

NESDIS

Policy and Procedures for IT Security Risk Management and Conducting Risk Assessments

October 8, 2013



Prepared by:

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration (NOAA)
National Environmental Satellite, Data, and Information Service (NESDIS)**

Table of Contents

Record of Changes/Revisions.....	4
1.0 Background and Purpose	1
2.0 Scope.....	2
3.1 Roles, Responsibilities, and Coordination.....	2
3.2 Authorization Official (AO)	2
3.3 NOAA Assistant Chief Information Officer (ACIO)	2
3.4 NESDIS Risk Executive Function.....	2
3.5 NESDIS IT Security Program Manager (ITSPM)	3
3.6 System Owner (SO).....	3
3.7 Information Technology Security Officer (ITSO)	4
3.8 Information System Security Officer (ISSO)	4
4.0 Management Commitment	4
5.1 Compliance.....	4
5.2 References.....	4
6.0 Policy.....	4
6.1 Policy Maintenance	5
6.2 Policy Feedback Process	5
6.3 Policy Effective Date	5
8.1 Procedures for Conducting Risk Assessments	7
8.2 Conduct an Initial Baseline Facilitated Risk Assessment.....	8
8.1.1 Assemble the Facilitated Risk Assessment Team	8
8.1.2 Understand the System and its Environment.....	8
8.1.3 Identify and Rate the Likelihood of Security Threats to the System	9
8.1.4 Identify and Rate the Impact of Security Vulnerabilities in the System	9
8.1.5 Determine Baseline Residual Risk and Document the Baseline Risk Assessment	10
8.2 Identify Security Impact Resulting From System Changes.....	11
8.2.1 Methods to Analyze Security Impact of System Changes.....	13
8.2.2 Associated Annual Reviews of the FIPS 199 and FIPS 200 Analyses.....	14
8.3 Review Results of Continuous Monitoring Security Activities and Assessments.....	15
8.3.1 POA&M Status.....	15
8.3.2 Vulnerability Scanning and Penetration Testing Results	15

8.3.3	Annual Security Controls Assessment Results	15
8.4	Review and Update System Threats	15
8.5	Review and Update System Vulnerabilities	17
8.6	Review and Update Risk Matrix.....	17
8.7	Develop Risk Mitigation Strategy	17
8.8	Update the Risk Assessment Report	18
8.9	Brief the AO	18
8.10	Update CSAM	18
8.11	Update SSP	19
	Appendix A: Common Information Security Threat Sources	20
	Appendix B: Common Information System Security Vulnerabilities	27
	Appendix C: Common Attack Methods.....	30
	Appendix D: Common Threat-Vulnerability Pairings	32
	Appendix E: Risk Matrix Example and Risk Ranges for Threats and Vulnerabilities.....	37

NESDIS IT SECURITY RISK MANAGEMENT POLICY AND PROCEDURES

Record of Changes/Revisions

Version	Date	Section	Author	Change Description
0.1d (draft)	2/16/2010	All	Noblis	Initial Draft
0.2d (draft)	3/12/2010	All	NESDIS OCIO	ITSO revisions to initial draft
0.3d (draft)	5/18/2010	3.1, 3.1.1, 3.1.2, 3.4, 3.6, 3.7, 3.8, 3.9, and 3.10.	Noblis	Revisions in response to comments from NESDIS Offices and Centers.
0.4d (draft)	7/27/2010	Footnote 1	NESDIS OCIO	Added footnote 1, ITSO edits
1.0 (final)	8/20/2010	All	NESDIS OCIO	Finalize and issue as Interim Technical Guide
2.0d (draft)	10/8/2013	All	NESDIS CID	Change from Interim Technical Guidance to Policy & Procedures Update for NIST SP 800-30 Rev 1 Update for NIST SP 800-39

1.0 Background and Purpose

Information systems are subject to serious *threats* that can have adverse effects on organizational operations and assets, individuals, other organizations, and the Nation by exploiting both known and unknown *vulnerabilities* to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems. Threats to information systems can include purposeful attacks, environmental disruptions, human/machine errors, and structural failures, and can result in harm to the national and economic security interests of the United States. Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations.

The National Institute of Standards and Technology (NIST), in Special Publication (SP) 800-39, *Managing Information Security Risk*, describes a holistic approach to managing information security risk that is integrated with and complementary to other organizational risk management programs and methodologies in place. Organizational risk can include many types of risk (e.g., program management risk, investment risk, budgetary risk, legal liability risk, safety risk, inventory risk, supply chain risk, and security risk). Security risk related to the operation and use of information systems is just one of many components of organizational risk that senior leaders/executives address as part of their ongoing risk management responsibilities.

Risk assessment is one of the fundamental components of an organizational risk management process as described in NIST Special Publication 800-39. Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems. The purpose of risk assessments is to inform decision makers and support risk responses by identifying: (i) relevant threats to organizations or threats directed through organizations against other organizations; (ii) vulnerabilities both internal and external to organizations; (iii) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring).

The Department of Commerce (DOC) Information Technology Requirement (CITR) 019, *Risk Management Framework*, requires that residual risks be assessed and documented (either through risk acceptance or establishment of Plans of Action and Milestones (POA&Ms) to remediate risks that are not being accepted), and deemed by the Authorizing Official (AO) to maintain risks at an acceptable level prior to granting the system Authorization to Operate (ATO) and placing the system into operation.

NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, outlines a methodology for assessing information security risk and presenting the risk in an understandable manner to AOs to make informed decisions regarding acceptance. Risk assessments are a key part of effective risk management and facilitate decision making at all three tiers in the risk management hierarchy including the organization level, mission/business process level, and information system level. Because risk management is ongoing, risk assessments are conducted throughout the system development life cycle, from pre-system acquisition (i.e., material solution analysis and technology development), through system acquisition (i.e., engineering/manufacturing development and production/deployment), and on into sustainment (i.e., operations/support).

The purpose of the NESDIS Risk Management Policy and Procedures is to communicate the NESDIS-specific procedures for performing baseline and annual risk assessments. Risk assessment identifies the risks to system security and determines the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. The objectives are to evaluate all vulnerabilities identified for the system during its risk assessment, to consider potential and likely threats capable of exploiting those vulnerabilities, to assess the countermeasures being implemented and/or planned to mitigate the risks, and to recommend additional countermeasures to adequately alleviate the risks.

Federal law and regulations, including Office of Management and Budget (OMB) Circular A-130, require all federally funded systems to adhere to a security program that incorporates risk management. NOAA is required to perform a risk assessment as part of the necessary Security Authorization process for information systems. Factors in considering the risk of operating information systems within NOAA include the responsibility for operating the nation's civil geostationary and polar-orbiting environmental satellites, and managing the largest collection of atmospheric and oceanographic data in the world. From this data, NOAA develops and provides environmental data and informational products and services critical to the provision of weather warnings and forecast, protection of life and property, the national economy, energy development and distribution, global food supplies, and the development and management of natural resources.

2.0 Scope

The scope of this document is limited to describing the process for determining and documenting information security risk as an integral part of an organizational risk management program. It applies to all NESDIS employees and contractors responsible for the development, operation, and maintenance of NESDIS information systems, including contractor owned and operated systems that contain NESDIS information.

3.1 Roles, Responsibilities, and Coordination

The following summarizes the roles and their responsibilities in the NESDIS security control selection, tailoring, and management process.

3.2 Authorization Official (AO)

The *Authorizing Official* formally accepts the residual information security risk as part of authorizing IT systems to operate.

3.3 NOAA Assistant Chief Information Officer (ACIO)

The *NOAA Assistant Chief Information Officer* establishes the organizational standards for assessing and managing risk within NESDIS.

3.4 NESDIS Risk Executive Function

The NESDIS senior executive leadership, in consultation with the ACIO, performs the Risk Executive function and is responsible for establishing the NESDIS-wide approach for managing agency-wide risk. Consistent with this oversight role, the risk executive (function) is the group within NESDIS that helps to ensure that: (i) risk-related considerations for individual information systems, to include authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions; and

(ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success. The risk executive (function) coordinates with the senior leadership of an organization to:

- Provide a comprehensive, organization-wide, holistic approach for addressing risk—an approach that provides a greater understanding of the integrated operations of the organization;
- Develop a risk management strategy for the organization providing a strategic view of information security-related risks with regard to the organization as a whole;
- Facilitate the sharing of risk-related information among authorizing officials and other senior leaders within the organization;
- Provide oversight for all risk management-related activities across the organization (e.g., security categorizations) to help ensure consistent and effective risk acceptance decisions;
- Ensure that authorization decisions consider all factors necessary for mission and business success;
- Provide an organization-wide forum to consider all sources of risk (including aggregated risk) to organizational operations and assets, individuals, other organizations, and the Nation;
- Promote cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility;
- Ensure that the shared responsibility for supporting organizational mission/business functions using external providers of information and services receives the needed visibility and is elevated to the appropriate decision-making authorities; and
- Identify the organizational risk posture based on the aggregated risk to information from the operation and use of the information systems for which the organization is responsible.

