NOAA/NESDIS

NESDIS-PR-1303.1

RISK MANAGEMENT PROCEDURAL REQUIREMENTS

December 2020

COMPLIANCE IS MANDATORY

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approval Page

Document Number: **NESDIS-PR-1303.1**	
Document Title Block: **NESDIS RISK MANAGEMENT PROCEDURAL REQUIREMENTS**	
Process Owner: Dan St. Jean	**Document Release Date**: December 31, 2020 **Expiration Date**: December 30, 2025

Prepared by:

ST JEAN.DANIEL.PAUL.1365819900 Digitally signed by ST JEAN.DANIEL.PAUL.1365819900 Date: 2021.03.30 07:14:30 -04'00'

_____ _____

Dan St. Jean Date
Acting Chief, Policies, Procedures, and
Systems Assurance Division
Office of Systems Architecture
and Advanced Planning

Approved by:

GRIFFIN.VANESSA.L.1204308663 Digitally signed by GRIFFIN.VANESSA.L.1204308663 Date: 2021.03.15 07:40:13 -04'00'

_____ _____

Vanessa Griffin Date
Director, Office of Systems Architecture
and Advanced Planning

Document Change Record

Version	Description	CCR#	Revised Sections	Date
1	Initial version		All	May 18, 2020

Table of Contents

Table of Figures

Table of Tables

1. Introduction

1.1. Purpose

This National Environmental Satellite, Data, and Information Service (NESDIS) Procedural Requirements document (NESDIS-PR-1303.1) establishes the Enterprise Risk Management (ERM) process and requirements by which NESDIS manages risks at all levels of the Enterprise. As the National Oceanic and Atmospheric Administration (NOAA) organization responsible for environmental data and products from satellites and other sources, and as a trusted authority to the Nation for weather and climate information, NESDIS has established this Procedural Requirements (PR) as a framework and guidance for risk management (RM). The document also serves as guidance for the development and implementation of RM Plans (RMPs) for the appropriate organizational elements of the NESDIS Enterprise.

1.2. Applicability

a. This PR applies to all NESDIS Offices (as defined in Appendix A). It applies to NESDIS employees and NESDIS support contractors that provide NESDIS technical work. It applies to other contractors, grant recipients, or parties to agreement only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

b. NESDIS Offices may develop office-level RM processes (if needed) that conform to this PR.

c. The requirements enumerated in this document are applicable to all projects (as defined in Appendix A). For existing projects, the Director of the Office of Systems Architecture and Advanced Planning (OSAAP) may approve requests for variance allowing continuation of current practices.

d. NOAA collaborates with many domestic and international partners to fulfill its mission. With OSAAP's concurrence and mutual agreement, NESDIS Offices may tailor the requirements of this PR or follow the partner's requirements management approach. This document should be used as a reference to compare with the partner's processes to verify their completeness.

e. In this PR, all mandatory actions (i.e., requirements) are identified by the symbol "[REQ]" to unambiguously define all requirements. They are also captured in the Requirements Matrix in Appendix C. The Requirements Matrix takes precedence if there are any discrepancies between the narrative and matrix with respect to identifying requirements. The terms "shall" and "must" are not used to specify mandatory actions because they can be interpreted as legally binding terminology, which removes all agency discretion and can create a potential liability problem for NOAA/NESDIS.

f. The requirements established in this PR may be tailored using the guidelines provided in Section 3.5.

1.3. Authority

NESDIS-PD-1110.1, NESDIS Systems Engineering and Program Management Policy

Note: The relationship of this document to other NESDIS program management and systems engineering documents is shown in Figure 1.

