessment context established in the initial step of the risk assessment process. The expectation for risk assessments is to adequately cover the entire threat space in accordance with the specific definitions, guidance, and direction established during the initial step. However, in practice, adequate coverage within available resources may dictate generalizing threat sources, threat events, and vulnerabilities to ensure full coverage and assessing specific, detailed sources, events, and vulnerabilities only as necessary to accomplish risk assessment objectives. Conducting risk assessments includes the following specific tasks:

- Identifying threat sources that are relevant to organizations and the threat events that could be produced by those sources;
- Identifying vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation;
- Determining the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful;
- Determining the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events); and
- Determining information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.

The specific tasks are presented in a sequential manner for clarity. However, in practice, some iteration among the tasks is both necessary and expected.[35] Depending on the purpose of the risk assessment, risk assessors may find reordering the tasks advantageous.[36] Whatever adjustments risk assessors make to the tasks described below, risk assessments should meet the stated purpose, scope, and assumptions established by the organizations initiating the assessments.

[35] For example, as vulnerabilities are identified, additional threat events might be identified by asking how the threat events could exploit the newly identified vulnerabilities. If risk assessors identify vulnerabilities first and then define threat events, they may find some threat events that do not map cleanly to vulnerabilities but do map to predisposing conditions.

[36] For example, the risk assessment could start with an identification of mission/business impacts at Tiers 1 and 2 using common techniques such as Mission Impact Analyses, Business Impact Analyses, Mission/Business Thread Analyses, or Business Continuity Analyses. The results of such analyses could enable risk assessors to focus attention on, and perform more detailed analysis of, potential threats to critical information systems, databases, communications links, or other assets.

STEP 2: CONDUCT THE ASSESSMENT

IDENTIFY THREAT SOURCES

TASK 2-1: Identify and characterize the threat sources of concern to the organization, including the nature of the threats and for adversarial threats, capability, intent, and targeting characteristics.

Supplemental Guidance: Organizations identify threat sources of concern and determine the characteristics associated with those threat sources. Certain characteristics (e.g., capabilities, intentions, and targeting) may define specific types of threat sources to be addressed. For threat sources identified by type or by name, the characteristics associated with the threat sources are also identified. The prepare step for the risk assessment includes organizational direction and guidance for conducting threat source identification and characterization including, for example: (i) sources for obtaining threat information; (ii) threat sources to consider (by type/name); (iii) threat taxonomy to be used; and (iv) process for identifying which threat sources are of concern for the risk assessment. Organizations make explicit any assumptions concerning threat sources including decisions regarding the identification of threat sources when specific and credible threat information is unavailable. The identification and characterization of Advanced Persistent Threats (APTs) can involve considerable uncertainty. Organizations annotate such threat sources with appropriate rationale and references (and providing classifications as necessary).

Appendix D provides a set of exemplary tables for use in identifying threat sources:

- Table D-1 provides a set of exemplary inputs to the threat source identification task;
- Table D-2 provides an exemplary taxonomy that can be used to identify and characterize threat sources;
- Tables D-3, D-4, and D-5 provide exemplary assessment scales to assess the risk factors (i.e., characteristics) of adversarial threat sources with regard to capability, intent, and targeting;
- Table D-6 provides an exemplary assessment scale for assessing the ranges of effects from threat events initiated by non-adversarial threat sources; and
- Tables D-7 and D-8 provide templates for summarizing and documenting the results of threat source identification and characterization.

If a particular type of threat source is outside the scope of the risk assessment or not relevant to the organization, the information in Tables D-7 and D-8 can be truncated accordingly. The information produced in Task 2-1 provides threat source inputs to the risk tables in Appendix I.

Summary Key Activities – Task 2-1

- Use **Table D-1** for threat source inputs.
- Use **Table D-2**, as extended or modified by the organization, to identify threat sources, updating **Table D-7** (adversary threat sources) and **Table D-8** (non-adversary threat sources).
- Use **Table D-1**, as extended or modified by the organization, to determine if threat sources are relevant to the organization (i.e., threat sources in scope), updating **Table D-7** (adversary threat sources) and **Table D-8** (non-adversary threat sources).
- For relevant adversary threat sources:
  - Use assessment scale in **Table D-3**, as extended or modified by the organization, to assess adversary capability, updating **Table D-7**.
  - Use assessment scale in **Table D-4**, as extended or modified by the organization, to assess adversary intent, updating **Table D-7**.
  - Use assessment scale in **Table D-5**, as extended or modified by the organization, to assess adversary targeting, updating **Table D-7**.
- For relevant non-adversarial threat sources:
  - Use assessment scale in **Table D-6**, as extended or modified by the organization, to assess the range of effects from threat sources, updating **Table D-8**.

IDENTIFY THREAT EVENTS

TASK 2-2: Identify potential threat events, relevance to the organization, and the threat sources that could initiate the events.

Supplemental Guidance: Threat events are characterized by the threat sources that could initiate the events, and for adversarial events, the tactics, techniques, and procedures used to carry out attacks. Organizations define these threat events with sufficient detail to accomplish the purpose of the risk assessment. Multiple threat sources can initiate a single threat event. Conversely, a single threat source can initiate multiple threat events. Therefore, there can be a many-to-many relationship between threat events and threat sources which can potentially increase the complexity of the analysis and the risk assessment. Organizations tailor the general descriptions of threat events to identify how each event could potentially harm organizational operations (including mission, functions, image, or reputation) and assets, individuals, other organizations, or the Nation. For non-adversarial threat events, organizations use the range of effects to identify the affected operations, assets, or individuals (see Task 2-5). For adversarial threat events, organizations use the event description and adversary targeting and intent to identify the affected operations, assets, or individuals. For each threat event identified, organizations determine the relevance of the event. Table E-4 provides a range of values for relevance of threat events. The values selected by organizations have a direct linkage to organizational risk tolerance. The more risk averse, the greater the range of values considered. Organizations accepting greater risk or having a greater risk tolerance are more likely to require substantive evidence before giving consideration to threat events. If a threat event is deemed to be irrelevant, no further consideration is given. For relevant threat events, organizations identify all potential threat sources that could initiate the events. Organizations can identify each pairing of threat source and threat event separately since the likelihood of threat initiation and success could be different for each pairing. Alternatively, organizations can assess likelihoods by considering the set of all possible threat sources that could potentially initiate a threat event. Organizations make explicit any assumptions and decisions when identifying threat events. Organizations also make explicit the process used for identifying threat events and the information sources used to identify the events. Finally, organizations capture information to support the determinations of uncertainty.

Appendix E provides a set of exemplary tables for use in identifying threat events:

- Table E-1 provides a set of exemplary inputs to the threat event identification task;
- Table E-2 provides representative examples of adversarial threat events expressed as TTPs;
- Table E-3 provides representative examples of non-adversarial threat events;
- Table E-4 provides exemplary values for the relevance of threat events to organizations; and
- Table E-5 provides a template for summarizing and documenting the results of threat event identification.

The information produced in Task 2-2 provides threat event inputs to the risk tables in Appendix I.

Summary of Key Activities – Task 2-2

- Use **Table E-1** for threat event inputs.
- Use **Table E-2** (adversary threat events) and **Table E-3** (non-adversary threat events) as extended or modified by the organization, to identify threat events, updating **Table E-5**.
- Use **Table D-7** and **Table D-8**, as extended or modified by the organization, to identify threat sources that could initiate the threat events, updating **Table E-5**.
- Use assessment scale in **Table E-4**, as extended or modified by the organization, to assess the relevance of threat events to the organization, updating **Table E-5**.
- Use **Table E-5** and **Table D-7** to update Columns 1-6 in **Table I-5** (adversary risk).
- Use **Table E-5** and **Table D-8** to update Columns 1-4 in **Table I-7** (non-adversary risk).

IDENTIFY VULNERABILITIES AND PREDISPOSING CONDITIONS

TASK 2-3: Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts to the organization.

Supplemental Guidance: The primary purpose of vulnerability assessments is to understand the nature and degree to which organizations, mission/business processes, and information systems are vulnerable to threat sources identified in Task 2-1 and the threat events identified in Task 2-2 that can be initiated by those threat sources. There is potentially a many-to-many relationship between threat events and vulnerabilities. Multiple threat events can exploit a single vulnerability, and conversely, multiple vulnerabilities can be exploited by a single threat event. Vulnerabilities can be identified at varying degrees of granularity and specificity. The level of detail provided in any particular vulnerability assessment is consistent with the purpose of the risk assessment and the type of inputs needed to support follow-on likelihood and impact determinations. Many risk assessments tend to rely on threat-vulnerability pairs as the focal point of the assessments. However, due to the ever-increasing complexity within organizations, mission/business processes, and the information systems supporting those processes, the number of vulnerabilities tends to be large. Therefore, the vulnerability identification task is used to understand the general nature of the vulnerabilities (including scope, number, and type) relevant to the assessment (see Task 1-3) and performing a cataloging of specific vulnerabilities as necessary to do so. Organizations determine which vulnerabilities are relevant to which threat events in order to reduce the space of potential risks to be assessed. Organizations also make explicit: (i) the process used to conduct vulnerability assessments; (ii) assumptions related to the assessments; (iii) credible sources and methods for obtaining vulnerability information; and (iv) the process/rationale for the conclusions reached as to how vulnerable organizations are to the identified threat events of concern. And finally, organizations capture information to support determination of uncertainty. In addition to identifying vulnerabilities, organizations also identify any predisposing conditions which may affect susceptibility to certain vulnerabilities. Predisposing conditions that exist within organizations (including mission/business processes, information systems, and environments of operation) can contribute to (i.e., increase or decrease) the likelihood that one or more threat events, once initiated by threat sources, result in adverse impacts to organizational operations, organizational assets, individuals, other organizations, or the Nation. Organizations determine which predisposing conditions are relevant to which threat events in order to reduce the space of potential risks to be assessed.

Appendix F provides a set of exemplary tables for use in identifying vulnerabilities and predisposing conditions:

- Table F-1 provides a set of exemplary inputs to the vulnerability and predisposing condition identification task;
- Table F-2 provides an exemplary assessment scale for assessing the severity of identified vulnerabilities;
- Table F-3 provides a template for summarizing/documenting the results of vulnerability identification;
- Table F-4 provides an exemplary taxonomy that can be used to identify and characterize predisposing conditions;
- Table F-5 provides an exemplary assessment scale for assessing the pervasiveness of predisposing conditions; and
- Table F-6 provides a template for summarizing/documenting the results of identifying predisposing conditions.

The information produced in Task 2-3 provides vulnerability and predisposing condition inputs to the risk tables in Appendix I.

