CHAPTER 8 PART I
RISK MANAGEMENT METHODOLOGY

1 BACKGROUND

The current heightened sense of national alert and the administration's focus on the security of Federal Information Technology (IT) assets requires that USDA take immediate action to secure our systems. In addition, the General Accounting Office (GAO) and USDA's Office of Inspector General (OIG) have issued reports over the past several years that describe persistent computer security weaknesses in the federal sector, which support this requirement. These pervasive weaknesses introduce risks that could allow malicious or unintentionally dangerous users to read, modify, delete or otherwise damage information or disrupt operations. The reasons or motivations of the attacker could include curiosity, criminal activities, sabotage, espionage or terrorism and could seriously affect USDA's mission.

Protection of information assets and maintaining the availability, integrity and confidentiality of USDA's information technology assets and telecommunications resources are vital in meeting USDA's program delivery requirements. Implementation of security measures such as a risk management program, effective security controls, certification and accreditation of IT systems and updated security plans are vital components in our response to this situation. This chapter concerns the implementation of USDA Risk Management (RM) Program. RM includes a structured approach to assessing risks, identifying vulnerabilities, and implementing appropriate mitigation strategies.

2 POLICY

USDA agencies and staff offices will perform formal Risk Assessments (RA) of all IT systems. Agency RAs can be conducted in accordance with the USDA Risk Assessment Methodology, Table 1, in this chapter or the Risk Assessment Methodology defined in NIST 800-30. Essentially both methodologies contain the same steps although not in the same order. Both are acceptable. A formal system risk analysis is required every three years or when a major change in made in a system. Major changes are defined as modifications to the system that affect the security controls and

which render the system vulnerable to compromise or intrusion. Waiver requests will be considered for extensions in compliance time only; all USDA IT systems will undergo regular risk assessments. USDA agencies and staff offices will include the cost for IT system mitigations in budgetary planning and prepare a business case to ensure that funding is available to implement protection against identified vulnerabilities.

Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation time; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each agency report this policy exception as a Plan of Action & Milestone (POA&M) in their FISMA reporting until full compliance is achieved. Interim exceptions cannot extend beyond the fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with a updated timeline for completion. CS will monitor all approved exceptions.

3 RESPONSIBILITIES

a The Associate CIO for Cyber Security will:

(1) Publish and update a USDA Risk Assessment Methodology policy to be used by agencies and staff offices;

(2) Assist agencies and staff offices in the secure implementation of the USDA Risk Assessment Program;

(3) Establish a department-wide contractual vehicle for providing risk assessment services;

(4) Review agency and staff office policy exception requests concerning this policy in a timely manner;

(5) Conduct periodic reviews of agencies and staff offices to ensure that IT systems have a new or updated risk assessments in accordance with this policy;

b Agency Management and Information Technology Officials or Chief Information Officer will:

(1) Actively implement this policy, including the use of the USDA Risk Assessment Methodology, Table 1, to conduct assessments of all IT systems and to implement risk mitigations;

(2) Ensure all IT professionals understand their role in the risk assessment process, with special emphasis on system owners, developers, security officers and system administrators;

(3) Use a formal System Development Life Cycle (SDLC) and Configuration Management (CM) approach in the management of IT systems to support the internal Risk Assessment Program;

(4) Ensure annual and quarterly FISMA reports reflect RAs performed for IT systems and that FISMA Plans of Actions and Milestones include action items to mitigate security weaknesses discovered through the RA process;

(5) Develop and submit IT budget, funding requests and business cases to implement necessary risk mitigations on agency systems, as required;

(6) Annually update System Security Plans to include RA date, major findings, mitigations and timeframes for action;

(7) Document residual risk in a Residual Risk Statement and ensure that remediations are made in the system or that the DAA continues to accept these risks in writing; and

(8) Take action to request a formal waiver for systems that do not comply with this policy.

c Agency Information System Security Program Managers (ISSPM) will:

(1) Read and become familiar with RA policy and agency roles;

(2) Support the implementation of the agency internal Risk Management Program;

(3) Participate in system risk assessments and document preparation, as required;

(4) Update System Security Plans with Risk Assessment information and participate in the development of risk mitigations;

(5) Participate in the development of cost estimates and submission of funding requests for mitigations, as required;

(6) Review and monitor all agency IT systems to ensure RAs are conducted as required by this policy; report non-compliant systems through the agency chain of command on a quarterly basis unless the system is under an approved formal exception; monitor remediation of non-compliance systems until compliance is achieved; and

(7) Participate in the development of agency policy exception requests, as necessary.

-END-

Table 1

USDA

Risk Assessment Methodology

February 11, 2003

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF APPENDICES

Introduction

The United States Department of Agriculture (USDA) positively impacts the many aspects of American and foreign constituents. The Department's diverse and complex missions serve the public in providing assistance in rural development, food, nutrition, and consumer services, management of national forests and grasslands, economic and scientific agricultural research, natural resource conservation and development, and administrative support to carry on these missions. In addition, the Department provides crucial emergency support function roles during outbreaks of human, animal, and plant diseases, and provides food during natural disasters. The USDA manages land and facilities under USDA jurisdiction and partners with local authorities to direct the rural fire control activities for national forests. Department employees inspect livestock, poultry, and other products to ensure food safety and wholesomeness.
The protection of information assets and maintaining the availability, integrity, and confidentiality of USDA Information Technology (IT) systems and telecommunications resources is vital in meeting the USDA's mission requirements. Consequently, information security has emerged as a top priority for the USDA. As technology has enhanced the ability to instantly share information between computers and networks, information security has also made USDA organizations more vulnerable to a wider family of threats including unlawful and destructive penetration and disruptions.

The USDA's security mandate for its information systems comes from the *E-Government Act of 2002, Title III, Federal Information Security Management Act*. This law and guidance from the Office of Management and Budget provides the Department with basic security requirements. In addition, the USDA follows the Homeland Security Directive HSPD-7, Critical Infrastructure Identification, Prioritization and Protection, which explains the key elements of the Administration's policy on critical infrastructure protection. HSPD-7 calls for a national effort to insure the security of the United States' increasingly vulnerable and interconnected infrastructure, particularly its cyber systems. These requirements, along with the President's own concerns, have led the USDA Secretary to direct the Office of the Chief Information Officer (OCIO) in a strategy to improve USDA's cyber security. A key aspect of this strategy is the implementation of an information systems risk management program. The USDA must implement a structured approach to assess risks to USDA information assets and identify vulnerabilities as well.

1. Purpose

The U.S. General Accounting Office (GAO) reports, issued over the past several years, describe persistent computer security weaknesses that place Federal operations such as national defense, law enforcement, air traffic control, and benefit payments at risk of disruption as well as fraud and inappropriate disclosures. These weaknesses include:

- Controls over access to sensitive and critical system data
- Controls over software development and changes
- Continuity of services plans

These types of weaknesses introduce risks that could allow malicious or unintentionally dangerous users to read, modify, delete, or otherwise damage information or disrupt operations for diverse purposes (i.e., curiosity, criminal activities, sabotage, espionage, or terrorism).

Whatever the reasons or motivations of the attacker (intentional or unintentional), the USDA mission could be adversely impacted. In order to minimize the disruption to the stated USDA mission, the USDA business manager or system owner must have a tool with which to evaluate the possible risks and their potential mitigations, in order to maximize the effectiveness of the application and limited resources. This document provides a methodology for conducting risk assessments at both the application and system level. This methodology serves as the model with which all USDA system owners will conduct risk assessments.

2. Scope

This risk assessment methodology is applicable to all USDA IT systems, general support or major application as well as systems that are classified and unclassified. This methodology follows guidance provided in NIST SP 800-30 *Risk Management Guide for Information Technology Systems,* dated January 2002, NIST SP 800-12 *An Introduction to Computer Security: The Handbook,* October 1995, NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996, NIST SP 800-26 *Security Self-Assessment Guide for Information Technology Systems,* August 2001, the *USDA Cyber Security Manual, Series 3500,* and other federal guidance (see Appendix B, Table B-1). USDA directives may be found on the web at the following URL: http://www.usda.gov/ocio/directives/DR/. As a methodology, the processes described in this document provides the USDA Department and Agency Program Manager(s) or System Owner(s) a flexible guideline to evaluate the risks posed by their respective IT systems.

It should be understood that requirements in other disciplines or areas that may overlap into IT security must be taken into consideration, but in general, are not addressed directly in the NIST guidance as part of the risk assessment process. Therefore, for the purpose of this Risk Assessment Methodology these disciplines/areas are not directly addressed.
The risk assessment process is a subordinate activity of the Certification and Accreditation (C&A) process, which is itself a subordinate System Life Cycle (SLC) task. There is a great inter-dependency between the three processes. The risk assessment process needs information from the C&A and SLC processes, while the C&A and SLC processes cannot effectively be completed without a risk assessment.

Risk Assessment Background

Information security has emerged as a top priority for the Department of Agriculture. As technology has enhanced the ability to share information instantaneously between computers and networks, it has also made USDA organizations more vulnerable to a wider family of threats including unlawful and destructive penetration and disruptions. Protection of information assets and maintaining the availability, integrity, and confidentiality of USDA information technology systems and telecommunications resources are vital in meeting USDA's program delivery requirements. A key aspect of protecting information assets is the implementation of an information systems risk management program. In particular, USDA must implement a structured approach to assess risks to USDA information assets and identify vulnerabilities.

3. USDA Risk Assessment Roles and Responsibilities

This section presents the USDA Risk Assessment Roles and Responsibilities. USDA's Office of the Chief Information Officer, with the support of Cyber Security (CS), has overall responsibility for the security of the USDA IT security infrastructure.