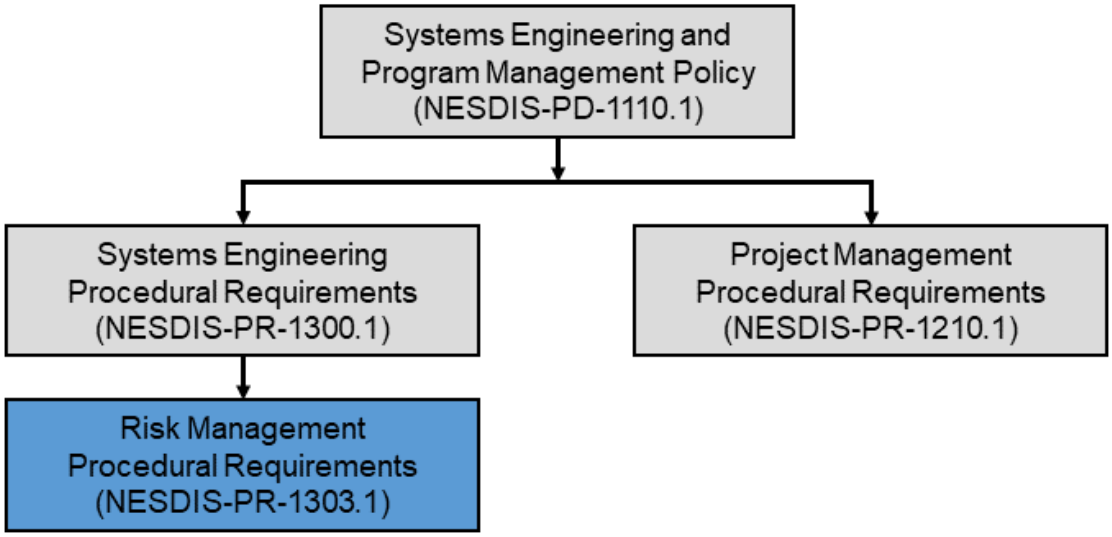


Figure 1: Hierarchy of Related Documents

1.4. Applicable Documents

a. OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control.
b. Department of Commerce Enterprise Risk Management Guidebook.
c. NOAA Framework for Enterprise Risk Management.
d. NESDIS-PR-1300.1, NESDIS Systems Engineering Procedural Requirements.
e. Commerce Information Technology Requirement (CITR-19) Risk Management Framework.

2. Roles and Responsibilities

2.1. Director, Office of Systems Architecture and Advanced Planning

For projects that do not execute solely within a single NESDIS Office, or meet the following criteria per Department of Commerce (DOC) Policy, OSAAP maintains the option to review and approve the RMPs:

- Does the project require special management attention because of its importance to NESDIS' mission or functions?
- Does the project have significant policy implications?
- Does the project have external visibility?
- Does the project have high development, operating, or maintenance costs?
- Does the project have an unusual funding mechanism?
- Is the project defined as major by DOC capital planning and investment control process?

[REQ-001] OSAAP ensures compliance with this PR.

2.2. NESDIS Office Directors

[REQ-002] NESDIS Office Directors establish policies, processes, and plans within their Office to execute the requirements of this PR.

2.3. Project Manager

[REQ-003] For project risk compliance, the Project Manager (PM) allocates adequate resources to meet the requirements of this PR commensurate with the scope, size, and complexity of the project.

2.4. NESDIS Authorizing Official's Designated Representative for CyberSecurity

[REQ-004] The NESDIS Authorizing Official's Designated Representative for Cybersecurity, acting on behalf of the Authorizing Official, is responsible for coordinating and carrying out the necessary activities required during the security accreditation for information systems in the project.

3. NESDIS Risk Management Procedural Requirements

3.1. Risk Management Concepts and Definitions

a. **Risk**: A risk is defined herein as a threat to NESDIS and its ability to meet its objectives. It is a threat with sufficient information to indicate a negative consequence when measured against a technical, cost, schedule, or programmatic objective of the Enterprise. Risks may also entail significant legal policy implications including the potential inability to fully implement agreements with stakeholders or partners (commercial, government, or international).

b. **Risk Management**: RM is the continuous process of coordinated activities regarding the management of risk. Successful management of risks requires focused management attention, and a deliberate, systematic process to identify and analyze risks, develop mitigations, and communicate threats to the Enterprise performance objectives in as accurate and specific terms as possible. The management of risks is a recursive process, where managers of the respective organizational elements are called upon to make informed risk trade decisions on a continuous basis and communicate them openly through planned and focused meetings and discussions. The key to a successful risk management framework for NESDIS as an Enterprise is early risk identification, prioritization, and mitigation, so that the likelihood and/or magnitude of negative consequences are minimized. Implementation and follow-through of approved mitigation strategies is important to reduce the likelihood and/or the severity of the consequences.