Summary of Key Activities – Task 2-3

- Use **Table F-1** for vulnerability and predisposing condition inputs.
- Use organization-defined information sources to identify vulnerabilities, updating **Table F-3**.
- Use assessment scale in **Table F-2**, as extended or modified by the organization, to assess the severity of identified vulnerabilities, updating **Table F-3**.
- Use **Table F-4**, as extended or modified by the organization, to identify predisposing conditions, updating **Table F-6**.
- Use assessment scale in **Table F-5**, as extended or modified by the organization, to assess the pervasiveness of predisposing conditions, updating **Table F-6**.
- Use **Table F-3** and **Table F-6** to update Column 8 in **Table I-5** (adversary risk) and Column 6 in **Table I-7** (non-adversary risk), as appropriate.

DETERMINE LIKELIHOOD

TASK 2-4: Determine the likelihood that threat events of concern result in adverse impacts to the organization, considering: (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities and predisposing conditions identified; and (iii) organizational susceptibility reflecting safeguards/countermeasures planned or implemented to impede such events.

Supplemental Guidance: Organizations employ a three-step process to determine the overall likelihood of threat events. First, organizations assess the likelihood that threat events will be initiated (for adversarial threat events) or will occur (for non-adversarial threat events). Second, organizations assess the likelihood that threat events once initiated or occurring, will result in adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Finally, organizations assess the overall likelihood as a combination of likelihood of initiation/occurrence and likelihood of resulting in adverse impact. Organizations also make explicit: (i) the process used to conduct likelihood determinations; (ii) assumptions related to the determinations; (iii) credible sources/methods for obtaining likelihood information; and (iv) the rationale for the conclusions reached with regard to the likelihood determinations. And finally, organizations capture information to support determination of uncertainty.

Appendix G provides a set of exemplary tables for use in determining likelihood of threat events:

- Table G-1 provides a set of exemplary inputs to the likelihood determination task;
- Table G-2 provides an exemplary assessment scale for assessing the likelihood of adversarial threat events;
- Table G-3 provides an exemplary assessment scale for assessing the likelihood of non-adversarial threat events occurring;
- Table G-4 provides an exemplary assessment scale for assessing the likelihood of threat events having adverse impacts if the events are initiated (adversarial) or occur (non-adversarial); and
- Table G-5 provides an exemplary assessment scale for assessing the overall likelihood of threat events (i.e., a combination of the likelihood of initiation/occurrence and the likelihood of impact).

Organizations assess the likelihood of threat event initiation by taking into consideration the characteristics of the threat sources of concern including capability, intent, and targeting (see Task 2-1 and Appendix D). If threat events require more capability than adversaries possess (and adversaries are cognizant of this fact), then the adversaries are not expected to initiate the events. If adversaries do not expect to achieve intended objectives by executing threat events, then the adversaries are not expected to initiate the events. And finally, if adversaries are not actively targeting specific organizations or their mission/business functions, adversaries are not expected to initiate threat events. Organizations can use the assessment scale in Table G-2 and provide a rationale for the assessment allowing explicit consideration of deterrence and threat shifting. Threat shifting is the response of adversaries to perceived safeguards, countermeasures, or obstructions, in which adversaries change some characteristic of their intent to do harm in order to avoid and/or overcome those safeguards, countermeasures, or obstacles. Threat shifting can occur in one or more domains including: (i) the time domain (e.g., a delay in attack or illegal entry to conduct additional surveillance, etc.); (ii) the target domain (selecting a different, less-protected target); (iii) the resource domain (e.g., adding resources to the attack in order to reduce uncertainty or overcome countermeasures); or (iv) the attack planning/attack method domain (e.g., changing the attack weapon or attack path). Threat shifting is a natural consequence of a dynamic set of interactions between threat sources and asset types targeted. With more sophisticated threat sources, it also tends to default to the path of least resistance to exploit particular vulnerabilities and the responses are not always predictable. In addition to the safeguards and countermeasures applied and the impact of a successful exploit of an organizational vulnerability, another influence on threat shifting is the benefit to the attacker. That perceived benefit on the attacker side can also influence how much/when threat shifting occurs. Organizations can assess the likelihood of threat event occurrence (non-adversarial) using Table G-3 and provide a similar rationale for the assessment.

Organizations assess the likelihood that threat events result in adverse impacts by taking into consideration the set of identified vulnerabilities and predisposing conditions (see Task 2-3 and Appendix F). For threat events initiated by adversaries, organizations consider characteristics of associated threat sources. For non-adversarial threat events, organizations take into account the anticipated severity and duration of the event (as included in the description of the event). Organizations can use the assessment scale in Table G-4 and provide a rationale for the assessment allowing explicit consideration as stated above. Threat events for which no vulnerabilities or predisposing conditions are identified, have a very low likelihood of resulting in adverse impacts. Such threat events can be highlighted and moved to the end of the table (or to a separate table), so that they can be tracked for consideration in follow-on risk assessments. However, no further consideration during the current assessment is warranted.

The *overall likelihood* of a threat event is a combination of: (i) the likelihood that the event will occur (e.g., due to human error or natural disaster) or be initiated by an adversary; and (ii) the likelihood that the initiation/occurrence will result in adverse impacts. Organizations assess the overall likelihood of threat events by using inputs from Tables G-2, G-3 and G-4. Any specific algorithm or rule for combining the determined likelihood values depends on: (i) general

organizational attitudes toward risk, including overall risk tolerance and tolerance for uncertainty; (ii) specific tolerances toward uncertainty in different risk factors; and (iii) organizational weighting of risk factors. For example, organizations could use any of the following rules (or could define a different rule): (i) use the maximum of the two likelihood values; (ii) use the minimum of the two likelihood values; (iii) consider likelihood of initiation/occurrence only, assuming that if threat events are initiated or occur, the events will result in adverse impacts; (iv) consider likelihood of impact only, assuming that if threat events could result in adverse impacts, adversaries will initiate the events; or (v) take a weighted average of the two likelihood values.

Threat-vulnerability pairing is undesirable when analyzing and assessing likelihood at the mission/business function level, and in many cases, is deprecated even at the information system level. This analysis approach typically drives the level of detail in identifying threat events and vulnerabilities, rather than allowing organizations to make effective use of sources of threat information and/or to identify threats at a level of detail that is meaningful. Depending on the level of detail in threat specification, a given threat event could exploit multiple weaknesses and dependencies. In assessing likelihoods, organizations need to look not only at vulnerabilities that threat events could exploit, but also at mission susceptibility to events for which no security controls (or viable implementations of security controls) exist (e.g., due to functional dependencies, particularly to external dependencies). In certain situations, the most effective way to reduce mission/business risk attributable to information security risk is to redesign mission/business processes so there are potential work-arounds when information systems are compromised.

The information produced in Task 2-4 provides threat event likelihood inputs to the risk tables in Appendix I.

Summary of Key Activities – Task 2-4

- Use **Table G-1** for likelihood determination inputs.
- Use organization-defined information sources to identify likelihood determination factors.
- Use assessment scales in **Table G-2** and **Table G-3**, as extended or modified by the organization, to assess the likelihood of threat event initiation (for adversary threats) and the likelihood of threat event occurrence (for non-adversary threats).
- Use assessment scale in **Table G-4**, as extended or modified by the organization, to assess the likelihood of threat events resulting in adverse impacts, given initiation or occurrence.
- Use assessment scale in **Table G-5**, as extended or modified by the organization, to assess the overall likelihood of threat event initiation/occurrence and the threat events resulting in adverse impacts.
- Use **Table G-2**, **Table G-4**, and **Table G-5** to update Columns 7, 9, and 10 in **Table I-5** (adversary risk) and **Table G-3**, **Table G-4**, and **Table G-5** to update Columns 5, 7, and 8 in **Table I-7** (non-adversary risk), as appropriate.

DETERMINE IMPACT

TASK 2-5: Determine the adverse impacts to the organization from threat events of concern considering: (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities and predisposing conditions identified; and (iii) organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

Supplemental Guidance: Organizations describe adverse impacts in terms of the potential harm caused to organizational operations and assets, individuals, other organizations, or the Nation. Organizations can also describe impacts in terms of failure to achieve one or more security objectives (i.e., confidentiality, integrity, or availability). Organizations make explicit: (i) the process used to conduct impact determinations; (ii) assumptions related to impact determinations; (iii) credible sources and methods for obtaining impact information; and (iv) the rationale for the conclusions reached with regard to impact determinations. Assessing impact can involve identifying assets or potential targets of threat sources, including information resources (e.g., information, information systems, information technologies, applications, data repositories, communications links), people, and physical resources (e.g., buildings, power supplies), which could be affected by threat events. The focus is on high-value assets (i.e., those assets for which loss, damage, or compromise could result in significant adverse impacts to organizations). Organizations may explicitly identify how established priorities and values guide the identification of high-value assets and impacts to organizational stakeholders. If not, priorities and values related to identifying targets of threat sources and organizational impacts can typically be derived from strategic planning and policies. For example, security categorization levels indicate the organizational impacts of compromising different types of information; Privacy Impact Assessments and criticality levels (when defined as part of continuity-of-operations planning or Mission/Business Impact Analysis) indicate the impacts of destruction, corruption, or loss of accountability for information resources to organizational stakeholders. Strategic plans and policies also assert or imply the relative priorities of immediate or near-term mission/business function accomplishment and long-term organizational viability (which can be undermined by reputation loss or by sanctions resulting from compromise of sensitive information). Organizations can also consider the range of effects of threat events including the relative size of the set of resources affected, when making final impact determinations. Organizational risk tolerance assumptions may state that threat events with an impact below a specific value do not warrant further analysis. And finally, organizations [illegible]e information to support determination of uncertainty.

Appendix H provides a set of exemplary tables for use in determining adverse impacts:

- Table H-1 provides a set of exemplary inputs to the impact determination task;
- Table H-2 provides representative examples of adverse impacts to organizations focusing on harm to organizational operations and assets, individuals, other organizations, and the Nation;
- Table H-3 provides an exemplary assessment scale for assessing the impact of threat events;
- Table H-4 provides an exemplary assessment scale for assessing the range of effects of threat events; and
- Table H-5 provides a template for summarizing/documenting adverse impacts.

The information produced in Task 2-5 provides adverse impact inputs to the risk tables in Appendix I.

Summary of Key Activities – Task 2-5

- Use **Table H-1** for impact determination inputs.
- Use organization-defined information sources to identify likelihood determination factors.
- Use **Table H-2**, as extended or modified by the organization, to identify adverse impacts and affected assets, updating **Table H-5**.
- Use assessment scales in **Table H-3** and **Table H-4**, as extended or modified by the organization, to assess the impact of threat events, updating **Table H-5**.
- Use **Table H-5** to update Column 11 in **Table I-5** (adversary risk) and Column 9 in **Table I-7** (non-adversary risk), as appropriate.

DETERMINE RISK

TASK 2-6: Determine the risk to the organization from threat events of concern considering: (i) the impact that would result from the events; and (ii) the likelihood of the events occurring.