This section outlines the overall risk assessment roles and responsibilities as outlined in NIST SP 800-30 *Risk Management Guide for Information Technology Systems*, January 2002 and their relation to the USDA organization. Although, the Office the Chief Information Officer is delegated with overall responsibility for risk management activities they need not perform the actual work, but rather ensure that the work is completed on time, and in a manner consistent with USDA and federal standards. Usually, risk assessment activities are conducted in a distributed manner, consistent with distributed workflows. This process is prevalent in the USDA business culture. Outlined below responsibilities are delineated for the various activities that comprise the Risk Assessment process.

- *USDA Chief Information Officer (CIO) & Senior Management* – under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also access and incorporate results of risk assessment activity into the decision making process.
- *USDA Associate CIO for Cyber Security (ACIO-CS)* – leads this office and is responsible for executing and monitoring the USDA agency-wide Security Program, ensuring security policies are founded on a continuous risk management cycle, understanding and allocating USDA resources to execute the Security Program, managing system technical, operational, and management controls to determine risk, determining the acceptable residual risk level, and ensuring the USDA Security Awareness and Training Program is implemented and conducted annually.
- *Agency Chief Information Officer (CIO)* – is responsible for the agency's IT planning, budgeting, and performance including its information security components. Decisions made by this official should be based on an effective risk management program.
- *Agency Information Systems Security Program Manager (ISSPM)*– the ISSPM, is responsible for ensuring security activities are integrated into the SLC for the business function. This includes ensuring that a Data Sensitivity assessment is completed in the Initiation Phase to completion of the Certification and Accreditation in the Operational/Maintenance Phase. IT security program managers and computer security officers are responsible for their organizations' security programs, including risk management. Therefore, they play a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize risks to the IT systems that support their organizations' missions. ISSPMs also act as major consultants in support of senior management to ensure that this activity takes place on an ongoing basis. It is important for agency ISSPMs to not only have an understanding of a comprehensive risk management program, but also an understanding of how the business program is integrated with the USDA Application SLC.
- *System and Information Owners* -The system and information owners are responsible for ensuring that proper controls are in place to address integrity,

confidentiality, and availability of the IT systems and data they own. Typically the system and information owners are responsible for changes to their IT systems. Thus, they usually have to approve and sign off on changes to their IT systems (e.g., system enhancement, major changes to the software and hardware). The system and information owners must therefore understand their role in the risk management process and fully support this process.

- *USDA Business and Functional Manager*– The managers responsible for business operations and IT procurement process must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accomplishment. Their involvement in the risk management process enables the achievement of proper security for the IT systems, which, if managed properly, will provide mission effectiveness with a minimal expenditure of resources.
- *USDA System Administrators* – USDA departmental and agency system developers ensure that IT system business and regulatory requirements are defined in the Initiation Phase, developed in the Development/Acquisition phase, implemented and tested in the Implementation Phase, and moved into a production status in the Operational Maintenance Phase. USDA administrators upgrade operating systems and apply system and security patches as well as make system changes based on USDA's business and IT needs. Administrators are defined as programmers, database administrators, engineers, etc., and may be USDA personnel, contractor, or mixture of both.
- *USDA Program Office IT System Administrator* – USDA departmental and agency System Administrators monitor and manage life-cycle activities, audit activities, assist with implementing access controls, manage computer incidents, and install security patches.
- *USDA System End Users* – USDA end users must understand day-to-day operational risk and how to apply mitigation techniques when required.

Step No.	1	2	3	4	5	6	7
Step Name	System Characterization	Conduct Vulnerability and Control Analysis	Conduct Threat Analysis	Conduct Impact Analysis	Develop a Risk Mitigation Strategy	Determine the Risk Level	Report the Residual Risk
USDA Roles	ACIO-CS, ISSPM, Program Manager & Business Managers	ACIO-CS, ISSPM, Program Manager & IT Developers	ACIO-CS,ISSPM, Program Office IT System Admins	ACIO-CS, ISSPM, Business Mgrs	ACIO-CS, ISSPM, Program Manager	ACIO-CS, ISSPM, Program Manager	ACIO-CS, ISSPM, Program Manager
Support Description	• Understand USDA risk and business requirements • Manage agency risk activities	• Allocate and manage vulnerability assessment resources and activities	• Manage threat analysis and scheduled activities	• Coordinate impact decisions and solutions with system owners	• Coordinate security controls that mitigate risk based on USDA policy, mission impact, and federal guidance	• Determine impact criticality to USDA and the nation	• Manage USDA risk mitigation plans and future risk
Methodology Activities	• Identify system mission • Review system architecture and determine system boundaries, interfaces and data flow • Determine data categories and sensitivity • Determine system lifecycle phase • Understand system users • Define system security policies	• Conduct manual assessments • Conduct automated scans, penetration tests, and ST&Es • Review previous security plans and risk assessments	• Determine threat types • Develop a listing of threat sources • Determine probability of threat occurrence	• Consider data categories • Determine mission impact severity in terms of confidentiality, integrity,and availability	• Review threat list • Consider impacts • Implement countermeasures • Review available resources • Determine mitigation priority list	• Determine threat probability and impact criticality	• Review threats/risk that will not be mitigated • Document remaining threats/risk for future action • Include residual risk in Certification and Accreditation package

Figure 1: Risk Assessment Steps and Roles

Figure 1, Risk Assessment Steps and Roles defines the key steps in this process and the individuals responsible for completing this part of the process.

2. Risk Theory

Absolute security, which assures 100 percent protection against all possible threats, at all times, is unachievable. Therefore, USDA requires a risk-based management process that weighs potential impacts (or losses), which may be expected to occur in the presence of a given vulnerability (with a particular threat probability), against the business resource cost of mitigating or eliminating the risk. The qualitative expression of this approach is listed below.

$$R_{(isk)} = \frac{V_{(ulnerability)} \times T_{(hreat)} \times I_{(mpact)}}{C_{(ountermeasures)}}$$

Risk assessments evaluate the sensitivity and criticality of the system or application data to the vulnerabilities, threats, impacts, and potential countermeasures that may exist in its environment. A risk assessment includes the following activities:

- System Characterization
- Conduct Vulnerability and Control Analysis
- Conduct Threat Analysis
- Conduct Impact Analysis
- Develop a Risk Mitigation Strategy
- Determine the Risk Level
- Develop Business Case
- Report the Residual Risk

3. Risk Assessment and the System Life-Cycle (SLC) Phases

The risk assessment process is one of the cyclic sub-activities presented in the NIST SP 800-12 *An Introduction to Computer Security: The Handbook,* October 1995, NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996, NIST SP 800-30 *Risk Management Guide for Information Technology Systems,* January 2002, and NIST SP 800-27 *Engineering Principles for Information Technology Security (A Baseline for Achieving Security*), June 2001. This document reflects the Risk Assessment Methodology Flowchart from NIST SP 800-30 as a crosswalk to the General USDA Risk Assessment Methodology. Both methodologies can be employed by agencies and are equally acceptable in establishing a formal Risk Methodology.

The Risk Assessment process must be tailored to the particular phase of the SLC, in which the system is operating. Specifically, some activities may not take place in all phases of the SLC, or may take on a modified methodology. Additionally, the entry point for the system under assessment must be considered. When assessing a system that is in a phase other than Initiation, provisions should be made for those products and activities that may be missing. As an example, when assessing a "legacy" system a quick inspection will reveal the system to be in the Operations and Maintenance Phase. Part of the assessment will be determining which, or how many, activities need to be completed from earlier phases of the SLC. Normally, the only other SLC Phases that can be entered, other than Initiation, are the Development/Acquisition,

Operations, and Maintenance Phases. The Implementation Phase is typically just a bridge between Development and Operations, and the Disposal Phase is the end of the cycle (entering here makes no sense). Figure 2 represents the five SLC phases in which a system might logically reside and the computer security activities associated with each phase.

This process should also be tied to the Capital Planning and Investment Control (CPIC) as routine risk assessments are designed to pinpoint weaknesses in USDA's new initiatives. Included in this material is Figure 3 depicting the Risk Assessment Phases and the corresponding Capital Planning and Investment Control (CPIC) Phase. This chart should be used to correlate both activities, which are all part of an effective SLC. Risk assessments and CPIC activities also support the overall Certification and Accreditation process. Therefore, it is critical that each agency link these activities together into one overall process supporting the investment or system.