3.5 NESDIS IT Security Program Manager (ITSPM)

The *NESDIS IT Security Program Manager* oversees the effective implementation of the organizational standards for assessing and managing risk within NESDIS as established by the ACIO, maintains implementation policies and procedures, and provides training to all NESDIS information security roles in security risk management concepts. The ITSPM advises the ACIO and Risk Executives within NESDIS and NOAA regarding information security risk and residual risk determination pertaining to NESDIS information systems.

3.6 System Owner (SO)

The information *System Owner* manages information security risk associated with IT systems under their responsibility in accordance with established regulations, policies, and security requirements. The SO will facilitate the baseline risk determination and coordinate with the ITSO for annual assessment and update of the risk baseline at least annually.

3.7 Information Technology Security Officer (ITSO)

The *Information Technology Security Officer* ensures that SOs annually conduct risk assessments in accordance with established regulations, policies, and security requirements. The ITSO advises the ITSPM and SOs regarding information security risk and residual risk determination pertaining to NESDIS information systems.

3.8 Information System Security Officer (ISSO)

The *Information System Security Officer* plays an active role in developing and updating the risk baseline. The ISSO assists the SO in the development of the baseline risk assessment, updates the risk assessment as warranted based on results of the annual IT security continuous monitoring activities, and coordinates with the ITSO in annual update of the risk assessment.

4.0 Management Commitment

The NESDIS Chief Information Division (CID) supports the NESDIS Assistant Administrator's (AA's) strong emphasis on securing NESDIS information and information systems. Through the issuance of this policy and accompanying process and procedures, it demonstrates this commitment by establishing and documenting a process for managing information security risk and conducting risk assessments to ensure an acceptable level of security residual risk is maintained for NESDIS information systems.

5.1 Compliance

The NESDIS ITSPM monitors – through periodic quality reviews and monthly performance metrics – initial and annual assessments of information security risk of NESDIS information systems to ensure compliance with applicable laws, directives, policies, and guidance. The ITSPM reports to the AA monthly, and to the ACIO and Office Directors as necessary regarding compliance. The AA, ACIO, and/or Office Directors may initiate actions as necessary to correct reported deficiencies, including reallocation of resources to improve implementation of security practices, or removal of an individual from their role as AO, SO, or ISSO.

5.2 References

- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments* (September 2012)
- NIST SP 800-39, *Managing Information Security Risk* (March 2011)
- Department of Commerce (DOC) *Information Technology Security Program Policy* (ITSP) section 4.0 (January 2009)
- CITR-019, *Risk Management Framework* (July 2012)
- NOAA IT Security Manual 212-1302 (March 2008)

6.0 Policy

As required by DOC ITSP Section 4.0, the NESDIS-specific risk management and assessment process and procedures shall align with the requirements of NIST SP 800-39 and NIST SP 800-30. SOs and others performing risk assessments within NESDIS shall comply with the procedures outlined in Section 7.0 of this document for the conduct of risk assessments. The risk assessment shall be updated at least annually based on review of system configuration changes

and results of continuous monitoring assessments and shall be updated no later than the anniversary date of the system's authorization to operate (ATO). Each NESDIS information system shall have its residual risk assessed prior to initial operation, *independently* at least annually after initial ATO, and whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or ATO status of the system. The residual security risk shall be documented and approved in writing by the AO at least annually as part of obtaining or maintaining a system's ATO.

The IT security risk management process does not replace other organizational processes for program, mission, and project risk management, and must integrate with these processes for maximum effectiveness within NESDIS.

6.1 Policy Maintenance

The NESDIS ITSPM shall review this policy and procedures annually and update as necessary to reflect implementation challenges and new requirements. All updates to this policy shall be subject to a NESDIS-wide vetting process providing an opportunity for stakeholders to comment on the programmatic implications of updates.

6.2 Policy Feedback Process

NESDIS personnel are encouraged to notify the ITSPM by e-mail to nesdis.it.security@noaa.gov regarding any errors found in the document or other clarifications or updates that are required.

6.3 Policy Effective Date

This policy is effective upon issuance. Practices for Managing IT Security Risk

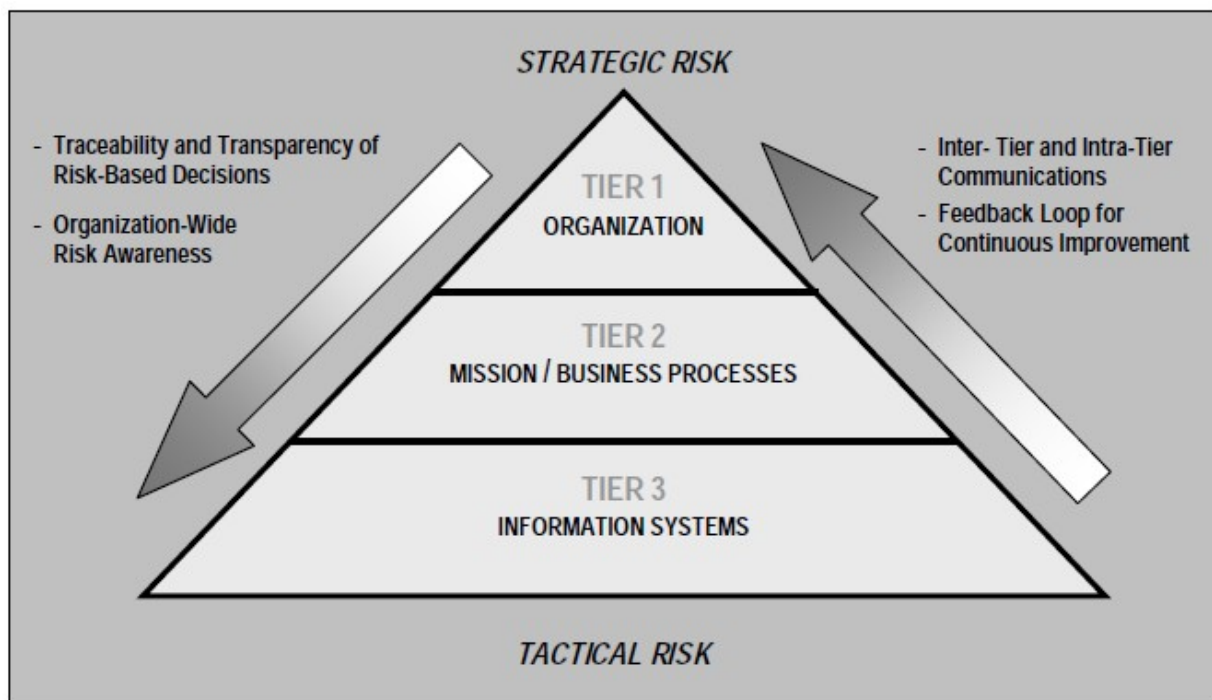
Risk management tasks begin early in the system development life cycle and are important in shaping the security capabilities of the information system. If these tasks are not adequately performed during the initiation, development, and acquisition phases of the system development life cycle, the tasks will, by necessity, be undertaken later in the life cycle and be more costly to implement. In either situation, all tasks are completed prior to placing the information system into operation or continuing its operation to ensure that: (i) information system-related security risks are being adequately addressed on an ongoing basis; and (ii) the authorizing official explicitly understands and accepts the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of a defined set of security controls and the current security state of the information system.

The Risk Management Framework (RMF) provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. Refer to the *NESDIS Risk Management Framework (RMF) Assessment and Authorization (A&A) Process Policy and Procedures* for implementing the RMF within NESDIS. It is available on the NESDIS IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php.

The IT security risk management process must consider and integrate with other organizational processes for program, mission, and project risk management, such as the DOC Enterprise Risk Management Process (information is available online at <https://max.omb.gov/community/display/DOC/Risk+Management+Guidebook>).

Managing information system-related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization—from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning and managing projects, to individuals on the front lines developing, implementing, and operating the systems supporting the organization’s core missions and business processes. Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization. Figure 7-1 illustrates a three-tiered approach to risk management that addresses risk-related concerns at: (i) the *organization* level; (ii) the *mission and business process* level; and (iii) the *information system* level.

Figure 7-1: Tiered Risk Management Approach



Source: NIST SP 800-39

Tier 1 addresses risk from an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy that includes:

- i. the techniques and methodologies the organization plans to employ to assess information system-related security risks and other types of risk of concern to the organization;
- ii. the methods and procedures the organization plans to use to evaluate the significance of the risks identified during the risk assessment;
- iii. the types and extent of risk mitigation measures the organization plans to employ to address identified risks;
- iv. the level of risk the organization plans to accept (i.e., risk tolerance);
- v. how the organization plans to monitor risk on an ongoing basis given the inevitable changes to organizational information systems and their environments of operation; and
- vi. the degree and type of oversight the organization plans to use to ensure that the risk management strategy is being effectively carried out.