Supplemental Guidance: Organizations assess the risks from threat events as a combination of likelihood and impact. The level of risk associated with identified threat events represents a determination of the degree to which organizations are threatened by such events. Organizations make explicit the uncertainty in the risk determinations, including, for example, organizational assumptions and subjective judgments/decisions. Organizations update the list of threat events, including information regarding identification of targeting information, impacts, and the determination of the risk associated with the events. Organizations can order the list of threat events of concern by the level of risk determined during the risk assessment—with the greatest attention going to high-risk events. One factor that is consistent when determining risk is that at certainty (i.e., one hundred percent probability), the risk level equals the impact level. Each risk corresponds to a specific threat event with a level of impact if that event occurs. In general, the risk level is typically not higher than the impact level, and likelihood can serve to reduce risk below that impact level. However, when addressing organization-wide risk management issues with a large number of missions/business functions, mission/business processes, and supporting information systems, the upper bound on risk always being equal to impact at certainty, may not hold due to the potential for aggregation of risk. When multiple risks materialize, even if each risk is at the moderate level, the aggregation of those moderate-level risks could aggregate to a higher level of risk for organizations. To address situations where harm occurs multiple times, organizations can define a threat event as multiple occurrences of harm and an impact level associated with the cumulative degree of harm. During the execution of Tasks 2-1 through 2-5, organizations capture key information related to uncertainties in risk assessments. These uncertainties arise from sources such as missing information, subjective determinations, and assumptions made. The effectiveness of risk assessment results is in part determined by the ability of decision makers to be able to determine the continued applicability of assumptions made as part of the assessment. Information related to uncertainty is compiled and presented in a manner that readily supports informed risk management decisions.

Appendix I provides a set of exemplary tables for use in determining risk:

- Table I-1 provides a set of exemplary inputs to the risk and uncertainty determination task;
- Table I-2 and Table I-3 provide exemplary assessment scales for assessing levels of risk;
- Tables I-4 and I-6 provide descriptions of column headings for key data elements used in risk determinations for adversarial and non-adversarial threat events, respectively; and
- Tables I-5 and I-7 provide templates for summarizing/documenting key data elements used in risk determinations for adversarial and non-adversarial threat events, respectively.

The information produced in Task 2-6 provides risk inputs to the risk tables in Appendix I.

Summary of Key Activities – Task 2-6

- Use **Table I-1** for risk and uncertainty determination inputs.
- Use **Table I-2** and **Table I-3**, as extended or modified by the organization, to determine risk, updating Column 13 in **Table I-5** (adversary risk) and Column 11 in **Table I-7** (non-adversary risk), as appropriate.

3.3 MAINTAINING THE RISK ASSESSMENT

The third step in the risk assessment process is to *maintain* the assessment. The objective of this step is to keep current over time, the specific knowledge of the risk organizations incur. The results of risk assessments inform risk decisions and risk responses by organizations. To support ongoing risk management decisions (e.g., authorization decisions for information systems and common controls), organizations maintain risk assessments to incorporate any changes detected through risk monitoring.[37] Risk monitoring provides organizations with the means to, on an ongoing basis: (i) verify *compliance*;[38] (ii) determine the *effectiveness* of risk response measures; and (iii) identify risk-impacting *changes* to organizational information systems and the environments in which those systems operate.[39] Maintaining risk assessments includes the following specific tasks:

- Monitoring risk factors identified in risk assessments on an ongoing basis and understanding subsequent changes to those factors; and
- Updating key components of risk assessments reflecting the monitoring activities carried out by organizations.

STEP 3: MAINTAIN THE ASSESSMENT

MONITOR RISK FACTORS

TASK 3-1: Conduct ongoing monitoring of the factors that contribute to changes in risk to organizational operations and assets, individuals, other organizations, or the Nation.

Supplemental Guidance: Organizations monitor risk factors of importance on an ongoing basis to ensure that the information needed to make credible, risk-based decisions continues to be available over time. Monitoring risk factors (e.g., threat sources and threat events, vulnerabilities and predisposing conditions, capabilities and intent of adversaries, targeting of organizational operations, assets, or individuals) can provide critical information on changing conditions that could potentially affect the ability of organizations to conduct core missions and business functions. Information derived from the ongoing monitoring of risk factors can be used to refresh risk assessments at whatever frequency deemed appropriate. Organizations can also attempt to capture changes in the effectiveness of risk response measures in order to maintain the currency of risk assessments. The objective is to maintain an ongoing situational awareness of the *security state* of the organizational governance structures and activities, mission/business processes, information systems, and environments of operation. The term *security state* is used broadly to encompass all factors that may affect the risk being incurred by organizations. Therefore, in applying the risk assessment context (i.e., scope, purpose, assumptions, constraints, risk tolerances, priorities, and trade-offs), organizations consider the part risk factors play in the risk response plan executed. For example, it is expected to be quite common for the security state of information systems (that is, factors measured within those systems) to reflect only a part of the organizational risk response, with response actions at the organization level or mission/business process level providing a significant portion of that response. In such situations, monitoring only the security state of information systems would likely not provide sufficient information to correlate with the overall risk being incurred by organizations. Highly capable, well-resourced, and purpose-driven threat sources can be expected to defeat commonly available protection mechanisms (e.g., by bypassing or tampering with such mechanisms). Thus, process-level risk response measures such as reengineering mission/business processes, wise use of information technology, or the use of alternate execution processes, in the event of compromised information systems, can be major elements of organizational risk response plans.

[37] *Risk monitoring*, the fourth step in the risk management process, is described in NIST Special Publication 800-39. The step in the risk assessment process to maintain the assessment results overlaps to some degree with the risk monitoring step in the risk management process. This reinforces the important concept that many of the activities in the risk management process are complementary and mutually reinforcing.

[38] Compliance verification ensures that organizations have implemented required risk response measures and that information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, and standards/guidelines are satisfied.

[39] Draft NIST Special Publication 800-137 provides guidance on the ongoing monitoring of organizational information systems and environments of operation.

UPDATE RISK ASSESSMENT

TASK 3-2: Update existing risk assessment using the results from ongoing monitoring of risk factors.

Supplemental Guidance: Organizations determine the frequency and the circumstances under which risk assessments are updated. Such determinations can include, for example, the current level of risk to and/or the importance of, core organizational missions/business functions. If significant changes (as defined by organizational policies, direction, or guidance) have occurred since the risk assessment was performed, organizations can revisit the purpose, scope, assumptions, and constraints of the assessment to determine whether all tasks in the risk assessment process need to be performed. Otherwise, the updates constitute *differential* or *incremental* risk assessments, identifying and assessing only how selected risk factors have changed, for example: (i) the identification of new threat events, vulnerabilities, predisposing conditions, undesirable and/or affected assets; and (ii) the assessments of threat source characteristics (e.g., capability, intent, targeting, and range of effects), likelihoods, and impacts. Organizations communicate the results of updated risk assessments to entities across all risk management tiers to ensure that responsible organizational officials have access to critical information needed to make ongoing risk-based decisions.

Summary of Key Activities – Maintaining Risk ssments

- Identify key **risk factors** that have been identified for ongoing monitoring.
- Determine **frequency** of risk factor monitoring activities and the **circumstances** under which the risk assessment needs to be updated.
- Reconfirm the **purpose**, **scope**, and **assumptions** of the risk assessment.
- Conduct the appropriate risk assessment **tasks**, as needed.
- Communicate the updated risk assessr nt **results** to appropriate organizational stakeholders.

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, INSTRUCTIONS, STANDARDS, AND GUIDELINES

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.

POLICIES, DIRECTIVES, INSTRUCTIONS

1. Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance (IA) Glossary*, April 2010.
2. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

STANDARDS

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

GUIDELINES

1. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
2. National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.
3. National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.
4. National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.
5. National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010.
6. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
7. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

8. National Institute of Standards and Technology Special Publication 800-70, Revision 2, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, February 2011.

9. National Institute of Standards and Technology Special Publication 800-137 (Initial Public Draft), *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, December 2010.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

This appendix provides definitions for security terminology used within Special Publication 800-30. The terms in the glossary are consistent with the terms used in the suite of FISMA-related security standards and guidelines developed by NIST. Unless otherwise stated, all terms used in this publication are also consistent with the definitions contained in the CNSS Instruction 4009, *National Information Assurance (IA) Glossary*.

Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Advanced Persistent Threat	An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.
Agency	See *Executive Agency*.
Analysis Approach	The approach used to define the orientation or starting point of the risk assessment, the level of detail in the assessment, and how risks due to similar threat scenarios are treated.
Assessment	See *Security Control Assessment* or *Risk Assessment*.
Assessment Approach	The approach used to assess risk and its contributing factors, including quantitatively, qualitatively, or semi-quantitatively.
Assessor	See *Security Control Assessor* or *Risk Assessor*.
Assurance [CNSSI 4009]	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.
[NIST SP 800-53]	Grounds for confidence that the set of intended security controls in an information system are effective in their application.

Assurance Case [Software Engineering Institute, Carnegie Mellon University]	A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute.
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*.
Authorization (to operate)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Authorization Boundary [NIST SP 800-37]	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
Authorizing Official [CNSSI 4009]	Senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
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.
Chief Information Security Officer	See *Senior Agency Information Security Officer*.

Classified National Security Information [CNSSI 4009]	Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
Common Control [NIST SP 800-37]	A security control that is inherited by one or more organizational information systems. See *Security Control Inheritance*.
Common Control Provider [NIST SP 800-37]	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).
Compensating Security Control [CNSSI 4009]	A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides 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.
Course of Action (Risk Response)	A time-phased or situation-dependent combination of risk response measures.
Cyber Attack [CNSSI 4009]	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Cyber Security [CNSSI 4009]	The ability to protect or defend the use of cyberspace from cyber attacks.
Cyberspace [CNSSI 4009]	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
Defense-in-Breadth [CNSSI 4009]	A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).

Defense-in-Depth [CNSSI 4009]	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
Enterprise [CNSSI 4009]	An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. See *Organization*.
Enterprise Architecture [CNSSI 4009]	The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.
Environment of Operation [NIST SP 800-37]	The physical surroundings in which an information system processes, stores, and transmits information.
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.
Fault Tree Analysis	A top-down, deductive failure analysis in which an undesired state of a system (top event) is analyzed using Boolean logic to combine a series of lower-level events. An analytical approach whereby an undesired state of a system is specified and the system is then analyzed in the context of its environment of operation to find all realistic ways in which the undesired event (top event) can occur.
Federal Agency	See *Executive Agency*.
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.
Hybrid Security Control [NIST SP 800-53]	A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See *Common Control* and *System-Specific Security Control*.