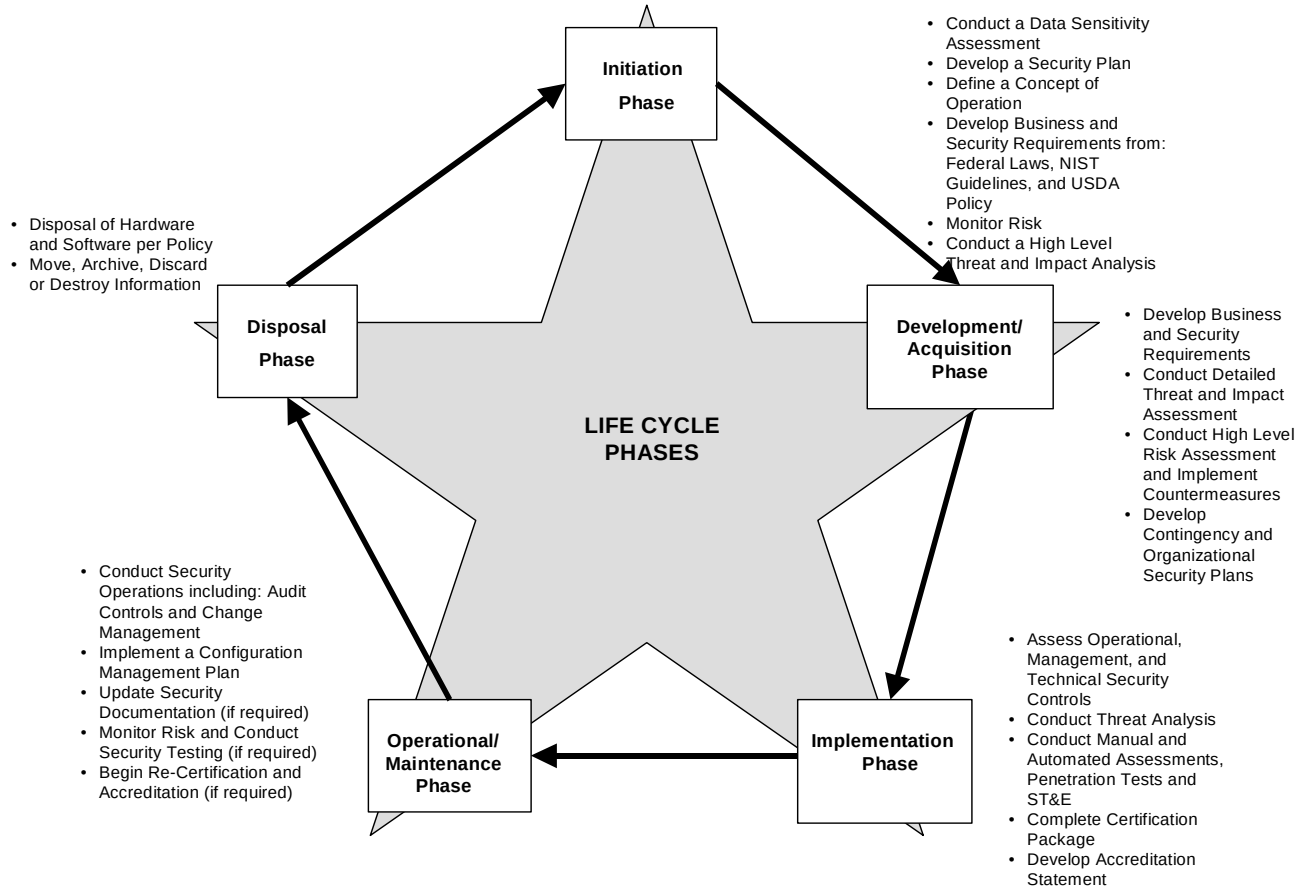

Figure 2: The Life-Cycle Phases and Risk Assessment Activities

RA PHASE	CPIC
Initiation	Pre-Select/Select
Development/Acquisition	Select
Implementation	Control
Operational/Maintenance	Evaluate/Steady State
Disposal	Steady State

15. Figure 3: Risk Assessment Crosswalk to CPIC

16. The Initiation Phase

This phase is the starting point of any IT system, although it may be done informally for small systems. The Initiation Phase includes completing a needs assessment, developing an operation concept, requirements, and architecture. A risk assessment can be initiated at different phases of the system life cycle. Therefore, not all risk assessment activities may apply to every system within a specific system life cycle phase. The USDA ISSPM and IT and Business Functional Program Managers (PMs) must understand which activities will and will not be applicable. However, better efforts made in this phase will result in a more effective and easier to maintain system in the future. In this phase of the lifecycle, the primary focus is to gather information in preparation for the following stages. Figure 4 discusses specific roles and activities in this phase.

INITIATION PHASE							
	System Characterization	**Vulnerability and Control Analysis**	**Threat Analysis**	**Impact Analysis**	**Risk Mitigation**	**Risk Level**	**Residual Risk**
USDA Roles	ACIO-CS, ISSPM, Program Manager, Business and Functional Manager	N/A	ACIO-CS, ISSPM, Program Manager	System Program Manager, Business and Functional Manager	ACIO-CS, ISSPM, Program Manager	ACIO-CS, ISSPM, NTSO, Program Manager	N/A
Activities	Conduct a Data Sensitivity Assessment Develop a Security Plan Define a Concept of Operation Develop Business and Security Requirements from: Federal Laws, NIST Guidelines, and USDA Policy	N/A	Conduct a High Level Threat Analysis	Conduct a High Level Mission Impact Analysis	N/A	Monitor Risk	N/A
Products	Concept of Operation Needs Assessment Security Plan	N/A	High Level Threat Assessment	Impact Analysis	Security Architecture Plan Security Requirements	N/A	N/A

Figure 4: Initiation Phase Risk Assessment Activities

17. The Development/Acquisition Phase

The Development/Acquisition Phase takes the information that was gathered in the Initiation Phase, and uses it to continue developing system and security requirements and set system parameters and conditions. In addition, at this point system developers must consider the myriad of laws, regulations and policies that will constrain the system. Outside the regulatory environment, the system developers must also ensure that the system is able to function in such a way to add value to the business owner's processes. From a security standpoint, this is where a high level or "paper" risk assessment is completed. This high-level risk assessment keeps the system design focused in the proper direction to meet its ultimate need. During this phase, a detailed threat and impact analysis is completed. Figure 5 discusses specific roles and activities in this phase.

DEVELOPMENT/ACQUISITION PHASE							
	System Characterization	**Vulnerability and Control Analysis**	**Threat Analysis**	**Impact Analysis**	**Risk Mitigation**	**Risk Level**	**Residual Risk**
USDA Roles	ACIO-CS, ISSPM, Program Manager, IT Developers	ACIO-CS, ISSPM, IT Developers, Program Manager	ACIO-CS, ISSPM, IT Developers, Program Manager	ACIO-CS, ISSPM, Program Manager, IT Developers	ACIO-CS, ISSPM, IT Developers	ACIO-CS, ISSPM, Program Manager	N/A
Activities	Define Security Architecture Continue Developing Security Requirements Update Security Plan Develop Contingency and Organizational Security Plans	Evaluate Standard Configurations	Conduct Detailed Threat Analysis	Conduct Detailed Impact Analysis	Develop High Level Risk Strategy and Implement Counter-measures Begin System Certification activities	Conduct High Level Risk Assessment	N/A
Products	Updated Security Plan, Contingency Plan and Organizational Security Plan Security Design Document	Initial Vulnerability Assessment	Threat List	Criticality Analysis	Risk Mitigation Strategy	High Level Risk Assessment	N/A

Figure 5: Development/Acquisition Phase Risk Assessment Activities

18. The Implementation Phase

During this phase, the system performs its intended business function. The Implementation Phase includes all those activities that occur prior to the system being placed into the "Production" status. It is possible that IT systems can enter the risk assessment at different phases in the SLC. Often legacy systems go into the risk assessment process in this phase, as they did not participate in the SLC from their inception. The significant activity of the Implementation Phase is the system Certification and Accreditation, of which risk assessment is a part. Figure 6 discusses roles and activities in this phase.

IMPLEMENTATION PHASE							
	System Characterization	**Vulnerability and Control Analysis**	**Threat Analysis**	**Impact Analysis**	**Risk Mitigation**	**Risk Level**	**Residual Risk**
USDA Roles	ACIO-CS, ISSPM, Program Manager, Program Office, IT System Admins, System Developers	ACIO-CS, ISSPM, Program Manager, Program Office, IT System Admins, System Developers	ACIO-CS, ISSPM, Program Manager	Program Manager	ACIO-CS, ISSPM, Program Manager	ACIO-CS, ISSPM, Program Office IT System Admins	ACIO-CS, ISSPM, Program Manager
Activities	Implement Security Architecture Develop Security Requirements Document	Review Intercon. Sec. Agree. (ISA) Assess Management, Operational, and Technical Controls Conduct Manual Assessments, Automated Assessments, Penetration Tests, ST&E	Conduct Threat Analysis	Conduct Criticality Analysis	Determine Risk Mitigations based on Vulnerabilities and Threats Implement Counter-measures	Qualify Risk Levels Complete the Certification Package Develop the Accreditation Statement	Residual Risk Analysis
Products	Security Design Document Security Plan	Technical, Management and Operations Vulnerability Assessment	Threat Analysis	Impact Analysis		Overall Risk Levels Complete Certification Package with Accreditation Statement	Risk Assessment Report Risk Statement

Figure 6: Implementation Phase Risk Assessment Activities

19. The Operational/Maintenance Phase

In this phase, the system continues to perform its stated mission. During this phase, the system is modified and hardware and software changes take place. The security architecture may change and hardware and software changes are tracked through configuration management and change control processes. New threats and risk factors might occur; therefore, security controls must be

consistently reviewed and updated as part of configuration management. Security plans and other system documentation must be updated when security architectural changes take place. Figure 7 discusses roles and activities in this phase.

OPERATIONAL/MAINTENANCE PHASE							
	System Characterization	**Vulnerability and Control Analysis**	**Threat Analysis**	**Impact Analysis**	**Risk Mitigation**	**Risk Level**	**Residual Risk**
USDA Roles	ACIO-CS, ISSPM, Program Manager, System Admins	ACIO-CS, ISSPM, System Admins	ACIO-CS, ISSPM, Program Manager	ACIO-CS, ISSPM, Program Manager	ACIO-CS, ISSPM, Program Manager	ACIO-CS, ISSPM, Program Manager, System Admins	ACIO-CS, ISSPM, Program Manager
Activities	Monitor Security Requirements and Make Changes When Required Implement a Configuration Management Plan	Continue Manual Assessments Continue Automated Assessments Conduct Penetration Tests and ST&E after System Changes	Monitor Threat	Monitor Impact to USDA Mission	Determine Risk Mitigations based on Vulnera-bilities and Threats Implement Additional Counter-measures If Required	Qualify Risk Levels	Residual Risk Analysis
Products	Configuration Management Plan Updated Security Architecture Updated Security Documentation	Updated Technical, Management and Operations Control Assessment	Updated Threat Analysis	Updated Impact Analysis	Updated Risk Mitigation Strategy	Updated Risk Levels	Updated Risk Assessment Report and Residual Risk Statement

Figure 7: Operational/Maintenance Phase Risk Assessment Activities

20. The Disposal Phase

Normally, the activities in this phase consist of monitoring the state of the system. The only risk related activity in the disposal phase is to ensure that data is disposed of in a manner consistent with USDA policy. If the system's data is no longer required, then it can simply be destroyed by approved means consistent with USDA policy. Usually, the system will be upgraded or some

part of the data will migrate to another IT system. It is important to ensure that adequate security controls have been implemented. Figure 8 discusses roles and activities in this phase.