As part of the overall governance structure established by the organization, the risk management strategy is propagated to organizational officials and contractors with programmatic, planning, developmental, acquisition, operational, and oversight responsibilities, including for example: (i)

authorizing officials; (ii) chief information officers; (iii) senior information security officers; (iv) enterprise/information security architects; (v) information system owners/program managers; (vi) information owners/stewards; (vii) information system security officers; (viii) information system security engineers; (ix) information system developers and integrators; (x) system administrators; (xi) contracting officers; and (xii) users.

Tier 2 addresses risk from a *mission* and *business process* perspective and is guided by the risk decisions at Tier 1. Tier 2 activities are closely associated with enterprise architecture and include: defining the core missions and business processes for the organization (including any derivative or related missions and business processes carried out by subordinate organizations);

- i. prioritizing missions and business processes with respect to the goals and objectives of the organization;
- ii. defining the types of information that the organization needs to successfully execute the stated missions and business processes and the information flows both internal and external to the organization;
- iii. developing an organization-wide information protection strategy and incorporating high-level information security requirements¹⁸ into the core missions and business processes; and
- iv. specifying the degree of autonomy for subordinate organizations (i.e., organizations within the parent organization) that the parent organization permits for assessing, evaluating, mitigating, accepting, and monitoring risk.

Because subordinate organizations responsible for carrying out derivative or related missions and business processes may have already invested in their own methods of assessing, evaluating, mitigating, accepting and monitoring risk, parent organizations may allow a greater degree of autonomy within parts of the organization or across the entire organization in order to minimize costs. When a diversity of risk assessment methods is allowed, organizations may choose to employ when feasible, some means of translation and/or synthesis of the risk-related information to ensure that the output of the different risk assessment activities can be correlated in a meaningful manner.

Tier 3 addresses risk from an *information system* perspective and is guided by the risk decisions at Tiers 1 and 2. Risk decisions at Tiers 1 and 2 impact the ultimate selection and deployment of needed safeguards and countermeasures (i.e., security controls) at the information system level.

Information security requirements are satisfied by the selection of appropriate management, operational, and technical security controls from NIST Special Publication 800-53. The security controls are subsequently allocated to the various components of the information system as system-specific, hybrid, or common controls in accordance with the information security architecture developed by the organization. Security controls are typically *traceable* to the security requirements established by the organization to ensure that the requirements are fully addressed during design, development, and implementation of the information system. Security controls can be provided by the organization or by an external provider. Relationships with external providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain arrangements.²¹

8.1 Procedures for Conducting Risk Assessments

This section provides the minimum mandatory set of activities to conduct and document initial and annual risk assessments within NESDIS to meet the requirements of federal, DOC, and NOAA policies.

8.2 Conduct an Initial Baseline Facilitated Risk Assessment

The baseline risk assessment consists of two phases, after which the baseline is reviewed and updated annually. The first phase is a Facilitated Risk Assessment (FRA). A FRA is an evaluation of the security posture of a general support system or major application. The assessment is fundamentally based on identifying a system's threats and vulnerabilities, performing a controls analysis, and results in the identification of residual risks and cost-effective risk mitigation recommendations. The purpose of the FRA is to provide the SO and Risk Executives with the information needed to develop a more secure system.

Specifically, this information helps these managers to:

- Identify security mechanisms that require testing,
- Prioritize project tasks, for incorporation of additionally required security mechanisms, and
- Manage project resources needed to complete development, integration, etc.

8.1.1 Assemble the Facilitated Risk Assessment Team

At the beginning of the *Development/Acquisition* Life Cycle Phase of the system, the SO assembles representatives from program management, the development staff, the user community, the certifying agent and the AO - all under the coordination of a "facilitator," which may be the ISSO, to form the FRA Team (FRAT). The FRAT performs a focused appraisal of the system's security architecture, identifying the system's vulnerabilities and the threats that can exploit those vulnerabilities after existing controls are taken into account. Ultimately, the team derives a list of residual risks (those not adequately suppressed by existing or proposed controls) and proposes a set of additional control recommendations and/or conclusions.

8.1.2 Understand the System and its Environment

The first step in the FRA process is to review the existing system description and other security related documents created in the *Initiation Phase* of the system's life cycle. Documentation gathered should include the AO-approved Federal Information Processing Standard (FIPS) 199 security categorization analysis, the Privacy Threshold Analysis (PTA), the e-Authentication Threshold Analysis (ETA), the AO-approved FIPS 200 security control requirements baseline analysis, the AO/AO's Designated Representative (AODR)-approved System Security Plan (SSP), and any other relevant documents such as system-specific and agency-wide policy/procedures or Interconnection Security Agreements created. In addition, vendor and Government security alerts and patch status need to be considered for relevance to the system risk posture. An examination of the system data, architecture design, and user groups ensures a common framework for evaluating risk to the system including management, operational and technical vulnerabilities caused by defective application or design of the respective controls.

System data refers to the information flow that exists within the system that is required for full system functionality. The review of the system data includes a qualitative evaluation of the extent to which the data should be secured against threats to its confidentiality, integrity, or availability as determined by the results of the FIPS 199 analysis.

The analysis of the system architecture looks at both the conceptual architecture, which is helpful in determining data flows and users, as well as the ‘as-built’ architecture, which enables the FRAT to evaluate system boundaries and interconnections. The FRAT evaluates the system’s security boundary and conducts an initial risk assessment.

8.1.3 Identify and Rate the Likelihood of Security Threats to the System

The next step using the FRA process is to identify and evaluate the threats that result from operating in the described IT environment and the likelihood that a potential vulnerability may be exploited by an identified threat within the construct of the associated threat environment. The FRAT should consider the threat-source motivation and capability to exploit a potential vulnerability. A threat is any agent (person, activity, or event) with the potential to cause harm to a system. Common threats for discussion by the FRAT are described in [Appendix A](#). The FRAT rates each threat as 1 [Low], 3 [Moderate], or 5 [High] based upon their likelihood of occurrence. The ratings, values, and descriptions are described below.

- High (5) - Expected to occur with some frequency; may occur during the course of normal operations (e.g., accidental errors).
- Moderate (3) - May occur under unusual circumstances; requires a single user with operator-level knowledge.
- Low (1) - Highly unlikely and not expected to occur; requires expert-level knowledge.

The FRAT then enters the threat likelihood ratings into the Risk Matrix, which when completed provides a quantitative composite value for potential residual risk where a threat intersects a vulnerability. An example of a Risk Matrix is shown in Appendix

E. A template for the Risk Matrix is available on the NESDIS IT Security Handbook website at

https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php.

The Risk Matrix template can be modified to add threats not listed in the template or to delete threats listed but not applicable to the system, which can also be accomplished by shading out the intersections where there is no first order relationship (e.g., a threat of fire cannot exploit inadequate account management).

8.1.4 Identify and Rate the Impact of Security Vulnerabilities in the System

The next step using the FRA process is to identify and evaluate the vulnerabilities that may be exploited by identified threats and to rate the adverse impact resulting from a successful threat exploiting an identified vulnerability. The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination

of any, of the following three security goals: integrity, availability, and confidentiality. A vulnerability is an inherent weakness in a system or its operating environment that may be exploited by a threat. Common vulnerabilities for discussion by the FRAT are described in [Appendix B](#).

The methodology to identify system vulnerabilities considers the control environment as described in the SSP. A control is a management, operational, or technical control that mitigates security risk by preventing, detecting, or correcting a vulnerable condition; by compensating for variations in meeting control objectives; or by reducing the likelihood of a successful threat or the impact of an exploited vulnerability. The FRAT may be supported by a skilled assessor, or the ISSO, who evaluates the controls that have been applied to reduce threat likelihood and vulnerability impact.

The FRAT or assessor can identify management, operational, and technical vulnerabilities associated with an IT system's processing environment via questionnaire (a security self-assessment checklist), interviews, document reviews, and/or the use of automated scanning tools and review of developer Security Test and Evaluation (ST&E) activities performed at the factory or development facility. A review of other industry sources (e.g., vendor Web pages that identify system bugs and flaws) can also be useful in preparing for the interviews and in identifying vulnerabilities specifically applicable to the IT system (e.g., a specific version of a specific operating system used by the system). The FRAT may also review current advisories issued by the N-CIRT, US-CERT, and the NIST National Vulnerability Database.

The FRAT rates each identified vulnerability as rated 1 [Low], 3 [Moderate], or 5 [High] based upon the impact if exploited, with consideration for risk mitigation controls currently in place. The ratings, values and descriptions are described below.

- High (5) - Extensive damage due to data loss, corruption, compromise, or prolonged denial of service, such as violation of highly sensitive data, endangerment of life, loss of integrity mechanisms, or corruption of security policies and rules.
- Moderate (3) - Moderate damage due to data loss, corruption, compromise, or denial of service, such as the release of sensitive information.
- Low (1) - Minor damage due to data loss, corruption, compromise, or denial of service, such as the violation of administrative policy.