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 systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.
Information [CNSSI 4009]	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
[FIPS 199]	An instance of an information type.
Information Owner [CNSSI 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal. See *Information Steward*.
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 Architecture	A description of the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.
Information Security Program Plan [NIST SP 800-53]	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
Information Steward [CNSSI 4009]	An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information System [44 U.S.C., Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Boundary	See *Authorization Boundary*.
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information System Resilience	The ability of an information system to continue to operate while under attack, even if in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack.
Information System Security Officer	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 Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
Information System-Related Security Risks	Risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. See *Risk*.
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.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

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.
Mission/Business Segment	Elements of organizations describing mission areas, common/shared business services, and organization-wide services. Mission/business segments can be identified with one or more information systems which collectively support a mission/business process.
National Security Information	See *Classified National Security Information.*
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.
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, Adapted]	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). See *Enterprise*.
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.

Predisposing Condition	A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation.
Qualitative Assessment	Use of a set of methods, principles, or rules for assessing risk based on nonnumerical categories or levels.
Quantitative Assessment	Use of a set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment.
Repeatability	The ability to repeat an assessment in the future, in a manner that is consistent with, and hence comparable to, prior assessments.
Reproducibility	The ability of different experts to produce the same results from the same data.
Risk [CNSSI 4009]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.]
Risk Assessment	The process of identifying, prioritizing, and estimating risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Risk Assessment Methodology	A risk assessment process, together with a risk model, assessment approach, and analysis approach.
Risk Assessor	The individual, group, or organization responsible for conducting a risk assessment.

Risk Executive (Function) [CNSSI 4009]	An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the 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 missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.
Risk Factor	A characteristic used in a risk model as an input to determining the level of risk in a risk assessment.
Risk Management [CNSSI 4009, adapted]	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Risk Mitigation [CNSSI 4009]	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.
Risk Model	A key component of a risk assessment methodology (in addition to assessment approach and analysis approach) that defines key terms and assessable risk factors.
Risk Monitoring	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.
Risk Response Measure	A specific action taken to respond to an identified risk.
Root Cause Analysis	A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.
Security Authorization (to Operate)	See *Authorization (to operate)*.
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.

Security Control Assessment [CNSSI 4009, Adapted]	The testing and/or evaluation of the management, operational, and technical security controls 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 an information system or organization.
Security Control Assessor	The individual, group, or organization responsible for conducting a security control assessment.
Security Control Baseline [CNSSI 4009]	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 Control Inheritance [CNSSI 4009]	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *Common Control*.
Security Controls [FIPS 199, CNSSI 4009]	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 Impact Analysis [NIST SP 800-37]	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See *System Security Plan* or *Information Security Program Plan*.
Security Policy [CNSSI 4009]	A set of criteria for the provision of security services.

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.
Semi-Quantitative Assessment	Use of a set of methods, principles, or rules for assessing risk based on bins, scales, or representative numbers whose values and meanings are not maintained in other contexts.
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. [Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information Security Officer* to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.]
Senior Information Security Officer	See *Senior Agency Information Security Officer*.
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
Supplementation (Security Controls)	The process of adding security controls or control enhancements to a security control baseline from NIST Special Publication 800-53 or CNSS Instruction 1253 in order to adequately meet the organization's risk management needs.
System	See *Information System*.
System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
System-Specific Security Control [NIST SP 800-37]	A security control for an information system that has not been designated as a common control or the portion of a hybrid control that is to be implemented within an information system.
Tailoring [NIST SP 800-53, CNSSI 4009]	The process by which a security control baseline 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 via explicit assignment and selection statements.

Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to the security control baseline. See *Tailoring*.
Technical Controls [FIPS 200]	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 [CNSSI 4009]	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, or modification of information, and/or denial of service.
Threat Assessment [CNSSI 4009]	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.
Threat Event	An event or situation that has the potential for causing undesirable consequences or impact.
Threat Scenario	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.
Threat Shifting	Response from adversaries to perceived countermeasures or obstructions, in which the adversaries change some characteristic of their intent to do harm in order to avoid or overcome countermeasures or obstacles.
Threat Source [CNSSI 4009]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.
Vulnerability [CNSSI 4009]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.
Vulnerability Assessment [CNSSI 4009]	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

APT	Advanced Persistent Threat
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
COOP	Continuity of Operations
COTS	Commercial Off-The-Shelf
DoD	Department of Defense
EA	Enterprise Architecture
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IA	Information Assurance
ICS	Industrial Control System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
NOFORN	Not Releasable to Foreign Nationals
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
RAR	Risk Assessment Report
RMF	Risk Management Framework
SCAP	Security Content Automation Protocol
SP	Special Publication
TTP	Tactic Technique Procedure
U.S.C.	United States Code

APPENDIX D

THREAT SOURCES

TAXONOMY OF THREATS SOURCES CAPABLE OF INITIATING THREAT EVENTS

This appendix provides: (i) a description of potentially useful inputs to the *threat source* identification task; (ii) an exemplary taxonomy of threat sources by type, description, and risk factors (i.e., characteristics) used to assess the likelihood and/or impact of such threat sources initiating threat events; (iii) an exemplary set of tailorable assessment scales for assessing those risk factors; and (iv) templates for summarizing and documenting the results of the threat source identification Task 2-1. The taxonomy and assessment scales in this appendix can be used by organizations as a starting point with appropriate tailoring to adjust for organization-specific conditions. Tables D-7 and D-8 are outputs from Task 2-1 and provide relevant inputs to the risk tables in Appendix I.

TABLE D-1: INPUTS – THREAT SOURCE IDENTIFICATION

Description	Provided To		
	Tier 1	**Tier 2**	**Tier 3**

From Tier 1: (Organization level)
- Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments. (Section 3.1, Task 1-4)
- Threat source information and guidance specific to Tier 1 (e.g., threats related to organizational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/business relationships).
- Taxonomy of threat sources, annotated by the organization, if necessary. (Table D-2)
- Characterization of adversarial and non-adversarial threat sources.
  - Assessment scales for assessing adversary capability, intent, and targeting, annotated by the organization, if necessary. (Table D-3, Table D-4, Table D-5)
  - Assessment scale for assessing the range of effects, annotated by the organization, if necessary. (Table D-6)
- Threat sources identified in previous risk assessments, if appropriate.
	No	Yes	Yes
			If not provided by Tier 2

From Tier 2: (Mission/business process level) - Threat source information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Mission/business process-specific characterization of adversarial and non-adversarial threat sources.	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Threat source information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). - Information system-specific characterization of adversarial and non-adversarial threat sources.	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

TABLE D-2: TAXONOMY OF THREAT SOURCES

Type of Threat Source	Description	Characteristics

ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
  - Organization
  - Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

ACCIDENTAL - Ordinary User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects

STRUCTURAL
- IT Equipment
  - Storage
  - Processing
  - Communications
  - Display
  - Sensor
  - Controller
- Environmental Controls
  - Temperature/Humidity Controls
  - Power Supply
- Software
  - Operating System
  - Networking
  - General-Purpose Application
  - Mission-Specific Application
	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects

ENVIRONMENTAL
- Natural or man-made disaster
  - Fire
  - Flood/Tsunami
  - Windstorm/Tornado
  - Hurricane
  - Earthquake
  - Bombing
  - Overrun
- Unusual Natural Event (e.g., sunspots)
- Infrastructure Failure/Outage
  - Telecommunications
  - Electrical Power
	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.
	Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).
		Range of effects

TABLE D-3: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY CAPABILITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

TABLE D-4: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY INTENT

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.
High	80-95	8	The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks.
Moderate	21-79	5	The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt the organization's cyber resources by establishing a foothold in the organization's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the organization's mission/business functions to achieve these ends.
Low	5-20	2	The adversary actively seeks to obtain critical or sensitive information or to usurp/disrupt the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.
Very Low	0-4	0	The adversary seeks to usurp, disrupt, or deface the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.

TABLE D-5: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY TARGETING

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.
High	80-95	8	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
Moderate	21-79	5	The adversary analyzes publicly available information to target persistently specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information.
Low	5-20	2	The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class.
Very Low	0-4	0	The adversary may or may not target any specific organizations or classes of organizations.

TABLE D-6: ASSESSMENT SCALE – RANGE OF EFFECTS FOR NON-ADVERSARIAL THREAT SOURCES

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The effects of the error, accident, or act of nature are sweeping, involving almost all of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure].
High	80-95	8	The effects of the error, accident, or act of nature are extensive, involving most of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], including many critical resources.
Moderate	21-79	5	The effects of the error, accident, or act of nature are wide-ranging, involving a significant portion of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], including some critical resources.
Low	5-20	2	The effects of the error, accident, or act of nature are limited, involving some of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], but involving no critical resources.
Very Low	0-4	0	The effects of the error, accident, or act of nature are minimal, involving few if any of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], and involving no critical resources.

TABLE D-7: TEMPLATE – IDENTIFICATION OF ADVERSARIAL THREAT SOURCES

Identifier	Threat Source Source of Information	In Scope	Capability	Intent	Targeting
Organization -defined	Table D-2 and Task 1-4 or Organization-defined	Yes / No	Table D-3 or Organization -defined	Table D-4 or Organization -defined	Table D-5 or Organization -defined

TABLE D-8: TEMPLATE – IDENTIFICATION OF NON-ADVERSARIAL THREAT SOURCES

Identifier	Threat Source Source of Information	In Scope	Range of Effects
Organization -defined	Table D-2 and Task 1-4 or Organization-defined	Yes / No	Table D-6 or Organization-defined

APPENDIX E

THREAT EVENTS

REPRESENTATIVE THREAT EVENTS INITIATED BY THREAT SOURCES

This appendix provides: (i) a description of potentially useful inputs to the *threat event* identification task; (ii) representative examples of adversarial threat events expressed as tactics, techniques, and procedures (TTPs) and non-adversarial threat events; (iii) expected or predicted values for the relevance of those threat events; and (iv) templates for summarizing and documenting the results of the threat identification Task 2-2. Organizations can eliminate certain threat events from further consideration if no adversary with the necessary capabilities has been identified. Organizations can also modify or augment the threat events provided to address specific TTPs with sufficient detail and at the appropriate classification level.[40] The representative threat events and predicated or expected values for the relevance of those events can be used by organizations as a starting point with appropriate tailoring to adjust for any organization-specific conditions. Table E-5 is an output from Task 2-2 and provides relevant inputs to the risk tables in Appendix I.

TABLE E-1: INPUTS – THREAT EVENT IDENTIFICATION

Description	Provided To		
	Tier 1	**Tier 2**	**Tier 3**
From Tier 1: (Organization level) - Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments. (Section 3.1, Task 1-4.) - Threat event information and guidance specific to Tier 1 (e.g., threats related to organizational governance, core missions/business functions, external mission/business relationships, management/operational policies, procedures, and structures). - Exemplary adversarial threat events, annotated by the organization, if necessary. (Table E-2) - Exemplary non-adversarial threat events, annotated by the organization, if necessary. (Table E-3) - Assessment scale for assessing the relevance of threat events, annotated by the organization, if necessary. (Table E-4) - Threat events identified in previous risk assessments, if appropriate.	No	Yes	Yes *If not provided by Tier 2*
From Tier 2: (Mission/business process level) - Threat event information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Mission/business process-specific characterization of adversarial and non-adversarial threat events.	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Threat event information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). - Information system-specific characterization of adversarial and non-adversarial threat events.	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

[40] The threat events in Table E-2 are provided at the *unclassified* level. Additional threat events at the *classified* level are available from selected federal agencies to individuals with appropriate security clearances and need to know.