DISPOSAL PHASE							
	System Characterization	**Vulnerability and Control Analysis**	**Threat Analysis**	**Impact Analysis**	**Risk Mitigation**	**Risk Level**	**Residual Risk**
USDA Roles	ACIO-CS, ISSPM, Program Manager, System Admins, IT Developers	N/A	N/A	N/A	N/A	N/A	N/A
Activities	Dispose of Hardware and Software per Policy Move, Archive, Discard or Destroy Information Sanitize Media	N/A	N/A	N/A	N/A	N/A	N/A
Products	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Figure 8: Disposal Phase Risk Assessment Activities

USDA Risk Assessment Methodology

Risk assessments are used to give USDA a baseline measurement of their system security controls. Therefore, this assessment provides USDA management with the capability to make informed decisions for allocating IT program resources needed to fulfill the business requirements.

The following sections detail how the specific Risk Assessment activities and products are implemented based on NIST SP 800-30 *Risk Management Guide for Information Technology Systems*. Figure 9 provides a pictorial representation of the General USDA Risk Assessment Methodology.

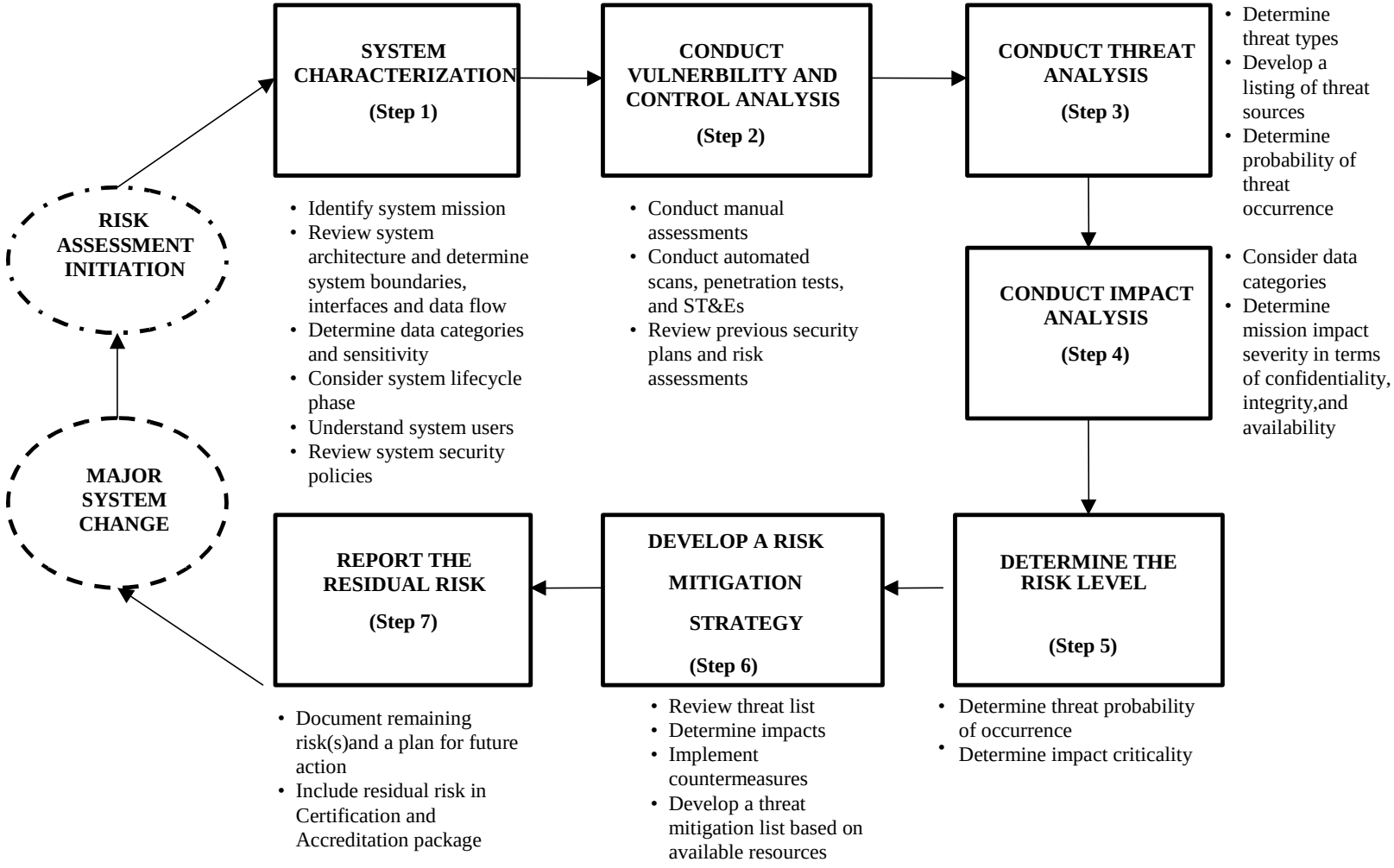

Figure 9: General USDA Risk Assessment Methodology

21. System Characterization

The first step in the risk assessment methodology is to characterize the system or application. This step establishes the scope of the risk assessment and provides information that is essential to defining the risk to the organizations mission or business functions. This step is necessary to ensure a clear understanding of the organization's mission, system operations and the nature of any potential mission impact. This step identifies system boundaries along with the IT resources and information that constitute it. These IT assets include:

- Business or technical requirements of the system
- Information infrastructure
- System or application data sensitivity
- Data flow(s)
- Interfaces to external systems
- System hardware and software
- Processes performed by the system
- Users of the system
- Applicable system security policies governing the system (agency policies, federal requirements, law)
- System security architecture that depicts the operating system, facilities where the system is contained, and information storage requirements of the system

The first step in characterizing an IT system is to define the business case for the system. The business case defines the system's function and importance to the Program and to USDA's overall mission. Often, the system can be defined in the negative, i.e. what would happen if the system did not exist or function correctly. The primary source of the business case information should be the System Owner, but secondary information may be obtained through system documents. For example, in order to expend capital funds on an IT project, the requesting Agency submits Office of Management and Budget (OMB) form 300B, which details the justification for the expenditure. Additionally, NIST SP 800-34 requires a Business Impact Analysis (BIA), which is also roughly equivalent to a business case. This BIA will also aid in the identification of the system's data needed for the next step of the process.
Figure 10 provides a model for identifying the sensitivity of data that is processed by a system or application. Identifying data sensitivity will help USDA understand the importance of their data and the loss to the organization. Sensitive unclassified or classified data will require special protection as well as controlled distribution and access. Identifying sensitive information and systems is essential to ensuring that USDA employs protective measures that are commensurate with the sensitivity of information processed, stored, or transmitted.

When determining the sensitivity of the data processed throughout an entire IT system, there is likely to be different levels processed concurrently. If multiple sensitivities exist on a single system, then the requirements must be met for all sensitivity levels. Since the protection requirements for more sensitive (or highly classified) levels of data usually encompass those of lower levels, one approach is to treat all data on the system as if it were of a sensitivity or classification of the highest level existing on the system. Other methods of protection may be employed as long as data is protected commensurate with its sensitivity.

Conflicts may arise when dealing with different levels of "sensitive but unclassified" (SBU) data. Some of the requirements can vary widely, and are not necessarily the same as other SBU data. However, it is the duty of the USDA system owner to know what kind of data is processed on their system and the associated protection requirements.

Sensitivity Level	**Description of Sensitivity Level** **Data stored, processed, or transported by computer or telecommunications resources, the inaccuracy, alteration, disclosure, or unavailability of which:**	**USDA-Specific Examples**
3	Would have an **IRREPARABLE IMPACT** on USDA missions, functions, image, customers or reputation, such that the catastrophic result would not be able to be repaired or set right again, or Could result in **LOSS OF MAJOR TANGIBLE ASSETS** or resources, including posing a threat to human life	Crop Futures (Statistical) Data [Time Sensitive] Network Data & Address Mapping Network and System Software Configuration Control Settings
2	Would have an **ADVERSE IMPACT** on USDA missions, functions, image, customers or reputation, such that the impact would place the USDA at a significant disadvantage, or Could result in **LOSS OF SIGNIFICANT TANGIBLE ASSETS** or resources	USDA Logistical Information USDA HR Data Privacy Act Data
1	Would have a **MINIMAL IMPACT** on USDA's missions, functions, image, customers or reputation, such that the impact would result in the least possible significant unfavorable condition with a negative outcome, or Could result in **LOSS OF SOME TANGIBLE ASSETS** or resources	USDA Org Chart Mission Statements Informational Announcements

Figure 10: Sensitivity Level and Description

22. Vulnerability and Control Analysis

The next step of the risk assessment is to conduct a vulnerability analysis. A vulnerability analysis identifies, evaluates, and reports security vulnerabilities in a system or application. The vulnerability analysis is based on system information that is captured using automated security tools as well as manual security assessments. This process identifies weaknesses or vulnerabilities that could be exploited deliberately or accidentally. This list is then used as input into further analysis, specifically the Level of Risk Determination.