The FRAT then enters the vulnerability impact ratings into the Risk Matrix, which when completed provides a quantitative composite value for potential residual risk where a threat intersects a vulnerability (see Appendix E). A template for the Risk Matrix is available on the NESDIS IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php. The Risk Matrix template can be modified to add vulnerabilities identified but not listed in the template or to delete vulnerabilities listed but not applicable to the system, which can also be accomplished by shading out the intersections where there is no first order relationship (e.g., a threat of fire cannot exploit inadequate account management).

8.1.5 Determine Baseline Residual Risk and Document the

Baseline Risk Assessment

In the next step of the FRA process, the FRAT or the assessor documents the baseline risk assessment in the Risk Assessment Report (RAR). A template for a RAR is available on the NESDIS IT Security Handbook website at

https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php.

The RAR includes a risk mitigation strategy to reduce the calculated risk by identifying controls that would cost-effectively reduce risk in the system operating environment. The assessor evaluates each identified vulnerability for risk reduction, develops a list and recommends additional controls as required, and estimates the risk reduction achieved by implementing the recommended controls. The assessor forwards the list of recommended controls to the SO for action.

The SO reviews the risks and the risk mitigation strategy, and decides whether to immediately implement the recommended corrective actions or to request either control tailoring¹ or POA&M² approval from the AO. If the vulnerability is remediated, the assessor or FRAT re-evaluates the condition and updates the RAR to reflect remediation if appropriate. If the SO opts to request AO approval of controls tailoring or POA&Ms, the SO prepares the approval package for AO signature in accordance with the respective NESDIS policies and procedures.

At this stage, the process yields a semi-quantitative measurement that is translated into the system's overall residual risk posture, or the remaining risk of operating the system in its current environment after considering the effectiveness of controls and risk mitigation countermeasures in place. The residual risk determination is the critical information the AO uses to grant an initial Interim Authorization to Test (IATT) the information system in an Integration and Testing environment. It is important to note that in the first phase FRA, the assessor makes a relative assessment; therefore, the result will always yield some threats and some vulnerabilities that have the greatest relative risk, given that every system functions with some level of risk. It is therefore the responsibility of the AO to determine if the identified residual risk is acceptable and the system may proceed to the *Implementation and Assessment* Phase of the system's life cycle.

8.2 Identify Security Impact Resulting From System Changes

After initial IATT is granted, changes to the system during the *Implementation and Assessment* Life Cycle Phase and the *Operations and Maintenance* Life Cycle Phase may have security implications because they may increase the likelihood of a threat exercising or exploiting a system vulnerability and/or increase the impact if the vulnerability were successfully exploited. Conversely, system changes such as remediation of POA&Ms may decrease the likelihood of a threat exercising a system vulnerability and/or decrease the impact if the vulnerability were successfully exploited. As indicated by Topics and Subtopics of Table 8-1, *Change Categories*, there are many types of system changes that could have security implications. The SO, assisted by support personnel including the ISSO, will review all changes to the system's configuration baseline for potential security implications. Change Control Requests (CCRs), Engineering Change Requests (ECRs), problem reports/trouble tickets must contain associated documentation showing the Security Impact Analysis (SIA) of changes proposed and reference an artifact documenting proper implementation of security controls for mitigation of risk. A template for an SIA is

available on the NESDIS IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php. The SO may adjust the initial weight of each threat and vulnerability documented in the Risk Matrix (see Sections [8.1.3](#) and [8.1.4](#)) and update the RAR based on this review.

Table 8-1: Change Categories

Topic	Additional Details/Subtopics
Contacts for the System	SO, Information System Security Officer (ISSO), individuals responsible for security, and any other contacts who are pertinent to system security.

Topic	Additional Details/Subtopics
System Description/ Characterization	System function; system mission objective, facility changes or relocation, architecture, interconnections, hardware, software, technical, security, deployment features, network devices, servers, and workstations.
Information/Data Flow	Processing flow of the application from system input to system output; data flow for each input path including external interfaces, user interfaces, and administrative interfaces.
Security Authorization Boundary Definition	External/perimeter interfaces for the system enforcing the demarcation of the authorization boundary; system’s direct management control; system function; system mission objective; system operating characteristics; system security need; general operating environment; organizations/facility responsible for the system operations.
System Interconnections	Where transmissions cross the system boundary (in/out); who/what entity is authorized to come into the system, and from which system; those connections to other systems that are not within the system’s security boundary (e.g., the Internet), unique system identifiers (if appropriate) security concerns, and Rules of Behavior of the other systems; type of communications (e.g., dedicated circuits, dial circuits, public data/voice networks, Internet) and the sensitivity level of the connecting system.
Applications Supported	Applications (major and minor ³) supported by the general support system; application function; information processed by the application.
Users/Web Access Requirements	Types of users, manner of accessing the system, the technical controls on that access, and the administrative and management controls on the user accounts; web-based activity; changes in publicly accessed information.

System Environment	Any environmental or technical factors that raise special security concerns (e.g., harsh/overseas location, fast track, Open network with public access, external facility, dial-up, bi-directional external interfaces, file sharing, Demilitarized Zone (DMZ) if used, modem pool, Internet access); the physical location(s) of the system and its backups (e.g., whether in a DOC facility or a contractor facility, whether the system is supported/maintained by government or contract staff, and the nature of contract support (if applicable)).
Hardware and Software Inventory	Component make/Original Equipment Manufacturer (OEM), model; version; service packs; whether the software is customized or Commercial Off-The-Shelf/Government Off-The-Shelf (COTS/GOTS) and government-owned or contractor-provided; perimeter security devices, firewalls, routers, switches, file/print/application servers, and example workstations and networked print devices; Operating System (OS); role perimeter devices play in protecting the system from the untrusted environment (e.g., DMZ set up to protect a web server from malicious Internet traffic and to protect the internal network from the web server to which it is connected if the web server is compromised).
Component Configuration	Configuration parameters; rule sets; OS and application hardening; system

Topic	Additional Details/Subtopics
Settings	specific settings within software.
Firewall Configuration Settings	Firewall configuration parameters and rule sets.
Dependencies on Other Systems	Trusted connections; untrusted connections and devices to prevent unauthorized system intrusion; nature of connection (Government-to-government (G2G), government-to-business (G2B), government-to-citizen (G2C)); controls to allow and restrict public access; connection agreements.
Existing Countermeasures	Changes to the intrusion detection installation, support, or processing; management, operational, or technical control or safeguard that detects or reduces the impact of a threat or vulnerability; changes to the configuration management processes.

8.2.1 Methods to Analyze Security Impact of System Changes

The SO, assisted by support personnel including the ISSO, must use all methods at his/her disposal to perform an SIA of changes, including interviews, collaborative meetings, personal knowledge, documentation, and testing. Documentation gathered should include the last RAR,⁴ updates to the AO-approved FIPS 199 and FIPS 200 analyses, approved updates of the SSP and supporting core documents, authorized CCRs, POA&Ms open as well as those closed within the prior 12 months, and any other relevant documents such as system-specific and agency-wide policy/procedures or Interconnection Security Agreements created or updated in the prior 12 months. In addition, revisions to NIST recommendations and vendor and Government security alerts and patch status need to be considered for relevance to the system risk posture.

8.2.2 Associated Annual Reviews of the FIPS 199 and FIPS 200 Analyses

The SO, assisted by support personnel including the information owners, must review

1) any changes to the information stored and processed by the system and 2) changes to the perceived criticality and/or sensitivity of that information, for impact on the current system FIPS 199 security categorization and FIPS 200 security controls baseline and associated tailoring. Changes associated with the information processed or stored on the system may change the system's FIPS 199 categorization, thus necessitating a different set of security controls to be applied to the system. If changes to the FIPS 199 and/or the FIPS 200 are identified, the SO should take this opportunity to update these documents and obtain AO approval. Controls now required due to an increased FIPS 199 categorization (e.g. from Moderate to High) that are not in-place may increase the likelihood of a threat exercising a system vulnerability and/or increase the impact if the vulnerability were successfully exploited. The opposite is also true for a decreased FIPS 199 categorization (e.g. from High to Moderate).⁵

⁴ A RAR template is available on the NESDIS IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php.

⁵ For more information, see the NESDIS *Federal Information Processing Standards Publication (FIPS) 199 Policy and Procedures* and the NESDIS *FIPS 200 Security Control Selection and Tailoring Policy and Procedures* available on the NESDIS IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php.

8.3 Review Results of Continuous Monitoring Security Activities and Assessments

The SO, assisted by support personnel, reviews and updates as necessary the RAR as warranted based on a review of the status and the results of ongoing security activities and assessments.⁶ After each update of the RAR, the final RAR is uploaded to the Cyber Security Assessment and Management (CSAM) system as an artifact in the System Overview/Status & Archive section of the system record.