TABLE E-2: REPRESENTATIVE EXAMPLES – ADVERSARIAL THREAT EVENTS

Threat Events	Description
Access sensitive information through network sniffing.	Adversary gains access to the exposed wired or wireless data channels that organizations (or organizational personnel) use to transmit information, and intercept communications. Adversary actions might include, for example, targeting public kiosks or hotel networking connections.
Adapt cyber attacks based on detailed surveillance.	Adversary adapts attacks in response to surveillance of organizations and the protective measures that organizations employ.
Exploit recently discovered vulnerabilities.	Adversary exploits recently discovered vulnerabilities in organizational information systems in an attempt to attack the systems before mitigation measures are available or in place.
Employ brute force login attempts/password guessing.	Adversary attempts to gain access to organizational information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.
Cause degradation or denial of attacker selected services or capabilities.	Adversary launches attacks specifically intended to impede the ability of organizations to function.
Cause deterioration/destruction of critical information system components and functions.	Adversary attempts to destroy or deteriorate critical information system components for purposes of impeding or eliminating the ability of organizations to carry out missions or business functions. Detection of this action is not a concern.
Combine internal and external attacks across multiple information systems and information technologies to achieve a breach or compromise.	Adversary combines attacks that require both physical presence within organizations and cyber methods to achieve success. Physical components may be as simple as convincing maintenance personnel to leave doors or cabinets open.
Compromise critical information systems via physical access by outsiders.	Adversary without authorized access to organizational information systems, attempts to physically gain access to the systems.
Compromise mission critical information.	Adversary takes action to compromise the integrity of mission critical information, thus preventing/impeding ability of organizations to which information is supplied, from carrying out operations.
Compromise information systems or devices used externally and reintroduce into the enterprise.	Adversary manages to install malware on information systems or devices while the systems/devices are external to organizations for purposes of subsequently infecting organizations when reconnected.
Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware) organizations are known to use.	Adversary is able to compromise the design, manufacturing, and/or distribution of critical information system components at selected suppliers.
Conduct reconnaissance, surveillance, and target acquisition of targeted organizations.	Adversary uses various means (e.g., scanning, physical observation) to examine and assess organizations and ascertain points of vulnerability.
Conduct phishing attacks.	Adversary attempts to acquire sensitive information such as usernames, passwords, or SSNs, by pretending to be communications from a legitimate/trustworthy source. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to Web sites that appear to be legitimate sites, while actually stealing the entered information.
Continuous, adaptive and changing cyber attacks based on detailed surveillance of organizations.	Adversary attacks continually change in response to surveillance of organizations and protective measures that organizations take.
Coordinating cyber attacks on organizations using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organizational operations.
Create and operate false front organizations that operate within the critical life cycle path to inject malicious information system components into the supply chain.	Adversary creates the appearance of legitimate suppliers that then inject corrupted/malicious information system components into the supply chain of organizations.
Deliver known malware to internal organizational information systems (e.g., virus via email).	Adversary uses common delivery mechanisms (e.g., email) to install/insert known malware (e. g., malware whose existence is known) into organizational information systems.
Deliver modified malware to internal organizational information systems.	Adversary uses more sophisticated means (e.g., Web traffic, instant messaging, FTP) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems.

Threat Events	Description
Devise attacks specifically based on deployed information technology environment.	Adversary develops attacks, using known and unknown attacks that are designed to take advantage of adversary knowledge of the information technology infrastructure.
Discovering and accessing sensitive data/information stored on publicly accessible information systems.	Adversary attempts to scan or mine information on publically accessible servers and Web pages of organizations with the intent of finding information that is sensitive (i.e., not approved for public release).
Distributed Denial of Service (DDoS) attack.	Adversary uses multiple compromised information systems to attack a single target, thereby causing denial of service for users of the targeted information systems.
Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones).	Adversary takes advantage of fact that transportable information systems are outside physical protection of organizations and logical protection of corporate firewalls, and compromises the systems based on known vulnerabilities to gather information from those systems.
Exploiting vulnerabilities in information systems timed with organizational mission/business operations tempo.	Adversary launches attacks on organizations in a time and manner consistent with organizational needs to conduct mission/business operations.
Externally placed adversary sniffing and intercepting of wireless network traffic.	Adversary strategically in position to intercept wireless communications of organizations.
Hijacking information system sessions of data traffic between the organization and external entities.	Adversary takes control of (hijacks) already established, legitimate information system sessions between organizations and external entities (e.g., users connecting from off-site locations).
Injecting false but believable data/information into organizational information systems.	Adversary injects false but believable data into organizational information systems. This action by the adversary may impede the ability of organizations to carry out missions/business functions correctly and/or undercut the credibility other entities may place in the information or services provided by organizations.
Insert subverted individuals into privileged positions in organizations.	Adversary has individuals in privileged positions within organizations that are willing and able to carry out actions to cause harm to organizational missions/business functions. Subverted individuals may be active supporters of adversary, supporting adversary (albeit under duress), or unknowingly supporting adversary (e.g., false flag). Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files, etc.) and may leverage access to one privileged capability to get to another capability.
Counterfeit/Spoofed Web site.	Adversary creates duplicates of legitimate Web sites and directs users to counterfeit sites to gather information.
Deliver targeted Trojan for control of internal systems and exfiltration of data.	Adversary manages to install software containing Trojan horses that are specifically designed to take control of internal organizational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions.
Employ open source discovery of organizational information useful for future cyber attacks.	Adversary mines publically accessible information with the goal of discerning information about information systems, users, or organizational personnel that the adversary can subsequently employ in support of an attack.
Exploit vulnerabilities on internal organizational information systems.	Adversary searches for known vulnerabilities in organizational internal information systems and exploits those vulnerabilities.
Inserting malicious code into organizational information systems to facilitate exfiltration of data/information.	Adversary successfully implants malware into internal organizational information systems, where the malware over time identifies and then successfully exfiltrates valuable information.
Installing general-purpose sniffers on organization-controlled information systems or networks.	Adversary manages to install sniffing software onto internal organizational information systems or networks.
Leverage traffic/data movement allowed across perimeter (e.g., email communications, removable storage) to compromise internal information systems (e.g., using open ports to exfiltrate information).	Adversary makes use of permitted information flows (e.g., email communications) to facilitate compromises to internal information systems (e.g., phishing attacks to direct users to go to Web sites containing malware) which allows adversary to obtain and exfiltrate sensitive information through perimeters.
Insert subverted individuals into the organizations.	Adversary has individuals in place within organizations that are willing and able to carry out actions to cause harm to organizational missions/business functions. Subverted individuals may be active supporters of adversary, supporting adversary (albeit under duress), or unknowingly supporting adversary (e.g., false flag).

Threat Events	Description
Insert counterfeited hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.
Inserting malicious code into organizational information systems and information system components (e.g., commercial information technology products) known to be used by organizations.	Adversary inserts malware into information systems specifically targeted to the hardware, software, and firmware used by organizations (resulting from the reconnaissance of organizations by adversary).
Inserting specialized, non-detectable, malicious code into organizational information systems based on system configurations.	Adversary launches multiple, potentially changing attacks specifically targeting critical information system components based on reconnaissance and placement within organizational information systems.
Insider-based session hijacking.	Adversary places an entity within organizations in order to gain access to organizational information systems or networks for the express purpose of taking control (hijacking) an already established, legitimate session either between organizations and external entities (e.g., users connecting from remote locations) or between two locations within internal networks.
Installing persistent and targeted sniffers on organizational information systems and networks.	Adversary places within the internal organizational information systems or networks software designed to (over a continuous period of time) collect (sniff) network traffic.
Intercept/decrypt weak or unencrypted communication traffic and protocols.	Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing publically known flaws), targets those communications, and gains access to transmitted information and channels.
Jamming wireless communications.	Adversary takes measures to interfere with the wireless communications so as to impede or prevent communications from reaching intended recipients.
Malicious activity using unauthorized ports, protocols, and services.	Adversary conducts attacks using ports, protocols, and services for ingress and egress that are not authorized for use by organizations.
Malicious creation, deletion, and/or modification of files on publicly accessible information systems (e.g., Web defacement).	Adversary vandalizes, or otherwise makes unauthorized changes to organizational Web sites or files on Web sites.
Mapping and scanning organization-controlled (internal) networks and information systems from within (inside) organizations.	Adversary installs malware inside perimeter that allows the adversary to scan network to identify targets of opportunity. Because the scanning does not cross the perimeter, it is not detected by externally placed intrusion detection systems.
Mishandling of critical and/or sensitive information by authorized users.	Authorized users inadvertently expose critical/sensitive information.
Multistage attacks (e.g., hopping).	Adversary moves attack location from one compromised information system to other information systems making identification of source difficult.
Network traffic modification (man in the middle) attacks by externally placed adversary.	Adversary intercepts/eavesdrops on sessions between organizations and external entities. Adversary then relays messages between the organizations and external entities, making them believe that they are talking directly to each other over a private connection, when in fact the entire communication is controlled by the adversary.
Network traffic modification (man in the middle) attacks by internally placed adversary.	Adversary operating within the infrastructure of organizations intercepts and corrupts data sessions.
Non-target specific insertion of malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware, or commercial information technology products. Adversary is not targeting specific organizations in this attack, simply looking for entry points into internal organizational information systems.
Operate across organizations to acquire specific information or achieve desired outcome.	Adversary does not limit planning to the targeting of one organization. Adversary observes multiple organizations to acquire necessary information on targets of interest.
Opportunistically stealing or scavenging information systems/components.	Adversary takes advantage of opportunities (due to advantageous positioning) to steal information systems or components (e. g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organizations.
Perimeter network reconnaissance/scanning.	Adversary uses commercial or free software to scan organizational perimeters with the goal of obtaining information that provides the adversary with a better understanding of the information technology infrastructure and facilitates the ability of the adversary to launch successful attacks.