System information is collected via the appropriate operating platform checklist, site surveys, and interviews with personnel responsible for the system, network-scanning tools, and available system and organizational documentation. Administrative and management assessments are applicable for all systems. A list of authorized checklist is found in Appendix C.

Specific types of vulnerabilities, and the processes needed to determine whether they are present, will vary depending on the nature of the system or application and whether the system is in the design, development, or test phase of the SLC or the operational phase that a production system resides.
If the system or application is in the *Initiation Phase* of the life cycle, then a risk-based approach would consider the design of the system architecture and it's associated security risks, determining security requirements along with conducting a data sensitivity assessment. Implementing effective security controls easily mitigate vulnerabilities discovered in this phase. If the system or application is in the *Developmental/Acquisition Phase,* then a threat and vulnerability analysis is conducted to assess the scope and magnitude of any associated risks. At this point and depending on the data's sensitivity, the system owner can *eliminate, mitigate or accept* those risks.

If the system is in the *Implementation or Operational/Maintenance Phase,* then the vulnerability analysis depends on automated software tools and manual inspections to assess the security controls that are in place and whether or not those controls are effective. Some proactive methods used to conduct a vulnerability analysis include:

- Automated vulnerability scan
- Network mapping
- Previous risk assessments, audit reports, security plans, and system test and evaluation report review

When considering the execution of a Vulnerability Assessment, the participants must keep in mind several factors. First, there may be prohibitions against system technical personnel running automated tools against their own systems. The reason for this is that the vulnerability testing and port scanning tools can have disastrous unintended consequences, such as taking IT systems off-line, without specialized tool operator training. In addition, attackers on the internal USDA network could use these tools as easily as legitimate users. Finally, some external (to USDA) oversight agencies do not see the validity in self-examination. Therefore, they demand that some outside organization be brought in to validate any results that may exist from previous assessments. Typically, external assessments can be brokered through the OCIO or the Office of the Inspector General (OIG). The *Disposal Phase* has no relevance to the vulnerability assessment. This phase disposes of system data and hardware or integrates data and hardware into another operational system.

23. Control Analysis

The next step is conducting a control analysis to assess the existence and implementation of *technical, operational and management* security controls. Some security controls serve to prevent a security event while others to detect security incidents. The overall objective of this step is to assess the status of present system security controls so that a detailed course of action can be developed to implement security controls that will provide the greatest return on investment. It is helpful to group the controls into three categories listed below. The information captured from existing security documentation and the information captured by assessing the implementation of current security controls is analyzed against the security requirements using both federal and USDA guidelines. The following lists of controls are not *all inclusive*, meaning each system owner must consider their individual areas of responsibility and apply security

controls using a risk-based approach which enable cost effective business decisions. General areas to be addressed include:

- System/data access controls
- System/data integrity controls
- Operating system implementation
- Auditing capabilities
- Security management procedures and controls
- Network security controls
- Disaster recovery

It is also helpful to note that some of the technical controls may be assessed during the automated assessments previously mentioned. The purpose of further manual reviews is to ensure that all the pertinent controls are assessed, and that all areas are adequately covered.

24. Controls Analyzed

In a control analysis, the following system or application security controls are analyzed:

Technical controls – are those safeguards incorporated into computer hardware, software or firmware and include:

- Access control mechanisms
- Antivirus software
- Identification & Authentication mechanisms
- Firewalls
- Encryption
- Audit trails
- Backups
- Intrusion detection systems

Operational controls - are those operational procedures, personnel and physical security measures established to provide an acceptable level of protection for computing resources and include:

- Security awareness and training
- Disaster recovery, contingency, and emergency plans
- Background investigations
- Security reviews and audits
- Separation of duties

Administrative and Management controls - are those security measures that focus on the management of the system and the management of risk. These measures include:

- Security reviews and assessments
- Risk assessments
- Rules of behavior

Again, it is important to consider each unique system or application to determine if additional technical, operational or management controls should be analyzed. Additionally, it is important

to detect and assess security mechanisms that *are not* included as part of the technical, operational, or management controls, but that present potential vulnerabilities.

25. Threat Analysis

The next step is conducting a threat analysis. A threat analysis is expressed as a function of the likelihood or the probability that a given threat-source will successfully exploit a given vulnerability. *It is important to note that without a vulnerability that can be exploited, a threat-source does not present a risk.* The information below details the threat analysis and includes the following activities:

- Identifying the threat source
- Determining the probability of the threat

26. Threat-Source Identification

Security threats can lead to loss or damage of USDA data and system components. Threat exploitation could result in the inability for the system/network administrators and end users to accomplish their mission in a timely manner. Alternate methods of obtaining access to USDA computing resources could be achieved, but this could result in errors, delays, and frustration. The lack of a comprehensive security program results in system vulnerabilities, which can be exploited causing realized threats. Both the source and the nature of possible threats must be understood in order to prevent the threat from occurring. Threats can occur from within USDA by an authorized user who has a valid user ID and password or from the outside by an unauthorized user with malicious intent. It is prudent to assume that when vulnerabilities exist there is a possibility the vulnerability will be exploited. This Risk Assessment chart below includes four broad threat types, which are stipulated to characterize a general threat environment. These threat types are summarized below in Figure 11 below.

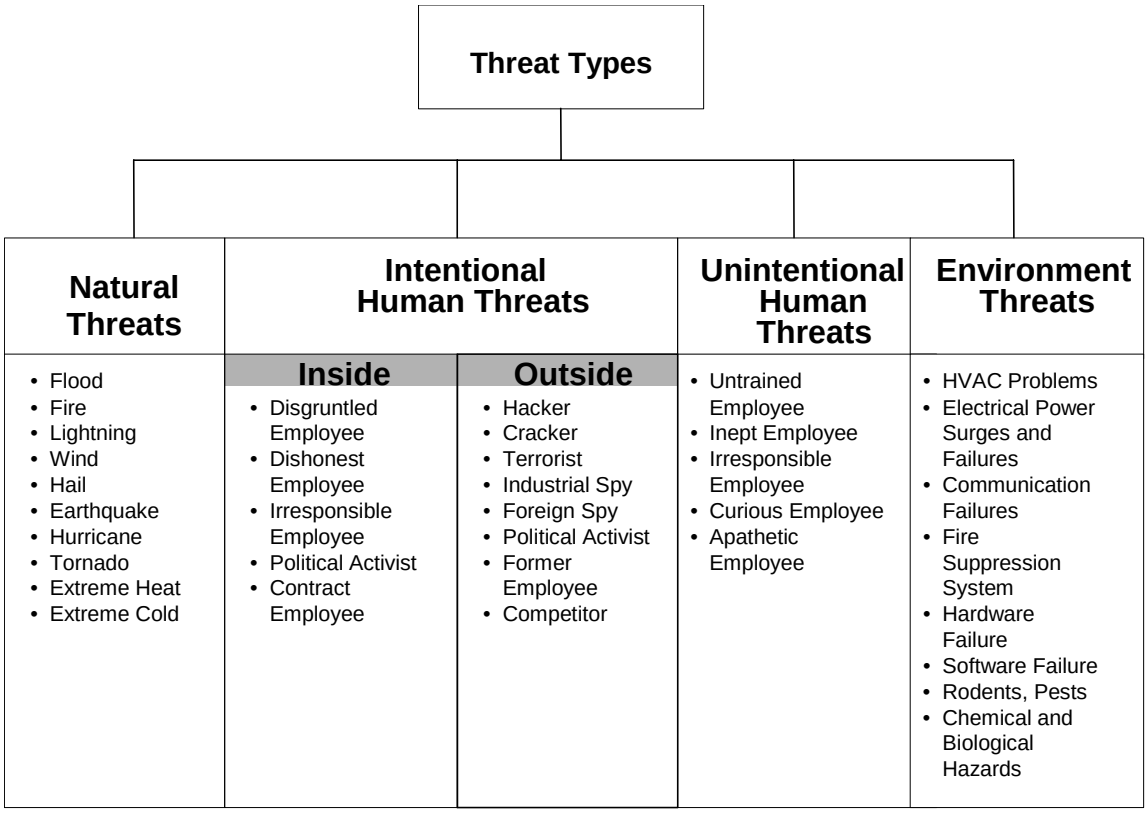

Figure 11: Threat Types

Natural threats - This threat type includes, but is not limited to:

- Fire, flood, earthquake, tornado, etc.
- Other "acts of nature."

Intentional human threats (insider and outsider) - This threat type includes, but is not limited to:

- Disgruntled employees seeking revenge by disrupting operations or causing public embarrassment.
- Dishonest employees motivated by financial gain/bribes.
- Application or system developers bypassing security controls to meet deadlines.
- Attacker gains access to a valid User ID and password (or PIN) by any of several means. He or she can gain access to information to perform unauthorized functions (view, add, modify, delete). He or she can place malicious software on the system either to deny service to specific resources, or to copy information (including passwords and user IDs, audit records, or software).
- Attacker gains access to the system and plants Trojan Horse programs to collect data from daily transactions, including production data, passwords and user IDs or audit records.
- Attacker gains access to system administrator privileges on a local server to modify authorizations.
- Attacker removes system equipment or software (theft/copyright infringement).

- Terrorist seeks to disrupt operations or cause embarrassment.
- Authorized user exceeds authority to gain access to unauthorized information.
- Authorized user performs unauthorized functions (add, modify, delete, browse data).
- Authorized user performs authorized functions (add, modify, delete) in an unauthorized manner (e.g., fraud).
- Authorized user places malicious software (e.g., virus, logic bomb) on a workstation or local server to deny service of local resources.
- Authorized user places malicious software (e.g., virus, logic bomb) on the system to deny service of resources.
- Authorized user places malicious software (e.g., Trojan Horse) on the system to monitor or copy information, including production data, passwords and user IDs, audit records, or software.