8.3.1 POA&M Status

The SO, assisted by support personnel, reviews the status of vulnerabilities identified in POA&Ms and, based on progress in correcting the deficiencies, and as necessary adjusts (increase or decrease) the initial weight of each threat and vulnerability documented in the Risk Matrix and updates the RAR. The SO reviews POA&Ms currently open as well as POA&Ms closed since the last update of the RAR.

8.3.2 Vulnerability Scanning and Penetration Testing Results

The SO, assisted by support personnel, reviews the results of the most recent quarterly vulnerability scans and system penetration tests (if applicable) and adjusts (increase or decrease) the weight of each threat and vulnerability documented in the Risk Matrix and updates the RAR.

8.3.3 Annual Security Controls Assessment Results

At least annually, the independent security Certifier assigned by the ITSO updates the RAR for the results of the annual security control assessment, vulnerability assessment, and penetration testing. The Certifier adjusts (increase or decrease) the weight of each threat and vulnerability documented in the Risk Matrix and updates the RAR.

8.4 Review and Update System Threats

A threat is any agent (person, activity or event) with the potential to cause harm to a system. All information systems, regardless of type and level of data processed, stored and transmitted, are subject to harm. The mere existence of the threat does not imply that the system will be harmed, but the potential for harm is always present. Threats exist simply because the system exists. For example, fire is a threat to any system, and even though the system may have adequate fire prevention, fire still remains a threat.

The SO, assisted by support personnel including the ISSO or independent Certifier, reviews and updates as necessary the documented threats to the system based on a review of:

- System changes (Section [8.1](#));
- Results of ongoing security activities and assessments (Section [8.2](#));
- Review of threat trends communicated through advisories issued by government entities that may include, but are not limited to: the NOAA Computer Incident Response Team (N-CIRT, at <https://www.csp.noaa.gov/noaa/advisories/>) and the U.S. Computer Emergency Readiness Team (<http://www.us-cert.gov/>);

⁶ For more information regarding security assessments, see the NESDIS *Policy and Procedures for Conducting Security Controls Assessments* available on the NESDIS IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php.

- Adding and assessing threats introduced since the last risk assessment that are relevant in the system environment; and
- Reviewing previously identified threats to determine that they are still valid and that the impacts to the system are the same.

Each threat is assigned a likelihood rating that its occurrence will impact the system. Existing protections should be considered, as the probability that a threat's occurrence will impact the system is significantly lower as a result of existing protections. All updates are to be documented in the Risk Matrix (see Section [8.6](#)).

8.5 Review and Update System Vulnerabilities

A vulnerability is an inherent weakness in the system design, physical layout, procedures, administration, personnel, management, hardware or software that may be exploited by a threat to cause harm to the information system. In other words, vulnerabilities indicate weaknesses or flaws in the system that have the potential for exploitation by a threat-source.

The SO, assisted by support personnel including the ISSO or the independent Certifier, reviews and updates as necessary the documented vulnerabilities to the system based on a review of system changes and results of ongoing security activities and assessments (Sections [8.2](#) and [8.3](#)). The SO may also review vulnerability trends communicated through advisories issued by government entities mentioned above in section 3.3 as well as the National Vulnerability Database (<http://nvd.nist.gov/>);

Vulnerabilities are rated based upon the impact if exploited and consider mitigations currently in place. All updates reflecting uncorrected vulnerabilities are to be treated as sensitive and documented in the Risk Matrix (see Section [8.6](#)).

8.6 Review and Update Risk Matrix

The Risk Matrix section of the RAR communicates an initial determination of risk measurement by multiplying the ratings assigned for threat likelihood (e.g., probability) and impact of an exploited vulnerability (see [Appendix E](#)). The SO, assisted by support personnel including the ISSO or the Certifier, will review the threat-vulnerability risk pairings for reasonableness to the system (see [Appendix D](#)) and update the Risk Matrix as necessary based on performance of the activities described in Sections [8.4](#) and [8.5](#).

8.7 Develop Risk Mitigation Strategy

For each threat and vulnerability grouping accepted as applicable to the system, the SO, assisted by support personnel including the ISSO and the security Certifier, develops a risk mitigation strategy and recommendations to mitigate or accept risk. This effort should start with threat-vulnerability pairings that result in a risk of harm to the system (see [Appendix D](#)). The SO should then determine whether to mitigate or request AO risk acceptance of any risk resulting from the threat-vulnerability pairings. The SO will develop one or more POA&Ms to address mitigation of risk that is considered unacceptable.

- Identification of Risk Mitigation Measures/Strategy – Each potential area of risk of harm to system operation is a candidate for risk mitigation. The SO or Certifier identifies possible mitigation strategies that target the greatest reduction of residual risk.

- Identification of Recommendations – The SO or Certifier uses previously defined results and general knowledge of the system to make recommendations on the implementation of mitigation strategies, the allocation of residual risk, operational constraints on the system, and recommendations for future enhancement. The recommendations are used as input to POA&Ms necessary for implementing the Risk Mitigation Strategy.
- Conclusions – The SO or Certifier summarizes the overall residual risk posture of the system, taking into account system strengths and compensating controls in place and functioning.

8.8 Update the Risk Assessment Report

The SO, assisted by support personnel including the independent Certifier for annual updates, must ensure, at least annually, that the RAR has been updated including:

- Identified Threats
 - Reviews of configuration changes
 - Reviews of security advisories
- Identified Vulnerabilities
 - Results of Annual Security Controls Assessments
 - Vulnerability assessment scans
 - Penetration testing reports (if applicable)
- Threat-Vulnerability Pairings (see [Appendix D](#))
- Risk Matrix (see [Appendix E](#))
- Risk mitigation measures/strategy
- Recommendations for corrective action (POA&Ms or controls baseline tailoring)
- Conclusions
- Record of Changes and date of the RAR. Even if there is no change to the risk posture of the system, the record of changes and document date must be updated to reflect that the annual review that took place.

8.9 Brief the AO

The SO, assisted by support personnel and the Certifier for annual updates, briefs the AO on the results of the risk assessment. They must disclose the Conclusions, the Risk Mitigation Strategy, and request AO approval of POA&Ms or controls tailoring to address the risk assessment recommendations.

8.10 Update CSAM

The SO, assisted by support personnel, must upload the updated and approved RAR to the Cyber Security Assessment and Management (CSAM) system (SSP Contents → Status section) according to the procedures outlined in the *NESDIS Federal Information Security Management Act (FISMA) Inventory Management Policy and Procedures*.

In addition, the SO enters new POA&Ms as approved by the AO. See the NESDIS *Plan of Action and Milestones Management Policy and Procedures* for more information on creating and managing POA&Ms.

8.11 Update SSP

The SO, assisted by support personnel, must update, at least annually, the SSP Section RA-3 and Appendix G, with the updated RAR artifact version and date. The SSP must also be updated with any new AO-approved POA&Ms, new control requirements, or requirements tailoring that resulted from the risk assessment.⁷

⁷ For more information on maintaining the SSP, see the NESDIS *System Security Plan Development and Maintenance Policy and Procedures* available on the NESDIS IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php.

Appendix A: Common Information Security Threat Sources

Common threat sources are categorized as: human threat (e.g., terminated employee), environmental threat (e.g., power outage), and natural (e.g., earthquake). Common threat sources are shown in the Table A-1 below.

Table A-1: Threats Sources and Actions

Source	Comments	Threat Action
Intentional Human Threats		
Hacker, cracker	Motivation: Challenge, ego, rebellion	Hacking Social engineering System intrusion, break-ins Unauthorized system access
Computer criminal	Motivation: Destruction of information, illegal information disclosure, monetary gain, unauthorized data alteration	Computer crime (e.g., cyber stalking) Fraudulent act (e.g., replay, impersonation, interception) Identity Theft Information bribery Spoofing System intrusion, break-ins
Terrorist	Motivation: Blackmail, destruction, exploitation, revenge	Bomb, terrorism Information warfare System attack (e.g., distributed denial of service [DoS]) System penetration System tampering
Industrial espionage	Companies, foreign governments, other government interests. Motivation: Competitive advantage, economic espionage	Economic exploitation Information theft Intrusion on personal privacy Social engineering System penetration Unauthorized system access Access to classified, proprietary, and/or technology-related information
Insiders	Poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees Motivation: Curiosity, ego, intelligence, monetary gain, revenge, unintentional errors (e.g., data entry error, programming error)	Assault on an employee Blackmail Browsing of proprietary information Computer abuse Fraud and theft Information bribery Input of falsified, corrupted data Interception Malicious code (e.g., virus, logic bomb, Trojan horse) Sale of personal information System bugs System intrusion, break-ins System sabotage Unauthorized system access
Cyber Threats		
Malicious Code	Viruses, Worms, Trojan Horses, Logic Bombs, Trap Doors	System operation impeded (e.g., slowed or stopped), Denial of Service (DoS) Data corruption