Threat Events	Description
Pollution of critical data.	Adversary implants corrupted and incorrect data in the critical data that organizations use to cause organizations to take suboptimal actions or to subsequently disbelieve reliable inputs.
Poorly configured or unauthorized information systems exposed to the Internet.	Adversary gains access through the Internet, to information systems that are not authorized for such access or that do not meet the specified configuration requirements of organizations.
Salting the physical perimeter of organizations with removable media containing malware.	Adversary places removable media (e.g., flash drives) containing malware in locations external to the physical perimeters of organizations but where employees are likely to find and install on organizational information systems.
Simple Denial of Service (DoS) Attack.	Adversary attempts to make an Internet-accessible resource unavailable to intended users, or prevent the resource from functioning efficiently or at all, temporarily or indefinitely.
Social engineering by insiders within organizations to convince other insiders to take harmful actions.	Internally placed adversaries take actions (e.g., using email, phone) so that individuals within organizations reveal critical/sensitive information (e.g., personally identifiable information).
Social engineering by outsiders to convince insiders to take armful actions.	Externally placed adversaries take actions (using email, phone) with the intent of persuading or otherwise tricking individuals within organizations into revealing critical/sensitive information (e.g., personally identifiable information).
Spear phishing attack.	Adversary employs phishing attacks targeted at high-value targets (e.g., senior leaders/executives).
Spill sensitive information.	Adversary contaminates organizational information systems (including devices and networks) by placing on the systems or sending to/over the systems, information of a classification/sensitivity which the systems have not been authorized to handle. The information is exposed to individuals that are not authorized access to such information, and the information system, device, or network is unavailable while the spill is investigated and mitigated.
Spread attacks across organizations from existing footholds.	Adversary builds upon existing footholds within organizations and works to extend the footholds to other parts of organizations including organizational infrastructure. Adversary places itself in positions to further undermine the ability for organizations to carry out missions/business functions.
Successfully compromise software of critical information systems within organizations.	Adversary inserts malware or otherwise corrupts critical internal organizational information systems.
Tailgate authorized staff to gain access to organizational facilities.	Adversary follows authorized individuals into secure/controlled locations with the goal of gaining access to facilities, circumventing physical security checks.
Tailored zero-day attacks on organizational information systems.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Zero-day attacks are based on adversary insight into the information systems and applications used by organizations as well as adversary reconnaissance of organizations.
Tamper with critical organizational information system components and inject the components into the systems.	Adversary replaces, though supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components that operate in such a manner as to severely disrupt organizational missions/business functions or operations.
Targeting and compromising home computers (including personal digital assistants and smart phones) of critical employees within organizations.	Adversary targets key employees of organizations outside the security perimeters established by organizations by placing malware in the personally owned information systems and devices of individuals (e.g., laptop/notebook computers, personal digital assistants, smart phones). The intent is to take advantage of any instances where employees use personal information systems or devices to convey critical/sensitive information.
Targeting and exploiting critical hardware, software, or firmware (both commercial off-the-shelf and custom information systems and components).	Adversary targets and attempts to compromise the operation of software (e.g., through malware injections) that performs critical functions for organizations. This is largely accomplished as supply chain attacks.
Unauthorized internal information system access by insiders.	Adversary is an individual who has authorized access to organizational information systems, but gains (or attempts to gain) access that exceeds authorization.
Undermine the ability of organizations to detect attacks.	Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations.

Threat Events	Description
Use remote information system connections of authorized users as bridge to gain unauthorized access to internal networks (i.e., split tunneling).	Adversary takes advantage of external information systems (e.g., laptop computers at remote locations) that are simultaneously connected securely to organizations and to nonsecure remote connections gaining unauthorized access to organizations via nonsecure, open channels.
Using postal service or other commercial delivery services to insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Adversary uses courier service to deliver to organizational mailrooms a device that is able to scan wireless communications accessible from within the mailrooms and then wirelessly transmit information back to adversary.
Zero-day attacks (non-targeted).	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Attacks are not based on any adversary insights into specific vulnerabilities of organizations.

TABLE E-3: REPRESENTATIVE EXAMPLES – NON-ADVERSARIAL THREAT EVENTS

Threat Source	Threat Event	Description
Accidental Ordinary User	Spill sensitive information	Authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
Accidental Privileged User or Administrator	Mishandling of critical and/or sensitive information by authorized users	Authorized privileged user inadvertently exposes critical/sensitive information.
Communication	Communications contention	Degraded communications performance due to contention.
Display	Unreadable display	Display unreadable due to aging equipment.
Earthquake	Earthquake at primary facility	Earthquake of organization-defined magnitude at primary facility makes facility inoperable.
Fire	Fire at primary facility	Fire (not due to adversarial activity) at primary facility makes facility inoperable.
Fire	Fire at backup facility	Fire (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Flood	Flood at primary facility	Flood (not due to adversarial activity) at primary facility makes facility inoperable.
Flood	Flood at backup facility	Flood (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Hurricane	Hurricane at primary facility	Hurricane of organization-defined strength at primary facility makes facility inoperable.
Hurricane	Hurricane at backup facility	Hurricane of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Processing	Resource depletion	Degraded processing performance due to resource depletion.
Storage	Disk error	Corrupted storage due to a disk error.
Storage	Pervasive disk error	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.
Windstorm or Tornado	Windstorm/tornado at primary facility	Windstorm/tornado of organization-defined strength at primary facility makes facility inoperable.
Windstorm or Tornado	Windstorm/tornado at backup facility	Windstorm/tornado of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.

TABLE E-4: RELEVANCE OF THREAT EVENTS

Value	Description
Confirmed	The threat event or TTP has been seen by the organization.
Expected	The threat event or TTP has been seen by the organization's peers or partners.
Anticipated	The threat event or TTP has been reported by a trusted source.
Predicted	The threat event or TTP has been predicted by a trusted source.
Possible	The threat event or TTP has been described by a somewhat credible source.
N/A	The threat event or TTP is not currently applicable. For example, a threat event or TTP could assume specific technologies, architectures, or processes that are not present in the organization, mission/business process, EA segment, or information system; or predisposing conditions that are not present (e.g., location in a flood plain). Alternately, if the organization is using detailed or specific threat information, a threat event or TTP could be deemed inapplicable because information indicates that no adversary is expected to initiate the threat event or use the TTP.

TABLE E-5: TEMPLATE – IDENTIFICATION OF THREAT EVENTS

Identifier	Threat Event Source of Information	Threat Source	Relevance
Organization-defined	Table E-2, Table E-3, Task 1-4 or Organization-defined	Table D-7, Table D-8 or Organization-defined	Table E-4 or Organization-defined

APPENDIX F

VULNERABILITIES AND PREDISPOSING CONDITIONS

FACTORS AFFECTING THE LIKELIHOOD OF SUCCESSFUL THREAT EXPLOITATION

This appendix provides: (i) a description of potentially useful inputs to the *vulnerability* and *predisposing condition* identification task; (ii) an exemplary taxonomy of predisposing conditions; (iii) exemplary assessment scales for assessing the severity of vulnerabilities and the pervasiveness of predisposing conditions; and (iv) a set of templates for summarizing and documenting the results of the vulnerability and predisposing condition identification task. The taxonomy and assessment scales in this appendix can be used by organizations as a starting point with appropriate tailoring to adjust for any organization-specific conditions. Tables F-3 and F-6 are outputs from Task 2-3 and provide relevant inputs to the risk tables in Appendix I.

TABLE F-1: INPUTS – VULNERABILITIES AND PREDISPOSING CONDITIONS

Description	Provided To		
	Tier 1	**Tier 2**	**Tier 3**

From Tier 1 (Organization level)
- Sources of vulnerability information deemed to be credible (e.g., open source and/or classified vulnerabilities, previous risk/vulnerability assessments, Mission and/or Business Impact Analyses). (Section 3.1, Task 1-4.)
- Vulnerability information and guidance specific to Tier 1 (e.g., vulnerabilities related to organizational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/business relationships).
- Taxonomy of predisposing conditions, annotated by the organization, if necessary. (Table F-4)
- Characterization of vulnerabilities and predisposing conditions.
  - Assessment scale for assessing the severity of vulnerabilities, annotated by the organization, if necessary. (Table F-2)
  - Assessment scale for assessing the pervasiveness of predisposing conditions, annotated by the organization, if necessary. (Table F-5)
	No	Yes	Yes
			If not provided by Tier 2

From Tier 2: (Mission/business process level) - Vulnerability information and guidance specific to Tier 2 (e.g., vulnerabilities related to organizational mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies).	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Vulnerability information and guidance specific to Tier 3 (e.g., vulnerabilities related to information systems, information technologies, information system components, applications, networks, environments of operation). - Security assessment reports (i.e., deficiencies in assessed controls identified as vulnerabilities). - Results of monitoring activities (e.g., automated and nonautomated data feeds). - Vulnerability assessments, Red Team reports, or other reports from analyses of information systems, subsystems, information technology products, devices, networks, or applications. - Contingency Plans, Disaster Recovery Plans, Incident Reports. - Vendor/manufacturer vulnerability reports.	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

TABLE F-2: ASSESSMENT SCALE – VULNERABILITY SEVERITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High	80-95	8	Relevant security control or other remediation is planned but not implemented.
Moderate	21-79	5	Relevant security control or other remediation is partially implemented and somewhat effective.
Low	5-20	2	Relevant security control or other remediation is fully implemented and somewhat effective.
Very Low	0-4	0	Relevant security control or other remediation is fully implemented, assessed, and effective.

TABLE F-3: TEMPLATE – IDENTIFICATION OF VULNERABILITIES

Identifier	Vulnerability Source of Information	Vulnerability Severity
Organization-defined	Task 2-3, Task 1-4 or Organization-defined	Table F-2 or Organization-defined

TABLE F-4: TAXONOMY OF PREDISPOSING CONDITIONS

Type of Predisposing Condition	Description

INFORMATION-RELATED
- Classified National Security Information
- Compartments
- Controlled Unclassified Information
- Personally Identifiable Information
- Special Access Programs
- Agreement-Determined
  - NOFORN
  - Proprietary
	Needs to handle information (as it is created, transmitted, stored, processed, and/or displayed) in a specific manner, due to its sensitivity (or lack of sensitivity), legal or regulatory requirements, and/or contractual or other organizational agreements.

TECHNICAL
- Architectural
  - Compliance with technical standards
  - Use of specific products or product lines
  - Solutions for and/or approaches to user-based collaboration and information sharing
  - Allocation of specific security functionality to common controls
- Functional
  - Networked multiuser
  - Single-user
  - Stand-alone / nonnetworked
  - Restricted functionality (e.g., communications, sensors, embedded controllers)
	Needs to use technologies in specific ways.

OPERATIONAL / ENVIRONMENTAL
- Mobility
  - Fixed-site (specify location)
  - Semi-mobile
  - Land-based (e.g., van)
  - Airborne
  - Sea-based
  - Space-based
  - Mobile (e.g., handheld device)
- Population with physical and/or logical access to components of the information system, mission/business process, EA segment
  - Size of population
  - Clearance/vetting of population
	Ability to rely upon physical, procedural, and personnel controls provided by the operational environment.