Unintentional human threats (insider and outsider) - This threat type includes, but is not limited to:

- Employee causing damage through accidental or inadvertent system misuse.
- Failure to follow security procedures, such as leaving a workstation logged on, sharing passwords, propping open secured doors, etc.
- Authorized user accidentally modifies or deletes data or software.
- Authorized user inadvertently releases unmarked or improperly marked sensitive data electronic media or in hard copy form (improper disposal).
- Authorized user accidentally exceeds authority to gain unauthorized access to information, including Privacy Act data.
- Authorized user performs unauthorized functions (add, modify, delete) and inadvertently performs an unauthorized activity.
- Authorized user inadvertently provides sensitive information to unauthorized individuals (hard copy or electronic format).
- Authorized user inadvertently provides direct access to system resources to unauthorized individuals.
- Authorized user inadvertently places malicious software (e.g., virus, logic bomb) on a workstation or local server to deny service of local resources.
- Authorized user inadvertently places malicious software (e.g., virus, logic bomb) on the system to deny service of specific resources.
- Authorized user inadvertently places malicious software (e.g., Trojan Horse) on the system to monitor or copy information, including production data, passwords and user IDs, audit records, or software.
- Authorized user inadvertently releases unmarked or improperly marked sensitive data on electronic media or in hard copy form due to improper disposition.
- Deficient system design and security testing.
- Improperly installed or improperly configured security controls.

Environmental threats - This threat type includes, but is not limited to:

- Failure of environmental controls, such as air conditioning, chilled water systems, humidifiers/de-humidifiers, and heating systems.
- Failure of supporting utilities, such as power and telecommunications.

- Failure of automated or manual fire and smoke suppression controls, to include both the failure to work when required and the false activation when not needed.
- Inappropriate or inexplicable behavior of systems and applications due to design flaws creating a denial of service or other vulnerability.

27. Probability of Threat Occurrence

One of the final steps in the threat analysis is to determine the probability of a threat occurrence or that a vulnerability will be exploited. Factors that govern threat probability include the motivation and capability of a given threat source, the severity of a vulnerability, and the effectiveness of current countermeasures. There are several approaches to understanding and qualifying threats. A simple way to describe threat probability by a given threat-source is the high, moderate, or low approach defined in Figure 12.

Consideration should also be given to the advantages and disadvantages of conducting a quantitative versus qualitative threat analysis. The advantage of the qualitative threat analysis is that it provides a relative prioritization of the risks and identifies immediate areas for improvement against the vulnerabilities. The disadvantage of the qualitative threat analysis is that it does not provide specific quantifiable measurements of the magnitudes of impact, therefore making the cost-benefit analysis of any recommended controls difficult.
The advantage of a quantitative threat analysis is that it provides a measurement of the magnitude that can be used in a cost-benefit analysis of recommended controls. The disadvantage is that depending on the units in which the measurement is expressed, the meaning of a quantitative threat analysis may be unclear, requiring that the result be interpreted in a qualitative manner. When quantitative values are the result of subjective judgments, the use of quantitative methods may hide the fact that the results are actually qualitative. One method to assist in quantifying impact is to:

- Estimate the frequency of the threat-source exercising the vulnerability over a specified time period (e.g., one year)
- Determine an approximate cost for each occurrence of the threat-source exercising the vulnerability
- Apply a weighted factor based on a subjective analysis of the relative priority of a specific threat exploiting a specific vulnerability

Even when hard and quantifiable data is not available, it is still paramount to estimate a *reasonable* percentage of success that each identified threat could be exploited for further analysis.

Success Level	Threat Description
High	The threat-source is in place, highly motivated and sufficiently capable. There are NO countermeasures to prevent the threat from being exploited.
Moderate	The threat-source exists, but countermeasures are in place that will impede successful exercise of the vulnerability. Or The threat-source lacks motivation or is only marginally capable of carrying out the threat.
Low	The threat-source lacks motivation or capability, security controls are in place to prevent successful exploitation of the threat, or significantly impede threat capability.

Figure12: Probability of Threat Occurrence

28. Impact Analysis

The next major step in the risk assessment is to determine the impact to USDA's mission that could result from the exploitation of each identified threat. The impact of a threat event can be described in terms of mission impacts resulting from data loss or compromise. Mission impact can be degraded when data integrity, availability, and/or confidentiality are affected. In order to determine the impact severity, identify the types of data processed by the system or application and categorize whether the data has a High, Medium or Low level of importance with respect to the data's confidentiality, integrity, availability as in the example in Figure 13. Next, use this information as input to understand the severity of impact described below.

Data Type	Confidentiality	Integrity	Availability
Statistical	Low	High	High
Product import, export, and availability information	Medium	High	High
Personnel	High	High	High
Certificate information	Medium	High	Medium
Forecast	High	High	Medium (Time Dependent)
Natural resources information	Medium	High	Medium
Financial	Medium	High	Medium
Program data	Medium	High	Medium
Farm and product information	Low	High	Medium (Time Dependent)
Procurement	Low (Time Dependent)	High	Medium
Payroll Summaries	Low	High	Medium

Figure 13: USDA-Specific Examples of Data Confidentiality, Integrity, and Availability

Loss of any of these data attributes will likely impact the mission in some manner as described below:

- ***Impact to Integrity*** **-** Integrity is impacted if unauthorized changes are made to the data or system, whether these changes are intentional or accidental. Violation of integrity may also result in the capability to launch a successful attack.
- ***Impact to Availability*** **–** Availability is impacted when a system or application is partly or completely unavailable to authorized users. This can result in loss of public confidence or processing time.
- ***Impact to Confidentiality*** **-** Confidentiality is at risk when data is made available to unauthorized users. This has far reaching consequences when sensitive data is being processed. Accountability and assurance are also at risk when user actions cannot be traced. For example, if the system administrator has system auditing turned off any intentional or unintentional activity cannot be identified or proven. Accountability

supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Impact to assurance indicates that there is not sufficient protection against unintentional user and/or software errors or the existence of adequate resistance to intentional penetration or by-pass. A successful exercise of a vulnerability results in a reduction in the grounds for confidence in the system.

Other intangible impacts (e.g., loss in public confidence, credibility) cannot be measured in specific units, but can be qualified in terms of critical, high, moderate, and low as described in Figure 14:

Impact	Description	Example of Impact to USDA
Critical Impact	Threat results in unavailability, modification, disclosure, or destruction of valued data or other system assets or loss of system services that is unacceptable due to the resulting disastrous national impact or likely deaths.	The unavailability of a USDA critical system that would leave USDA without the capability to warn the public of an impending or in-process disaster. This scenario could cause loss of life and disastrous effects to USDA.
High Impact	Threat results in unavailability, modification, disclosure, or destruction of valued data or other system assets or loss of system services that is unacceptable due to the resulting significant degradation of mission or possible injury to persons.	The loss of a critical resource that would mean USDA couldn't access their automated property data: therefore, USDA could not respond to pending emergencies. This situation would severely degrade USDA's critical mission.
Moderate Impact	Threat results in discernible but recoverable unavailability, modification, disclosure, or destruction of data or other system assets or loss of system services, resulting in transitory, yet important mission impact but no injury to persons.	The unavailability of the Integrated Financial Management System (IFMIS) would cause USDA to delay payment of claims to private individuals and private insurance companies. This scenario would briefly interrupt USDA's mission, but loss of life would not occur.
Low Impact	Threat results in unavailability, modification, disclosure, or destruction of data or degradation of system services that does not cause a significant mission impact or injury to persons.	The unavailability of USDA's website, would degrade USDA's mission and may cause embarrassment, but bodily injury or death would not occur.

Figure 14: Example of Impact Severity and Description

29. Level of Risk Determination

One of the final steps of the risk assessment is determination of risk to the system and data. Four major components help determine an information system's level of risk:

- Systems vulnerabilities
- Threat environment
- Mission impact

- Countermeasures

This process is accomplished by combining ratings generated in the threat, impact, vulnerabilities and countermeasures analysis in a qualified methodology. Figure 15 below provides a model or an example of determining an overall risk rating based on analysis of the threats, impacts, vulnerabilities, and countermeasures in previous steps. For example, if the Probability of Threat Occurrence, for a specific threat, is *Moderate* and the Impact is *High* Impact, the overall Level of Risk for that threat is *Moderate*.

	Probability of Threat Occurrence For A Given Vulnerability		
Impact	High	Moderate	Low
Critical Impact	Critical	High	Moderate
High Impact	High	Moderate	Low
Moderate Impact	Moderate	Moderate	Low
Low Impact	Low	Low	Low

Figure 15: Example of Risk Level

Develop a Risk Mitigation Strategy

In developing and implementing technical and administrative solutions for each approach, it is important to keep the USDA goals and mission in mind. Some simple principles of mitigating risk include the following:

- Preventing risk before it occurs. This means understanding the importance of risk early in the lift-cycle process. It is critical that system and application developers implement security controls in the design phase rather than attempt to retrofit security when the system or application is in production.
- Limit risk by implementing security controls that protect the data without impacting system or application performance. In other words, secure the data, but consider the business cost to USDA for the controls that are put in place.
- Detect and respond quickly by conducting security and awareness training sessions to educate USDA personnel on the importance of good security practices and threat detection; help them to understand what actions to take when a threat is either about to happen or is in progress.

Countermeasures are those actions that an organization can take to lessen or eliminate the threats or impacts of vulnerabilities identified in an IT system. Typically, these countermeasures are thought of in terms of Technical controls, such as access control lists or registry settings. However, Managerial and Operational controls can also be used as effective countermeasures.