		Data loss
--	--	-----------

Source	Comments	Threat Action
Software Errors	Design errors, bugs, crashes	System operation impeded (e.g., slowed or stopped)
		Data corruption
		Data loss
Natural Threats		
Severe storm	Hurricane, severe electrical storm, tornado	Property destruction
		DoS (system down)
		Information loss
Flood	High water, storm surge	Property destruction
		DoS (system down)
		Information loss
Other natural disasters	Volcano, tsunamis, earthquake	Property destruction
		DoS (system down)
		Information loss
Environmental Threats		
Contaminants	Gas leak, incident in parking garage, accidental release of chemicals, dirty bomb	Physical access to facility denied
		DoS (system down)
		Information loss
Fire	Directly affecting IT facility or within the building	Property destruction
		Physical access to facility denied
		DoS (system down)
Water damage	Burst pipe, sprinklers engaged	Property destruction
		DoS (system down)
		Information loss
Computer/LAN room environmental extremes	Temperature and humidity	Property destruction
		DoS (system down)
		Information loss
Long term power failure	Power failure of more than the lifetime of the Uninterrupted Power Supply (UPS.) Power grid outage, local power outage	DoS (system down)
		Information loss
Communications failure	Dedicated lines down, Internet connection down, phone lines down	Information loss
		DoS
Disaster	Train derailment, vehicle accident, meteorite	Property destruction
		Physical access to facility denied
		DoS (system down)
		Information loss

Source: NIST SP 800-30

Regardless of the source of the threat, the confidentiality, integrity, and availability of system resources and information, if not properly safeguarded, are at risk. Table A-2 shows the potential impact of identified threats used in determining impact of a threat on vulnerability.

Table A-2: Threat Impact on Security Objectives

THREAT	THREAT IMPACT		
	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
INTENTIONAL HUMAN THREAT			
Bombing/Bomb Threat			X
Sabotage	X	X	X

Arson	X	X
-------	---	---

THREAT	THREAT IMPACT		
	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Vandalism	X	X	X
Theft	X	X	X
Unauthorized Access	X	X	X
Deletion/Erasure		X	X
Blackmail	X		
Hacker	X	X	X
Fraud/Falsification	X	X	X
Message Modification	X	X	X
Computer Abuse/Misuse		X	X
Omission			X
UNINTENTIONAL HUMAN THREAT			
Accidents	X	X	X
Operational/Procedural Errors	X	X	X
Negligence	X	X	X
Unavailability of Key Personnel		X	X
Improper Software Configuration	X	X	X
CYBER THREATS			
Malicious Code (Viruses, Worms, Trojan Horses, Logic Bombs, Trap Doors)	X	X	X
Software Errors (Buffer Overflows)	X	X	X
Password Cracking/Guessing	X		
Spoofing (Impersonation)	X	X	
Packet Capture	X	X	
NATURAL THREATS			
Rain/Snow Storms			X
Earthquakes			X
Flood			X
Hurricane			X
Tornado			X
Lightning			X
ENVIRONMENTAL THREATS			
Environmental Control Failure (Temperature, Humidity, Dust)		X	X
Power Fluctuations/Outages		X	X
Hardware Malfunction/Failure		X	X
Fire Damage			X
Water Damage (Sprinkler System Activation/Rupture)			X
Structural Failure			X

Table A-3 below describes insider threat behaviors.

Table A-3. Human Threat Description

User Type	Behavior
-----------	----------

Malicious Authorized User	Disgruntled employees can violate the confidentiality, integrity, and of their employer’s system, as they are the group most familiar with the system, its security controls, and its vulnerabilities. They also may know what actions might cause the most damage. Disgruntled employees typically believe that they have been treated unfairly by their employer in some way, such as in their pay, promotions or demotions, or the amount of respect received from their peers or superiors.
---------------------------	---

User Type	Behavior
Non-malicious Authorized User	The primary threat to data integrity comes from authorized users who inadvertently compromise the confidentiality, integrity, or accessibility of a system, such as through errors, omissions, or unwise or inappropriate practices. Such threats usually come from employees who are insufficiently trained in the use of the system; appropriate security practices; or threats and vulnerabilities. In some cases, damage is caused directly by the user; in others, the user inadvertently creates vulnerabilities.
Former Employees	Former system users or administrators may retain the ability to access the information systems of their former organizations because of their knowledge of security countermeasures and system vulnerabilities. This is particularly the case if their accounts and access rights are not terminated promptly after their departure. In addition, former employees often maintain personal relationships with others in the organization, and this potentially provides a means to obtain information relevant to security– or perhaps even insider assistance.
Partners and Service Support Staff	Maintenance personnel, cleaning crews, support contractors, and partner staff are often allowed unsupervised access and typically do not have the same screening as the supported organization.

Appendix B: Common Information System Security Vulnerabilities

Table B-1 lists and describes the types of *potentially* exploitable vulnerabilities that may exist within a typical IT system. These are the types of vulnerabilities that the SCA procedures are designed to identify through application of the NIST SP 800-53A Revision 1 SCA methodology.

Table B-1: Description of Potentially Exploitable IT System Vulnerabilities

Vulnerability	Description
Inadequate Security Policy	The organization's security policy is not sufficiently defined and/or documented to ensure an appropriate level of security is implemented. There also may be differences between the implementation, the written policy, and the emerging NOAA policies.
Inadequate System Administration	Account administration for the system may become overwhelmed if the global system account administration architecture fails to account for adequate data sharing and Continuity of Operations (COOP). Current procedures may prove inadequate to address demand and maintenance.
Inadequate User Account Management	The practical aspects of the sites will require examination as to whether user accounts will be disabled upon reassignment, termination, or lack of use.
Inadequate Personnel Management	Requirements for clearances and nondisclosure of sensitive or private information may not be currently inculcated within the community. Procedures to screen personnel place an additional burden on personnel management.
Incomplete Contingency Plan	A contingency plan should address adequate recovery of the system in the event of a disaster. Additionally, the primary and the backup system may be collocated. This increases the impact of a local disaster taking out both sites and functionality.
Inadequate Warning Banner	The adequacy of the warning banner to address sensitive processing, Privacy Act information, and mandatory notification of activity monitoring should be assessed.
Use of Replayable Identification and Authentication (I&A)	Password Management affects the strength of I&A. Passwords can be replayed and shared. The impact of using replayable I&A should be assessed for impact on the system at each location.
Sharing of ID or Passwords (Use of Group Passwords)	Use of group or shared passwords violates the use of the password to authenticate individuals. As a result, both I&A and Accountability requirements fail to be met. The system should be assessed in the environment to determine if there is a likelihood of users sharing accounts or using group passwords.
Inadequate Audit Log	There may be cases where inadequate data has been captured in the audit log to reconstruct an event after it is detected. An example may be that after a specific sensitive file has been released to the press, the list of users that accessed the file may not be recoverable, losing accountability. A detailed description of the audit logs will be provided in the SSP.
Inadequate Audit Analysis	The team should assess the adequacy of current procedures to review audit data and violation reports.
Data Transmissions in the Clear	Sensitive data should not transverse communication links in the clear. When transmission is necessary, the system should encrypt data when transmitting it. The completeness of the implementation for all potentially sensitive information should be assessed and the impact determined of any potential unencrypted link.
Susceptibility to Line Tapping	Use of network components that are susceptible to line tapping may cause loss of confidentiality.
Inconsistent Physical Perimeter Definition	The physical perimeter for the overall enterprise varies from location to location according to facility protocol. In addition, the mission of given organization may lend itself to a more open environment.
Inadequate Facilities	For some reason (i.e., natural disaster), a system facility or a location cannot be accessed, or the facility is deficient in some way.
Data Unavailability	For some reason the data necessary for the continued processing of the system is unavailable.
Inadequate Hardware / Component	Are there components in the hardware that are inadequate to meet the needs of this major application?
Unstable or Insufficient Communication Medium	Available communications links may not be adequate to handle the volume of system transactions. In addition, the communication media supporting the system worldwide may not be consistent or stable.
Inadequate or Missing Documents	Failure to develop or acquire documentation necessary to perform the function and handle emergencies, as well as meet Government requirements may lead to undetected system vulnerabilities in tools that are provided but not used.
Weak Rules of Behavior	Rules of Behavior do not clearly describe allowed and disallowed activities

Untrained Users	There may be inadequacy of the security training for enterprise personnel to resulting in a vulnerability that will surface with or after deployment.
-----------------	---

Vulnerability	Description
No Individual Accountability	There is no ability to hold users responsible for activities occurring under their account.
No System Change Control	Configuration Management (CM) should be assessed for adequacy with regard to hardware configurations. Without an adequate CM program, there is no method to predict and track software development or fielded versions of the system.
No Software Change Control	CM should be assessed for adequacy with regard to software version control and features of locally developed software. Without an adequate CM program, there is no method to predict and track site implementation and modifications of the software.
No Separation of Duties	The same privileged users are responsible for critical system administration activities (e.g. account management, granting of access or privileges) and the auditing of those facilities. Such assignment invalidates the accountability of their use of those privileges because the privileged users are auditing themselves
Unlimited User Privileges	Users have system privileges in excess of those required to do their jobs.
Poor Patch Management	Vendor patches are not appropriate or consistently implemented.
Interconnection Weaknesses	Weaknesses in interconnected systems can expose connected systems.
Copyright Protection Violations	Unauthorized use of copyrighted programs can leave an organization open to significant financial penalties.
Poor Logical Access Controls	Logical access controls are not consistently employed to protect sensitive data from unauthorized access.
Weak Passwords/No Passwords	Users are allowed to select easily guessed passwords or passwords are not implemented. A detailed description of the password registry settings will be provided in the SSP.
Unprotected Networks	No protections (e.g. firewalls, Anti-Virus software, Internet Protocol (IP) filtering) are employed to protect the network.
Weak Integrity Verification	Weak Integrity Verification may not detect data corruptions.
Live Data on Website	Live data on a website presents a double vulnerability in that corrupt data may be distributed before being vetted, and the live data is more vulnerable to corruption by an attacker.
Unknown Vulnerabilities	This is a place holder to consider if there is any vulnerability that is not otherwise addressed.