TABLE F-5: ASSESSMENT SCALE – PERVASIVENESS OF PREDISPOSING CONDITIONS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Applies to **all** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
High	80-95	8	Applies to **most** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Moderate	21-79	5	Applies to **many** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Low	5-20	2	Applies to **some** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Very Low	0-4	0	Applies to **few** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).

TABLE F-6: TEMPLATE – IDENTIFICATION OF PREDISPOSING CONDITIONS

Identifier	Predisposing Condition Source of Information	Pervasiveness of Condition
Organization-defined	Table F-4, Task 1-4 or Organization-defined	Table F-5 or Organization-defined

APPENDIX G

LIKELIHOOD OF OCCURRENCE

DETERMINING THE LIKELIHOOD OF THREAT EVENTS CAUSING ADVERSE IMPACTS

This appendix provides: (i) a description of potentially useful inputs to the *likelihood*[41] determination task; and (ii) exemplary assessment scales for assessing the likelihood of threat event initiation/occurrence, the likelihood of threat events resulting in adverse impacts, and the overall likelihood of threat events being initiated or occurring and doing damage to organizational operations, assets, or individuals. The assessment scales in this appendix can be used by organizations as a starting point with appropriate tailoring to adjust for any organization-specific conditions. Tables G-2, G-3, G-4, and G-5 are outputs from Task 2-4 and provide relevant inputs to the risk tables in Appendix I.

TABLE G-1: INPUTS – DETERMINATION OF LIKELIHOOD

Description	Provided To		
	Tier 1	**Tier 2**	**Tier 3**
From Tier 1 (Organization level) - Sources of threat information identified for organization-wide use (e.g., specific information that may be useful in determining likelihoods such as adversary capabilities, intent, and targeting objectives). - Likelihood information and guidance specific to Tier 1 (e.g., likelihood information related to organizational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/business relationships). - Guidance on organization-wide levels of likelihood needing no further consideration. - Assessment scale for assessing the likelihood of threat event initiation (adversarial threat events), annotated by the organization, if necessary. (Table G-2) - Assessment scale for assessing the likelihood of threat event occurrence (non-adversarial threat events), annotated by the organization, if necessary. (Table G-3) - Assessment scale for assessing the likelihood of threat events resulting in adverse impacts, annotated by the organization, if necessary. (Table G-4) - Assessment scale for assessing the overall likelihood of threat events being initiated or occurring and resulting in adverse impacts, annotated by the organization, if necessary. (Table G-5)	No	Yes	Yes *If not provided by Tier 2*
From Tier 2: (Mission/business process level) - Likelihood information and guidance specific to Tier 2 (e.g., likelihood information related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies).	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Likelihood information and guidance specific to Tier 3 (e.g., likelihood information related to information systems, information technologies, information system components, applications, networks, environments of operation). - Historical data on successful and unsuccessful cyber attacks; attack detection rates. - Security assessment reports (i.e., deficiencies in assessed controls identified as vulnerabilities). - Results of monitoring activities (e.g., automated and nonautomated data feeds). - Vulnerability assessments, Red Team reports, or other reports from analyses of information systems, subsystems, information technology products, devices, networks, or applications. - Contingency Plans, Disaster Recovery Plans, Incident Reports. - Vendor/manufacturer vulnerability reports.	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

[41] The term *likelihood*, as discussed in this guideline, is not likelihood in the strict sense of the term; rather, it is a likelihood score. That is, risk assessors do not define a likelihood function in the statistical sense. Instead, risk assessors assign a score (or likelihood assessment) based on available evidence, experience, and expert judgment. Combinations of factors such as targeting, intent, and capability thus can be used to produce a score representing the likelihood of threat initiation; combinations of factors such as capability and vulnerability severity can be used to produce a score representing the likelihood of adverse impacts; and combinations of these scores can be used to produce an overall likelihood score.

TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is almost certain to initiate the threat event.
High	80-95	8	Adversary is highly likely to initiate the threat event.
Moderate	21-79	5	Adversary is somewhat likely to initiate the treat event.
Low	5-20	2	Adversary is unlikely to initiate the threat event.
Very Low	0-4	0	Adversary is highly unlikely to initiate the threat event.

TABLE G-3: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT OCCURRENCE (NON-ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
High	80-95	8	Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.
Moderate	21-79	5	Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.
Low	5-20	2	Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.
Very Low	0-4	0	Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is almost certain to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is highly likely to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is unlikely to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.

TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	High	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

APPENDIX H

IMPACT

EFFECTS OF THREAT EVENTS ON ORGANIZATIONS, INDIVIDUALS, AND THE NATION

This appendix provides: (i) a description of useful inputs to the impact determination task; (ii) representative examples of adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation; (iii) exemplary assessment scales for assessing the impact of threat events and the range of effect of threat events; and (iv) a template for summarizing and documenting the results of the impact determination Task 2-5. The assessment scales in this appendix can be used by organizations as a starting point with appropriate tailoring to adjust for any organization-specific conditions. Table H-5 is the output from Task 2-5 and provides relevant inputs to the risk tables in Appendix I.

TABLE H-1: INPUTS – DETERMINATION OF IMPACT

Description	Provided To		
	Tier 1	**Tier 2**	**Tier 3**
From Tier 1 (Organization level) - Sources of threat information identified for organization-wide use (e.g., specific information that may be useful in determining likelihoods such as adversary capabilities, intent, and targeting objectives). - Impact information and guidance specific to Tier 1 (e.g., impact information related to organizational governance, core missions/business functions, management and operational policies, procedures, and structures, external mission/business relationships). - Guidance on organization-wide levels of impact needing no further consideration. - Identification of critical missions/business functions. - Exemplary set of impacts, annotated by the organization, if necessary. (Table H-2) - Assessment scale for assessing the impact of threat events, annotated by the organization, if necessary. (Table H-3) - Assessment scale for assessing the range of threat effects, annotated by the organization, if necessary. (Table H-4)	No	Yes	Yes *If not provided by Tier 2*
From Tier 2: (Mission/business process level) - Impact information and guidance specific to Tier 2 (e.g., impact information related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Identification of high-value assets.	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Impact information and guidance specific to Tier 3 (e.g., likelihood information affecting information systems, information technologies, information system components, applications, networks, environments of operation). - Historical data on successful and unsuccessful cyber attacks; attack detection rates. - Security assessment reports (i.e., deficiencies in assessed controls identified as vulnerabilities). - Results of continuous monitoring activities (e.g., automated and nonautomated data feeds). - Vulnerability assessments, Red Team reports, or other reports from analyses of information systems, subsystems, information technology products, devices, networks, or applications. - Contingency Plans, Disaster Recovery Plans, Incident Reports.	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

TABLE H-2: EXAMPLES OF ADVERSE IMPACTS

Type of Impact	Impact

HARM TO OPERATIONS	- Inability to perform current missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Inability, or limited ability, to perform missions/business functions in the future.
	  - Inability to restore missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Harms (e.g., financial costs, sanctions) due to noncompliance.
	  - With applicable laws or regulations.
	  - With contractual requirements or other requirements in other binding agreements.
	- Direct financial costs.
	- Relational harms.
	  - Damage to trust relationships.
	  - Damage to image or reputation (and hence future or potential trust relationships).

HARM TO ASSETS	- Damage to or loss of physical facilities. - Damage to or loss of information systems or networks. - Damage to or loss of information technology or equipment. - Damage to or loss of component parts or supplies. - Damage to or of loss of information assets. - Loss of intellectual property.
HARM TO INDIVIDUALS	- Identity theft. - Loss of Personally Identifiable Information. - Injury or loss of life. - Damage to image or reputation. - Physical or psychological mistreatment.

HARM TO OTHER ORGANIZATIONS	- Harms (e.g., financial costs, sanctions) due to noncompliance.
	  - With applicable laws or regulations.
	  - With contractual requirements or other requirements in other binding agreements.
	- Direct financial costs.
	- Relational harms.
	  - Damage to trust relationships.
	  - Damage to reputation (and hence future or potential trust relationships).

HARM TO THE NATION	- Damage to or incapacitation of a critical infrastructure sector.
	- Loss of government continuity of operations.
	- Relational harms.
	  - Damage to trust relationships with other governments or with nongovernmental entities.
	  - Damage to national reputation (and hence future or potential trust relationships).
	- Damage to current or future ability to achieve national objectives.

TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

TABLE H-4: ASSESSMENT SCALE – RANGE OF EFFECTS OF THREAT EVENTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The effects of the error, accident, or act of nature are sweeping, involving almost all of the cyber resources of the organization.
High	80-95	8	The effects of the error, accident, or act of nature are extensive, involving most of the cyber resources of the organization, including many critical resources.
Moderate	21-79	5	The effects of the error, accident, or act of nature are substantial, involving a significant portion of the cyber resources of the organization, including some critical resources.
Low	5-20	2	The effects of the error, accident, or act of nature are limited, involving some of the cyber resources of the organization, but involving no critical resources.
Very Low	0-4	0	The effects of the error, accident, or act of nature are minimal or negligible, involving few if any of the cyber resources of the organization, and involving no critical resources.

TABLE H-5: TEMPLATE – IDENTIFICATION OF ADVERSE IMPACTS

Type of Impact	Impact Affected Asset	Security Objectives Not Achieved	Maximum Impact
Table H-2 or Organization-defined	Table H-2 or Organization-defined	Organization-defined	Table H-3 and H-4 or Organization-defined

APPENDIX I

RISK

ASSESSING RISK TO ORGANIZATIONS, INDIVIDUALS, AND THE NATION

This appendix provides: (i) a description of potentially useful inputs to the risk determination task including considerations for uncertainty of determinations; (ii) exemplary assessment scales for assessing the levels of risk; (iii) tables for describing content (i.e., data inputs) for adversarial and non-adversarial risk determinations; and (iv) templates for summarizing and documenting the results of the risk determination Task 2-6. The assessment scales in this appendix can be used by organizations as a starting point with appropriate tailoring to adjust for any organization-specific conditions. Table I-5 (adversarial risk) and Table I-7 (non-adversarial risk) are the outputs from Task 2-6.