Frequently these Managerial and/or Operational controls are more effective, as they offer a systemic solution that can be integrated in to the SLC. Some examples of Operational controls are:

- Procedures for assigning new user names and passwords
- Contingency Planning/Disaster Recovery Procedures

Some examples of Managerial controls that might be used as countermeasures include:

- A new, more stringent, password policy
- The re-direction of organizational resources
- A Security Awareness and Training program

These controls can make the existing vulnerabilities harder to exploit, or in some cases, eliminate them altogether. The maximum benefit from these countermeasures is usually gained quickly from the deployment of technical controls, but in a more sustained fashion with Operational and Managerial controls.

The process for risk mitigation is as follows:

- Review each potential threat and the action(s) that are necessary to reduce or eliminate the threat such as adding access controls to critical assets
- Determine the cost of mitigating the threat to the organization
- Decide whether the financial output is possible for each threat. For instance, what hardware or software measures will add protection and is the cost justifiable
- Implement the solution that reduces or mitigates the threat

30. Develop Business Case

An effective risk assessment is an integral part of the business enabling process, which provides a road map to move an organization from near-term tactical security implementations to long-term strategic planning. Most organizations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. Business owners and functional managers must ensure that their organizations have the capabilities needed to accomplish its mission. A risk assessment must provide managers the ability to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organization's missions. A well-structured risk assessment, when used effectively, must help management identify appropriate controls for providing the mission-essential security capabilities. A key measure of success for a risk assessment is its ability to be used by managers to obtain the necessary funding needed to mitigate risk and to make strategic decisions on how to allocate funds and resources to protect critical assets. In addition, the business case can support the decision by the Designated Accrediting Authority (DAA) to accept the responsibility for certain system risks.

As part of the mitigation strategy, it is important that a business case be developed that provides the appropriate managers with the understanding and supporting details that will allow them to obtain funding to implement the mitigation strategy. The business case must provide a direct linkage between the need to implement necessary security controls and the ability to meet business requirements.

Residual Risk

As stated earlier the ability to eliminate all risk in an IT environment is hardly achievable. Every system or application will have some degree of risk. Therefore, USDA must understand and make business decisions concerning what threats are the most critical, somewhat critical and non-critical; or, risks that are categorized as *High*, *Medium*, or *Low*. If a cost-benefit analysis has been conducted, then it is easy to make cost effective decisions.
Within federal agencies, the acceptance of risk is closely linked with the system *Certification and Accreditation*. Meaning, USDA must first make the determination as to those risks or threats that are the most critical and financially justifiable to mitigate. At this point, actions must be taken to implement security solutions. Second, those risks that are only marginally critical may or may not be mitigated. The cost may be too great and not justifiable. In addition, threats or risks that are non-critical may not be mitigated or they may be eliminated in the future when system software or hardware changes are made or they may pose no immediate threat.
Those threats that are not immediately mitigated are known as the system or application's *residual risk*. These threats/risk along with the business reason for not mitigating or eliminating the threats/risk must be listed on the *Residual Risk Statement* and presented to the *USDA CIO or Designated Approving Authority (DAA)* as part of the *Certification and Accreditation Package*. At that point, the DAA will permit the system or application to continue to operate while the risks are mitigated, accept the risk or order the system to be shutdown. Many times a system shutdown is not acceptable, therefore the security officer or manager must continue to document these risks and USDA must continue to work toward mitigating risk or continue to accept these known threats.

Using the residual risk as input, the System and Information Owners must develop an action plan that outlines their activities and timeline for resolving these threats/risk. The action plan serves as guidance for reaching a Full System Certification status.

Risk Assessment Report

A Risk Assessment Report will be developed for each risk assessment and serves as the final product of the risk assessment process. The Risk Assessment Report captures a 'snapshot in time' of the system security posture. Findings from the risk assessment are based on the system configuration documentation gathered in the initial phase of the assessment, personnel interviews as well as results from automated tools. The report is organized into the following sections:

- Section 1: Introduction – Section 1 provides the background needed to put the risk assessment in context. It describes the purpose of the assessment and identifies the scope, in terms of both system boundaries and areas to be assessed.
- Section 2: System Characterization – Section 2 describes the system's business or technical requirements, information infrastructure and data sensitivity, data flow(s), interfaces to other systems, hardware and software components, system security architecture, which depicts the operating system, facilities where the system is contained, and information storage requirements, and, applicable system security policies governing the system (agency policies, federal requirements, law)
- Section 3: Findings – Section 3 identifies system security vulnerabilities, potential threats and impacts, at a higher (or aggregate) level than is presented in the Appendices.

- Section 4: Analysis and Recommendations – Section 4 looks at the findings enumerated in Section 3, and analyzes them in terms of Business Risk. Section 4 also provides recommendations for mitigating each risk, as well as a listing of residual risks (if any).

APPENDIX A
GLOSSARY

Accountability - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Accreditation - Accreditation is a management authorization and approval granted to a major application or general support system to process in an operational environment. It is made based on a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security. Accreditation is synonymous with the term **authorize processing.** See also ***Authorize Processing, Certification,*** and ***Designated Approving Authority.***
Asset - A major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems.
Adequate security - Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by USDA operate effectively and provides appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.
Application - The use of information resources (information and information technology0 to satisfy a specific set of user requirements.
Assurance - Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass.
Authorize Processing - A management action that authorizes in writing a system based on an assessment of management, operational, and technical controls. By authorizing processing in a system the management official accepts the risks associated with it. Authorize processing is synonymous with the term **Certification**. See also ***Accreditation, Certification,*** and ***Designated Approving Authority.***
Automated Information System (AIS) - An AIS is any assembly of electronic equipment, hardware, software, and firmware configured to collect, create, communicate, disseminate, process, store, and control data or information. This includes numerous items beyond the central processing unit and associated random access memory, such as input/output devices (keyboards, printers, etc.). AIS is a term used to establish the scope of computer security.
Availability - The security goal that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise causes a denial of service or data and unauthorized use of system resources.
Business Owner - Is synonymous with the term Business Process Owner. See **Information Owner**
Certification - Certification is a major consideration prior to authorizing processing, but not the only consideration. Certification is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation

meets a pre-specified set of security requirements. Certification is synonymous with the term **authorize processing.** See also ***Accreditation*** and ***Authorize Processing.***

Confidentiality - The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit.

Denial of service - The prevention of authorized access to resources or the delaying of time-critical operations.

Designated Approving Authority - The agency official that accredits the AIS prior to deployment, re-accredits the AIS every 3 years, or when major changes are made.

General Support System - An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations

Individual Accountability - Requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

Information Owner - The designated individual responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains that responsibility even when the data/information are shared with other organizations.

Integrity - The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

IT-related risk - The net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur. IT related-risks arise from legal liability or mission loss due to:

- Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information
- Non-malicious errors and omissions
- IT disruptions due to natural or man-made disasters
- Failure to exercise due care and diligence in the implementation and operation of the IT

IT security goal - See security goal

Life-Cycle - A logical set of planning phases defined in NIST SP 800-14, consisting of: Initiation Phase; Development/Acquisition Phase; Implementation Phase; Operation/Maintenance Phase; and Disposal Phase to describe the system operational status.

Material Weakness - A significant weakness used to identify control weaknesses that pose a significant risk or a threat to the operations and/or assets of an audited entity. "Material weakness" is a very specific term that is defined one way for financial audits

and another way for weaknesses reported under the Federal Managers Financial Integrity Act of 1982. Such weaknesses may be identified by auditors or by management.
Networks - include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network (LAN) or wide area network (WAN), including public network (PN) such as the Internet and the Public Switched Telephone Network (PTSN).
Operational Controls - Those controls that address security methods that focuses on mechanisms that primarily are implemented and executed by people (as opposed to systems).
Policy - a management issued document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.
Procedures - are contained in a management issued document that focuses on the security control areas and management's position.
Risk - is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity. Risk is synonymous with "IT-related risk."
Risk analysis - See risk assessment
Risk Assessment (RA) - The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.
Risk management (RM) - An ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk. Simply stated, RM is a total process of identifying, controlling, and mitigating information system related risks. This RM process includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. RM as an overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.
Rules of Behavior - The rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal government equipment, assignment and limitation of system privileges, and individual accountability.
Security - Security is a system property. Security is much more that a set of functions and mechanisms. Information system security is a system characteristic as well as a set of mechanisms that span the system both logically and physically.
Security goal - The five security goals are integrity, availability, confidentiality, accountability, and assurance.
Sensitive Information - Information whose loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled.

Sensitivity - an information technology environment consists of the system, data, and applications that must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and/or availability that is determined by an evaluation of the sensitivity of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components.
System - is a generic term for the hardware, software, physical, administrative, and organizational issues that need to be considered when addressing the security of an organization's information resources and is used for briefness to mean either a major application or a general support system.
System Operational Status - either (1) Operational - system is currently in operation, (2) Under Development - system is currently under design, development, or implementation, or (3) Undergoing a Major Modification - system is currently undergoing a major conversion or transition.
Subject - A subject is any active entity that causes information to flow among passive entities called objects.
Technical Controls - Those hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.
Threat - The potential for a "threat-source" (defined below) to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.
Threat-source - Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) the situation and method that may accidentally trigger a vulnerability.
Threat analysis - The examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
Vulnerability - A flaw or weakness in system security procedures, design, implementation, internal controls, etc., that could be exploited (accidentally triggered or intentionally exploited) and result in a violation of the system's security policy.