Appendix C: Common Attack Methods

Vast amounts of information and software are available on the Internet that enable an intruder or malicious insider to detect vulnerabilities and penetrate systems and networks. Table C-1 below describes several attack methods.

Table C-1. Attack Method Descriptions

Attack Method	Method Description
Remote Penetration	Attacks launched from a remote location, typically over the Internet.
Local Penetration	Attacks that are implemented on the system utilizing direct physical access to it.
Denial of Service (DoS)	These attacks result in the system being unavailable for its intended use. It may involve flooding a network connection beyond its capacity, so a system is effectively unable to communicate; overloading a system’s internal processing, so it slows to a virtual halt; or causing a system to crash. A DoS does not necessarily involve penetration, and may only last only as long as the system is actively being attacked, however it might also have lasting effects.
Network Scanners	These are programs that search a network in order to determine its structure, and find computers and network services available to be attacked.
Vulnerability Scanners	These are programs similar to network scanners, but they also assess whether a system is vulnerable to particular types of attack.
Password Crackers	These are programs that obtain passwords by extracting and deciphering them from their storage on a system.
Dictionary Attacks	This attack determines a password through repeated guessing, attempting access repeatedly with different words from a dictionary. It may be utilized by a password cracker program or through remote login attempts over a network.
Brute-Force Attacks	This attack determines a password through repeated guessing, exhaustively trying every possible combination of letters, digits, and other characters it may contain. This type of attack is rarely practical to use over a network, but is a common method used by password crackers, which can work extremely fast due to their direct access to the file storing the passwords.
Sniffers	These are programs that eavesdrop on network traffic. Often they have features to automatically extract usernames and passwords, or record specific “conversations” between systems, such as those involving a particular users’ access to a Web site or use of instant messaging. Certain network services, such as FTP, are particularly vulnerable to this attack because they transmit data without encrypting it.
Malicious Code	Programs designed to corrupt or collect data or block the use of data and other system resources or assist in identity theft or other acts of fraud.

Hackers, fraudsters, and other criminals utilize methods to trick a user into accepting a falsehood as fact. Some examples of attacks, referred to as spoofing or phishing, are shown in Table C-2 below.

Table C-2. Spoofing Methods Description

Attack Method	Method Description
E-mail Spoofing	An attacker forges an e-mail message to make it appear that the message originated from a third party This type of exploit is also referred to as “phishing.”
IP Spoofing	A person manipulates the data his computer is sending over a network so that it appears to be originating from a different network address. This can be used to implement a Denial-of-Service (DoS) attack, or to defeat security that controls access based on the source’s network address.
Domain Spoofing	An attacker may corrupt the domain name system so that when users attempt to access a particular host by name, such as www.example.net, they are actually directed to a different Internet host.

Web Spoofing	A third party constructs a fake Web site that looks and functions like another trusted site. This spoofed site may be used to disseminate false information or to collect sensitive data that users would normally submit only to a trusted host.
--------------	---

Appendix D: Common Threat-Vulnerability Pairings

System-specific threats are identified from interviews with the Project Manager, System Engineers, and other system personnel as well as through reviews of reference and system documentation. The following table D-1 lists the 17 common threat-source vulnerability pairings applicable to information systems within NESDIS. Each of these pairings is categorized into one or more of the four major threat categories listed below:

- Denial of service – the application or its data is not available when needed
- Destruction - the application or its data has been destroyed, also referred to as a loss of integrity
- Unauthorized modification - the integrity of the application or its data has been damaged through unauthorized modification
- Unauthorized disclosure of data – data, such as a user’s password, has been viewed by unauthorized individuals.

Table D-1: Threat-Source/Vulnerability Pairings

Threat Source	Vulnerability Description	Denial of Service	Destruction	Unauthorized Modification	Unauthorized Disclosure
Fire	Inadequate fire suppression practices could result in system equipment or facilities damage by accidental or intentional fire.	✓	✓		
Natural Disaster	Inadequate facility protections or plans and resources for backup processing and system resumption could result in system damage or interruption by natural occurrences (e.g., earthquakes, hurricanes, tornadoes).	✓	✓		✓
Water Damage/ Leaks	Inadequate facility protections or plans and resources for backup processing and system resumption could result in system damage or interruption by water from internal or external sources.	✓	✓		
Sabotage/ Theft/ Vandalism	Inadequacies in physical security controls and weaknesses in logical access controls could result in sabotage, theft, and vandalism of IT system components and data. Sabotage is premeditated destruction or malicious modification of assets or data for personal or political reasons. Vandalism is the destruction of system resources with no clearly defined objective. Theft is the unauthorized removal of computer equipment or media.	✓	✓	✓	✓

Malicious Hackers (Crackers)/ Social	Inadequacies in software configuration management, patch management, system and software integrity controls, and personnel	✓		✓	✓
--------------------------------------	--	---	--	---	---

Threat Source	Vulnerability Description	Denial of Service	Destruction	Unauthorized Modification	Unauthorized Disclosure
Engineering	training could result in software being modified to bypass system security controls, manipulate data, or cause denial of service. Social engineering is the human-to-human interaction in which a hacker gathers data for use in modifying or manipulating the system.				
Malicious Software	Inadequacies in software configuration management, patch management, and system and software integrity controls could result in malicious software such as viruses or Worms being introduced to the system, causing damage to the data or software.	✓	✓	✓	✓
Unintentional Human Error	Inadequacies in software configuration management, patch management, system and software integrity controls, and personnel training could result in application and support system components being inappropriately modified or destroyed due to unintentional administrator or user error.	✓	✓	✓	✓
Bomb Threat	Inadequate plans and resources for continuity of operations and emergency management could result in system damage or interruption due to notification of the existence of an explosive device at a facility, whether true or not, which may interrupt system services.	✓	✓		
Power Interruptions or Failure	Inadequate facility protections or plans and resources for uninterruptible power supply could result in system damage or interruption by a power failure or fluctuation. This may cause denial of service to authorized users (failure) or a modification of data (fluctuation).	✓		✓	
Improper Storage of Media	Unauthorized personnel may gain access to sensitive data when media (e.g., excess equipment, diskettes, hard copy, etc.) is not properly stored.		✓	✓	✓
Unauthorized Access to Facility	Inadequate safeguards, procedures, or inattentiveness of personnel may permit access to the facility by unauthorized personnel.		✓	✓	✓

Unauthorized System Access	Inadequate safeguards, procedures, or inattentiveness of personnel may		✓	✓	✓
----------------------------	--	--	---	---	---

Threat Source	Vulnerability Description	Denial of Service	Destruction	Unauthorized Modification	Unauthorized Disclosure
	result in access to the computer area by unauthorized personnel.				
Hardware Malfunction or Failure	Failure or malfunction of hardware may cause denial of service to system users. Additionally, hardware configuration may be altered in an unauthorized manner, leading to inadequate configuration control or other situations that may impact the system.	✓		✓	✓
Software Malfunction or Failure	Software malfunction or failure resulting from insufficient configuration controls (i.e., testing new releases, performing virus scans) may result in system failures.	✓	✓	✓	✓
Communication Failure	Communication links may fail during use or may not provide appropriate safeguards for data.	✓		✓	✓
Environmental Control Failure	Air conditioning, heating, or humidity controls may malfunction resulting in extreme temperatures and humidity causing damage to system components.	✓	✓		
Misuse of System Resources	Individuals may employ system resources for unauthorized purposes.	✓	✓	✓	✓

Appendix E: Risk Matrix Example and Risk Ranges for Threats and Vulnerabilities

The threat likelihood and vulnerability impact ratings are entered into the Risk Matrix, which when completed provides a quantitative value for potential residual risk where a threat intersects a vulnerability. A spreadsheet template for the Risk Matrix is available on the NESDIS IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php. An example of a completed Risk Matrix is provided in Figure E-1.