TABLE I-1: INPUTS – RISK

Description	Provided To		
	Tier 1	**Tier 2**	**Tier 3**
From Tier 1 (Organization level) - Sources of risk and uncertainty information identified for organization-wide use (e.g., specific information that may be useful in determining likelihoods such as adversary capabilities, intent, and targeting objectives). - Guidance on organization-wide levels of risk (including uncertainty) needing no further consideration. - Criteria for uncertainty determinations. - List of high-risk events from previous risk assessments. - Assessment scale for assessing level of risk, annotated by the organization, if necessary. (Table I-2) - Assessment scale for assessing the level of risk as a combination of likelihood and impact, annotated by the organization, if necessary. (Table I-3)	No	Yes	Yes *If not provided by Tier 2*
From Tier 2: (Mission/business process level) - Risk-related information and guidance specific to Tier 2 (e.g., risk and uncertainty information related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies).	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Risk-related information and guidance specific to Tier 3 (e.g., likelihood information affecting information systems, information technologies, information system components, applications, networks, environments of operation).	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	**Level of Impact**				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

TABLE I-4: COLUMN DESCRIPTIONS FOR ADVERSARIAL RISK TABLE

Column	Heading	Content
1	Threat Event	Identify threat event. (Task 2-2; Table E-1; Table E-2; Table E-5; Table I-5.)
2	Threat Sources	Identify threat sources that could initiate the threat event. (Task 2-1; Table D-1; Table D-2; Table D-7; Table I-5.)
3	Capability	Assess threat source capability. (Task 2-1; Table D-3; Table D-7; Table I-5.)
4	Intent	Assess threat source intent. (Task 2-1; Table D-4; Table D-7; Table I-5.)
5	Targeting	Assess threat source targeting. (Task 2-1; Table D-5; Table D-7; Table I-5.)
6	Relevance	Determine relevance of threat event. (Task 2-2; Table E-1; Table E-4; Table E-5; Table I-5.) If the relevance of the threat event does not meet the organization's criteria for further consideration, do not complete the remaining columns.
7	Likelihood of Attack Initiation	Determine likelihood that one or more of the threat sources initiates the threat event, taking into consideration capability, intent, and targeting. (Task 2-4; Table G-1; Table G-2; Table I-5.)
8	Vulnerabilities Predisposing Conditions	Identify vulnerabilities which could be exploited by threat sources initiating the threat event, the severity of the vulnerabilities, the predisposing conditions which could increase the likelihood of adverse impacts, and the pervasiveness of the predisposing conditions. (Task 2-5; Table F-1; Table F-2; Table F-3; Table F-4; Table F-5; Table F-6; Table I-5.)
9	Likelihood that Initiated Attack Succeeds	Determine the likelihood that the threat event, once initiated, will result in adverse impact, taking into consideration threat source capability, vulnerabilities, and predisposing conditions. (Task 2-4; Table G-1; Table G-4; Table I-5.)
10	Overall Likelihood	Determine the likelihood that the threat event will be initiated and result in adverse impact (i.e., combination of likelihood of attack initiation and likelihood that initiated attack succeeds). (Task 2-4; Table G-1; Table G-5; Table I-5.)
11	Level of Impact	Determine the adverse impact (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) from the threat event. (Task 2-5; Table H-1, Table H-2; Table H-3; Table H-4; Table H-5; Table I-5.)
12	Risk	Determine the level of risk as a combination of likelihood and impact. (Task 2-6; Table I-1; Table I-2; Table I-3; Table I-5.)

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11	12
Threat Event	Threat Source	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting							

TABLE I-6: COLUMN DESCRIPTIONS FOR NON-ADVERSARIAL RISK TABLE

Column	Heading	Content
1	Threat Event	Identify threat event. (Task 2-2; Table E-1; Table E-3; Table E-5; Table I-7.)
2	Threat Sources	Identify threat sources that could initiate the threat event. (Task 2-1; Table D-1; Table D-2; Table D-8; Table I-7.)
3	Range of Effects	Identify the ranges of effects from the threat source. (Task 2-1; Table D-1; Table D-6; Table I-7.)
4	Relevance	Determine relevance of threat event. (Task 2-2; Table E-1; Table E-4; Table E-5; Table I-7.) If the relevance of the threat event does not meet the organization's criteria for further consideration, do not complete the remaining columns.
5	Likelihood of Threat Event Occurring	Determine the likelihood that the threat event will occur. (Task 2-4; Table G-1; Table G-3; Table I-7.)
6	Vulnerabilities Predisposing Conditions	Identify vulnerabilities which could be exploited by threat sources initiating the threat event, the severity of the vulnerabilities, the predisposing conditions which could increase the likelihood of adverse impacts, and the pervasiveness of the predisposing conditions. (Task 2-5; Table F-1; Table F-2; Table F-3; Table F-4; Table F-5; Table F-6; Table I-7.)
7	Likelihood that Threat Event Results in Adverse Impact	Determine the likelihood that the threat event, once initiated, will result in adverse impact, taking into consideration vulnerabilities and predisposing conditions. (Task 2-4; Table G-1; Table G-4; Table I-7.)
8	Overall Likelihood	Determine the likelihood that the threat event will occur and result in adverse impacts (i.e., combination of likelihood of threat occurring and likelihood that the threat event results in adverse impact). (Task 2-4; Table G-1; Table G-5; Table I-7.)
9	Level of Impact	Determine the adverse impact (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) from the threat event. (Task 2-5; Table H-1, Table H-2; Table H-3; Table H-4; Table H-5; Table I-7.)
10	Risk	Determine the level of risk as a combination of likelihood and impact. (Task 2-6; Table I-1; Table I-2; Table I-3; Table I-7.)

TABLE I-7: TEMPLATE – NON-ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10
Threat Event	Threat Source	Range of Effects	Relevance	Likelihood of Event Occurring	Vulnerabilities and Predisposing Conditions	Likelihood Event Results in Adverse Impact	Overall Likelihood	Level of Impact	Risk

APPENDIX J

RISK PRIORITIZATION

APPROACHES TO ESTABLISHING TRUST RELATIONSIPS

A risk assessment, may identify a number of risks that appear to be of similar ranking (e.g., 78, 82, 83) or severity (e.g., moderate, high). When too many risks are clustered at or about the same level, a method is needed to prioritize risk responses and where to apply limited resources. Such a method should be tied to mission/business needs and maximize the use of available resources. A rational and common sense prioritization is a key component of risk-based protection and becomes necessary when requirements cannot be fully satisfied. To adequately defend risk response decisions made by senior leaders/executives (e.g., why certain risks were or were not mitigated), decision makers should know or be able to obtain the answers to the following questions:

In the event the identified risk (or set of risks) materialized—

- How critical would the *immediate* impact be to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation?
- How critical would the *future* impact be to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation?

The answers to the above questions provide the basis for a justifiable prioritization that is based on current and future organizational needs. Mission/business owners (or their designees) and mission/business subject matter experts can be consulted to obtain the most complete and up-to-date information.

These first two questions are tied directly to strategic and tactical operational considerations. Applying the first two questions above may or may not provide sufficient differentiation between risks for identifying which risks require greater attention for mitigation. Senior leaders/executives must decide whether a critical mission/business need today warrants jeopardizing the future capabilities of the organization. If needed, repeat this process for risks with less severity based on current and future capabilities.

Next, answer the following questions to further refine a group of risks with the same or similar rating.

- What is the expected loss from a single occurrence of the threat?
- If the risk can materialize more than once, what is the overall expected loss for the time period of concern?

In the event that recovery cost for a risk materializing once, is expected to be equal to or greater than the investment in the asset, organizations consider addressing the risk to the greatest extent possible or revisiting other ways of fulfilling the mission/business activities.

The remainder of the questions can be used to better understand the relationship of a particular risk and/or mitigation to other risks and/or mitigations. If a risk materializes that is closely related to multiple risks, it is likely that a cluster of risks will materialize at or near the same time.

Managing the adverse impact from one threat occurrence may be possible; managing multiple risks of high impact that materialize at the same time may be beyond the capacity of the organization and therefore needs to be managed much more closely.

Will the materialization of a particular risk result in:

- A high likelihood or virtual certainty in other identified risks materializing?
- A high likelihood or virtual certainty in other identified risks *not* materializing?
- No particular effect on other identified risks materializing?

If a risk is highly coupled to other risks or seen as likely to lead to other risks materializing (whether the risk is the cause or materializes concurrently), such risks are given extra attention and are likely to warrant resources applied to them in hopes of preventing multiple risks from materializing at or near the same time. If a risk materializing will actually decrease the likelihood of other risks materializing, then further analysis is warranted to determine which risks become a lower priority to mitigate. To maximize the use of available resources within the organization, the cost of risk mitigation considers whether the mitigation addresses: (i) more than one risk; or (ii) one or more risks completely, partially, or not at all.

APPENDIX K

SUMMARY OF TASKS

RISK ASSESSMENT TASKS AND ASSOCIATED RISK TABLES

TABLE K-1: SUMMARY OF RISK ASSESSMENT TASKS

TASK	TASK DESCRIPTION
Step 1: Prepare for Risk Assessment	
TASK 1-1 IDENTIFY PURPOSE Section 3.1	Identify the purpose of the risk assessment in terms of the information the assessment is intended to produce and the decisions the assessment is intended to support.
TASK 1-2 IDENTIFY SCOPE Section 3.1	Identify the scope of the risk assessment in terms of organizational applicability, time frame supported, and architectural/technology considerations.
TASK 1-3 IDENTIFY ASSUMPTIONS AND CONSTRAINTS Section 3.1	Identify the specific assumptions and constraints under which the risk assessment is conducted.
TASK 1-4 IDENTIFY INFORMATION SOURCES Section 3.1	Identify the sources of threat, vulnerability, and impact information to be used in the risk assessment.
TASK 1-5 DEFINE RISK MODEL Section 3.1	Define (or refine) the risk model to be used in the risk assessment.
Step 2: Conduct Risk Assessment	
TASK 2-1 IDENTIFY THREAT SOURCES Section 3.2, Appendix D	Identify and characterize the threat sources of concern to the organization, including the nature of the threats and for adversarial threats, capability, intent, and targeting characteristics.
TASK 2-2 IDENTIFY THREAT EVENTS Section 3.2, Appendix E	Identify potential threat events, relevance to the organization, and the threat sources that could initiate the events.
TASK 2-3 IDENTIFY VULNERABILITIES AND PREDISPOSING CONDITIONS Section 3.2, Appendix F	Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts to the organization.

TASK	TASK DESCRIPTION
TASK 2-4 DETERMINE LIKELIHOOD Section 3.2, Appendix G	Determine the likelihood that threat events of concern result in adverse impact to the organization, considering: (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities and predisposing conditions identified; and (iii) organizational susceptibility reflecting safeguards/countermeasures planned or implemented to impede such events.
TASK 2-5 DETERMINE IMPACT Section 3.2, Appendix H	Determine the adverse impact to the organization from threat events of concern considering: (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities and predisposing conditions identified; and (iii) organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.
TASK 2-6 DETERMINE RISK Section 3.2, Appendix I	Determine the risk to the organization from threat events of concern considering: (i) the impact that would result from the events; and (ii) the likelihood of the events occurring.
Step 3: Maintain Risk Assessment	
TASK 3-1 MONITOR RISK FACTORS Section 3.3	Conduct ongoing monitoring of the factors that contribute to changes in risk to organizational operations and assets, individuals, other organizations, or the Nation.
TASK 3-2 UPDATE RISK ASSESSMENT Section 3.3	Update existing risk assessment using the results from ongoing monitoring of risk factors.