APPENDIX B
FEDERAL LEGISLATION AND USDA POLICY

Legislation	Citation	Description
GAO Accounting and Information Management Division *Federal Information System Controls Audit Manual* (FISCAM) dated January 1999	Section 2.2 Assess Inherent Risk and Control Risk	This document states "a comprehensive high-level risk assessment should be the starting point for developing or modifying an entity's security policies and plan. Such assessments are important because they help make certain that all threats and vulnerabilities are identified and considered, that the greatest risks are identified, and that appropriate decisions are made regarding which risks to accept and which to mitigate through security controls."
Office of Management (OMB) A-130	Appendix III	This Appendix establishes a minimum set of controls to be included in federal automated information security programs; assigns federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123. The appendix states that "rather than continue to try to precisely measure risk; security efforts are better served by generally assessing risks and taking actions to manage them"
Federal Information Security Management Act of 2002 (FISMA)	Public Law (PL) No. 107-347, Title III	OMB Memorandum, 03-18, "*Implementation Guidance for the E-Government Act of 2002*" Permanently reauthorizes and amends agency information security requirements through the Federal Information Security Management Act (FISMA);

Legislation	Citation	Description
Homeland Security Presidential Directive	Hspd-7, Dated 12/17/03	This Bush Administration directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. Critical infrastructure and key resources provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being. While it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the country, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks.
OMB Circular A-127, Transmittal Memorandum No. 1 Revised July 23, 1993	Section 7. Financial Management System Requirements	The circular states “Agencies shall plan for and incorporate security controls in accordance with the Computer Security Act of 1987 and Circular A-130 for

Legislation	Citation	Description
		those financial management systems that contain "sensitive information" as defined by the Computer Security Act."
Clinger Cohen Act of 1996	Section 5112, Capital planning And Investment Control. Part (c).	The Clinger-Cohen Act requires the heads of federal agencies to link IT investments to agency accomplishments. The Clinger-Cohen Act also requires that agency heads establish a process to select, manage and control their IT investments. In reference to risk the act states " The Director shall develop, as part of the budget process, a process for analyzing, tracking, and *evaluating the risks* and results of all major capital investments made by an executive agency for information systems."
Paperwork Reduction Act of 1995	Section 3504. Authority and functions of Director, '(g) With respect to privacy and security, the Director shall—part (1), (2), and (3).	This act requires federal agencies, consistent with the Computer Security Act of 1987 (40 U.S.C. 759 note), to identify and afford security protections commensurate with the *risk* and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency.
United States General Accounting Office	GAO/AMID-99-139 (Exposure DRAFT)	Information Security Risk Assessment - Practices of Leading Organizations
National Institute of Standard (NIST)	Publication 500-174	Guide for Selection Automated Risk Analysis Tools
National Institute of Standard (NIST)	Special Publication 800-3	Establishing a Computer Security Incident Response Capability (CSIRC)
National Institute of Standard (NIST)	Special Publication 800-4	Computer Security Considerations in Federal Procurement: A Guide for

Legislation	Citation	Description
		Procurement Initiators, Contracting Officers and Computer Security Officials
National Institute of Standard (NIST)	Special Publication 800-5	A Guide to the Selection of Anti-Virus Tools and Techniques
National Institute of Standard (NIST)	Special Publication 800-6	Automated Tools for Testing Computer System Vulnerability
National Institute of Standard (NIST)	Special Publication 800-7	Security in Open Systems
National Institute of Standard (NIST)	Special Publication 800-8	Security Issues in the Database Language SQL
National Institute of Standard (NIST)	Special Publication 800-9	Good Security Practices for Electronic Commerce, Including Electronic Data Interchange
National Institute of Standard (NIST)	Special Publication 800-12	An introduction to Computer Security: The NIST Handbook
National Institute of Standard (NIST)	Special Publication 800-13	Telecommunications Security Guidelines for Telecommunications Management Network
National Institute of Standard (NIST)	Special Publication 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
National Institute of Standard (NIST)	Special Publication 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does,
National Institute of Standard (NIST)	Special Publication 800-26	Security Self-Assessment Guide for Information Technology Systems
National Institute of Standard (NIST)	Special Publication 800-27	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
National Institute of Standard (NIST)	Special Publication 800-28	Guidelines on Active Content and Mobile Code
National Institute of Standard (NIST)	Special Publication 800-30	Risk Management Guide
National Institute of Standard (NIST)	Special Publication 800-33	Underlying Technical Models for

Legislation	Citation	Description
		Information Technology Security
National Institute of Standard (NIST)	Special Publication 800-34	Contingency Planning Guide for Information Technology Systems
National Institute of Standard (NIST)	Special Publication 800-40 (DRAFT)	Procedures for Handling Security Patches
National Institute of Standard (NIST)	Special Publication 800-41	Guidelines on Firewalls and Firewall Policy
National Institute of Standard (NIST)	Special Publication 800-46	Security for Telecommuting and Broadband Communications
National Institute of Standard (NIST)	Special Publication 800-47 (DRAFT)	Guide for Interconnecting Information Systems
National Security Agency (NSA)	INFOSEC Assessment Methodology (IAM)	INFOSEC Assessment Methodology (IAM) entire program.

APPENDIX C
USDA ASSESSMENT CHECKLISTS

Information Systems Security Assessment Guide
Windows NT Server Information Asset Security Risk Assessment Guide
Windows NT Workstation Information Asset Security Risk Assessment Guide
Windows 2000 Server Information Asset Security Risk Assessment Guide
Windows 2000 Professional (Workstation) Information Asset Security Risk Assessment Guide
UNIX Information Asset Security Risk Assessment Guide
Telecommunications Information Asset Security Risk Assessment Guide
A/S 400 Information Asset Security Risk Assessment Guide
Personal Electronic Devices (PEDs) Information Asset Security Risk Assessment Guide
Application Software Development/Acquisition Risk Assessment Guide
Web Farm Information Asset Security Risk Assessment Guide
Mainframe Information Asset Security Risk Assessment Guide
Information Asset Security Risk Assessment Checklist for Classified Systems

APPENDIX D
RISK ASSESSMENT CHECKLIST

The USDA's key to implementing a successful enterprise-wide IT security program is the ability to identify and protect critical information assets. Risk management encompasses three processes: risk assessment, evaluation of risk, and risk mitigation. Risk management is the process that allows USDA managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' mission.

Agency Identification

Agency (Agency, Office, Bureau, Service, etc.):	
Address:	
ISSPM:	
ISSPM Phone Number:	
Date of last Assessment:	

Preparation

The following steps will assist you in preparing for the Security Assessment.

Step 1. **Identify key personnel.** The Information Systems Security Assessment Guide will assist you in determining the areas of responsibility of the personnel who are needed to obtain information and assistance in completing the assessment. Make an appointment with those personnel if necessary.

Name(s)	Area of Responsibility	Appointment Date/Time
Director/Agency CIO:		
Associate Director(s):		
Division Chief(s):		
Application Owners(s):		
Program Manager(s)		
Facility ISSPM:		
Security Representative(s):		
LAN Security Officer(s):		
Facility/Installation Security Officer(s):		
System Administrator(s):		
Network Administrator(s):		
Application Administrator(s):		
Other Key Personnel:		

Step 2. Identify the IT assets to be assessed. Obtain copies of the appropriate USDA IT Asset Checklists. Notify the appropriate managers and/or system/application administrator(s) ahead of time to ensure that they are available when you are ready to execute the checklists. Should there be a system or systems identified for which there is no checklist, a determination must be made as to how that system will be assessed.

Asset	Number to be assessed
Window NT Server	
Windows NT Workstation	
Windows 2000 Server	

Windows 2000 Professional (Workstation)	
UNIX	
AS/400	
Mainframe	
Telecommunications (network)	
Personal Electronic Devices (PEDs)	
Web Farm	
Classified System	
Application Software	

Step 3. Identify and obtain copies of all required security documentation for review. The following documents are listed in the Information Systems Security Assessment Guide. Other documents, such as previous assessments and recent vulnerability scan reports, will also provide further insight and assistance in performing the assessment.

Document Title	Available		Date of Document	Comments
	Yes	No		
Continuity of Operations Plan				
Key Management Plan				
Personnel Security Policy/Procedures				
Management Control Plan				
Disaster Recovery Plan				
Physical Security Policy				
IT Security Policy/Procedures				
Trusted Facility Manual (or equivalent document)				
Configuration Management Plan				
IS/Network Security Plan				
Security Features User Guide (or equivalent document)				
Interconnection Security Agreement (ISA)				

Perform Assessment

Step 4. **Execute the Information Systems Security Assessment Guide.** As well as determining whether administrative policies are in place and being implemented, the information listed below should come out during the interviews. This information is pertinent to properly analyzing risk and determining mitigation strategies.
Business Mission:
System Mission:
System users and support personnel activities:
System and data categories and sensitivity:
User interfaces and processes performed:
System architecture:
System boundaries:
Information resources that constitute the domain of interest:
Internal and external interfaces:
Data used or produced by the system and the data flow:

Step 5: Conduct risk assessments of the identified IT systems. Using the appropriate IT Asset Checklists perform the assessment for each system.
Step 6: Conduct Threat Analysis: Determine the level of threat to the systems based on the results of the checklists. A. Determine threat types B. Review automated scan reports if available C. Develop a listing of threat sources D. Determine probability of threat occurrence
Step 7: Conduct Impact Analysis A. Consider data categories B. Determine mission impact severity in terms of confidentiality, integrity, and availability
Step 8: Develop a Risk Mitigation Strategy A. Review threat list B. Consider impacts C. Determine countermeasures D. Determine mitigation priority list
Step 9: Develop Business Case – Provide business based reasons for obtaining/allocating the funding necessary to implement the mitigation strategy.
Step 10: Identify Residual Risk A. Review threat/risk that will not be mitigated B. Document remaining threats/risks for future action C. Include residual risk in Assessment Report
Step 11: Create Risk Assessment Report