Figure E-1: Example Risk Matrix

Threats	Vulnerability																							Risk Total for Threat	Risk Exposure Level from Threats													
	WIS	Inadequate Security Policy	Inadequate System Administration	Inadequate User Account Management	Inadequate Personnel Management	Inadequate Contingency Plan	Inadequate Warning Banners	Use of Replayable RSA	Sharing of ID or Passwords	Inadequate Audit Log	Inadequate Audit	Data Transmissions in Plain Text	Susceptibility to Line Tapping	Inconsistent Physical Parameter Definition	Inadequate Facilities	Data Unavailability	Inadequate Hardware / Component	Unstable / Insufficient Communication	Inadequate / Missing Documents	Weak Rules of Behavior	Untrained Users	No Individual Accountability	No System Change Control			No Software Change Control	No Separation of Duties	Unlimited User Privilege	Poor Patch Management	Interconnection Weaknesses	Copyright Protection Violations	Weak Passwords	Poor Logical Access Controls	Weak Integrity Verification	Unprotected Networks	Live Data On Website	Unknown Vulnerability	
Natural Disaster	1																																			5	L	
Fire	1																																				5	L
Transportation Accident	1																																				5	L
Electrical Disturbance	1																																				5	L
Electrical Failure	1																																				5	L
Hardware Failure	1																																				8	L
Environmental Failure	1																																				5	L
Liquid Leakage	1																																				5	L
Chemical or Biological Contamination	1																																				4	L
Operator Error	1	5																																			28	L
User Error	1	5	1	3	1	1					5	5																									23	L
Configuration Error	5	5	5																																		115	M
Software Error	3																																				33	M
Resource Consumption - Computer	1	3	1								3	3																									19	L
Resource Consumption - Comms	1	5	1								5	5																									18	L
Telecommunication Interruption	1																																				4	L
External Influence / Terrorism	1			3	1	1																															8	L
Theft	1			3	1	1																															20	L
Fraud	1			3	1	1	1	1	5	5																											24	L
Intentional Disclosure	1			3	1	1																															10	L
Eavesdropping	1			3	1	1																															9	L
Social Engineering	1			3	1	1																															9	L
Information Warfare	1			3	1	1																															19	L
Mission Disruption	5			5																																	300	M
Malicious Programs / Virus	3			3							15	15																									129	M
Unauthorized Access	3	3	3	3						3	15	15																									135	M
Unauthorized Modification / Vandalism	5	25	5	15	5	5				5	25	25																									300	M
Disgruntled Employee / Insider Penetration / Unauthorized Use	5	25	5	15	5	5				5	25	25																									285	M
Unknown Threat	3										15	15																									78	H
Risk Total for Vulnerability	70	24	32	66	33	29	15	10	120	145	22	2	20	24	29	29	21	10	15	30	65	31	75	24	20	32	30	120	24	6	43	55	15	1483				
Risk Exposure Level from Vulnerabilities		M	L	M	L	L	L	L	L	M	M	L	L	L	L	L	L	L	M	L	M	M	M	M	M	M	M	M	H	M	M	M	H	M	1483	Moderate		

When the threat likelihood ratings are completed, the Risk Exposure Range Levels for Threats is consulted to equate the numerical threat scores to a Low, Moderate, or High risk level. Table E-1 shows the Risk Exposure Range Levels for Threats.

Table E-1: Risk Exposure Range Levels for Threats

<i>Threat Description</i>	<i># of Exploitable Vulnerabilities</i>	<i>Low</i>		<i>Medium</i>		<i>High</i>	
Natural Disaster/Acts of Nature	5	1	15	16	75	76	125
Fire	5	1	15	16	75	76	125
Transportation Accident	5	1	15	16	75	76	125
Electrical Disturbance	5	1	15	16	75	76	125
Electrical Failure	5	1	15	16	75	76	125
Hardware Failure	6	1	18	19	90	91	150
Environmental Failure	5	1	15	16	75	76	125
Liquid Leakage	5	1	15	16	75	76	125
Chemical or Biological Contamination	4	1	12	13	60	61	100
Operator Error	10	1	30	31	150	151	250
User Error	9	1	27	28	135	136	225
Configuration Error	13	1	39	40	195	196	325
Software Error	5	1	15	16	75	76	125
Resource Consumption - Computer	7	1	21	22	105	106	175
Resource Consumption - Comms	6	1	18	19	90	91	150
Telecommunication Interruption	4	1	12	13	60	61	100
External Influence / Terrorism	6	1	18	19	90	91	150
Theft	14	1	42	43	210	211	350
Fraud	10	1	30	31	150	151	250
Intentional Disclosure	6	1	18	19	90	91	150
Eavesdropping	9	1	27	28	135	136	225
Social Engineering	7	1	21	22	105	106	175
Information Warfare	11	1	33	34	165	166	275
Mission Disruption	16	1	48	49	240	241	400
Public Website Failure	0	1	0	1	0	1	0
Public Website Defamation	0	1	0	1	0	1	0
Malicious Programs / Virus	19	1	57	58	285	286	475
Unauthorized Access	19	1	57	58	285	286	475
Unauthorized Modification / Vandalism	26	1	78	79	390	391	650
Disgruntled Employee	25	1	75	76	375	376	625
Unknown Threats	6	1	18	19	90	91	150
Totals/Ranges	273	31	819	820	4095	4096	6825

When the vulnerability impact ratings are completed, the Risk Exposure Range Levels for Vulnerabilities is consulted to equate the numerical threat scores to a Low, Moderate, or High risk level. Table E-2 shows the Risk Exposure Range Levels for Vulnerabilities.

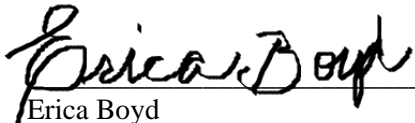
Table E-2: Risk Exposure Range Levels for Vulnerabilities

<i>Vulnerability Description</i>	<i># of Threat Exploits</i>	<i>Low</i>		<i>Medium</i>		<i>High</i>	
Inadequate Security Policy	6	1	18	19	90	91	150
Inadequate System Administration	10	1	30	31	150	151	250
Inadequate User Account Management	8	1	24	25	120	121	200
Inadequate Personnel Management	8	1	24	25	120	121	200
Incomplete Contingency Plan	19	1	57	58	285	286	475
Inadequate Warning Banners	3	1	9	10	45	46	75
Use of Replayable I&A	8	1	24	25	120	121	200
Sharing of ID or Passwords	8	1	24	25	120	121	200
Inadequate Audit Log	10	1	30	31	150	151	250
Inadequate Audit Analysis	11	1	33	34	165	166	275
Data Transmissions in the Clear	2	1	6	7	30	31	50
Susceptibility to Line Tapping	2	1	6	7	30	31	50
Inconsistent Physical Perimeter Definition	8	1	24	25	120	121	200
Inadequate Facilities	15	1	45	46	225	226	375
Data Unavailability	19	1	57	58	285	286	475
Inadequate Hardware/ Component	11	1	33	34	165	166	275
Unstable/Insufficient Communication	13	1	39	40	195	196	325
Inadequate / Missing Documents	2	1	6	7	30	31	50
Weak Rules of Behavior	5	1	15	16	75	76	125
Untrained Users	8	1	24	25	120	121	200
No Individual Accountability	7	1	21	22	105	106	175
No System Change Control	7	1	21	22	105	106	175
No Software Change Control	7	1	21	22	105	106	175
No Separation of Duties	10	1	30	31	150	151	250
Unlimited User Privileges	11	1	33	34	165	166	275
Poor Patch Management	8	1	24	25	120	121	200
Interconnection Weaknesses	12	1	36	37	180	181	300
Copyright Protection Violations	4	1	12	13	60	61	100
Weak Passwords/No Passwords	6	1	18	19	90	91	150
Poor Logical Access Controls	8	1	24	25	120	121	200
Weak Integrity Verification	6	1	18	19	90	91	150
Unprotected Networks	7	1	21	22	105	106	175
Live Data on Website	3	1	9	10	45	46	75
Unknown Vulnerabilities	1	1	3	4	15	16	25
Totals/Ranges	273	34	819	820	4095	4096	6825

Approval Page


Document Number: NQP-3413, Revision 2.1	
Document Title Block: Policy and Procedures for IT Security Risk Management and Conducting Risk Assessments	
Process Owner: NESDIS Chief Information Division	Document Release Date: October 8, 2013

Prepared by:


Erica Boyd
Ambit- Associate Consultant
NESDIS Chief Information Office

3/26/15
Date:

Approved by:


Irene Parker
Assistant Chief Information Officer - Satellites

3/26/15
Date:

Document Change Record

VERSION	DATE	CCR #	SECTIONS AFFECTED	DESCRIPTION
2.1	March 26, 2015	----	ALL	Baseline NQP-3413