c. **Enterprise Risk Management**: ERM is RM applied throughout the entire organization. ERM is an effective agency-wide approach to addressing the full spectrum of the organization's significant risks by considering the combined array of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an Enterprise-wide, strategically aligned portfolio view of organizational challenges that provides improved insight about how to more effectively prioritize and manage risks to mission delivery.

d. **Project and Program Risk Management**: Project RM seeks to minimize the likelihood and consequences of events that could negatively impact project goals and objectives. Project goals and objectives are typically reflected in the project's functional, budget, and schedule requirements. Managing risks to these requirements and objectives is inherent to a PM's job. Similar expectations are required of Program Managers. Project requirements as well as program goals and objectives are derived from and support the top-level DOC/NOAA/NESDIS goals and objectives. Projects and programs are initiated to improve the DOC/NOAA/NESDIS ability to meet their mission.

e. **Project Risk Management vs. Enterprise Risk Management**: While project RM focuses on the risks to project goals and objectives, ERM focuses on how these same risks impact DOC/NOAA/NESDIS goals and objectives. Therefore, PMs should not only identify and assess the risks to the project, but also identify the impact these projects'

risks would have on NOAA/NESDIS programs within the scope of DOC goals and objectives.

f. **Characterization of Risks**: Risks are characterized in two dimensions as follows.
   1. Likelihood: Likelihood is the quantitative and/or qualitative probability of the occurrence of a threat event.
   2. Consequence/Impact: Consequence/impact is the severity, importance, or significance as it relates to the outcome of the event occurring and what naturally follows (including timeframe or condition). It refers to the magnitude of negative impact that can be expected to result from the occurrence of a threat event.

g. **Risk Appetite**: The amount of risk an organization is willing to accept in pursuit of value is referred to as risk appetite. Without defining risk appetite clearly, an organization may be taking risks well beyond management's comfort level or may be passing up strategic opportunities due to an assumption of risk aversion. As NESDIS risk culture evolves, setting the risk appetite will improve the rigor of identifying top enterprise risks to meeting NESDIS mission.

h. **Risk Inventory (Risk Register)**: The risk inventory or risk register consists of recommended risk data to be collected and maintained for each risk. Figure 2 shows the DOC Risk Inventory Template.

Risk Inventory - DOC Template

The risk inventory shows recommended risk data to be collected and maintained per risk. Fields for risk scores assume that the Department-Level scoring methodology is used. If the scoring approach needs to be tailored to a particular area (i.e. a project or program), then consequence categories may be added. A note about this spreadsheet: Some fields contain pull-down menus. Fields marked **DO NOT EDIT** will automatically calculate the needed value and should not be adjusted.

#	Status (Select open or closed)	Risk Category (select one)	Risk Title	Risk Statement	DOC Risk Score (1 to 5)						DO NOT EDIT - Maximum Consequence	DO NOT EDIT DOC Score (L, C)	DO NOT EDIT DOC Severity	Rank	Impact Timeframe (Select Near: felt this FY; Mid: felt next FY; Far: felt in 3-5 yrs)	Risk Applicability (Select Common or Unique)	Span of Control (Select Within Bureau, Within DOC, Outside DOC)	Key Controls (List any policy or procedure in place to manage this)
					Likelihood	Consequence: Performance (incl cost & sch)	Consequence: Reputation	Consequence: Budget	Consequence: Compliance	Consequence: Safety & Security								

Figure 2: DOC Risk Inventory Template

i. **Issue**: An issue is a realized risk. An issue will be generated when a risk is triggered, and NESDIS is addressing the resulting consequences. Issues that were not previously identified as risks can also arise. If NESDIS is committing resources to recover from a negative event, this will be reported and managed as an issue.

j. **Concerns**: The NESDIS ERM process recognizes that there are other "concerns" that will need to be addressed and managed in the RM process. These concerns may be

candidate risks that are going through formal analysis and assessment and mitigation planning, or they may simply be candidate risks with insufficient information on which NESDIS leadership needs to maintain vigilance to provide early warning of arising risks.

3.2. Risk Management Process

NESDIS ERM function is informed by guidance and best practices from Office of Management and Budget (OMB) Circular A-123, the DOC ERM Framework, and the NOAA ERM Framework.

a. **Enterprise Risk Categories**

1. Categories of risk enable insight into trends in a portfolio view of the Enterprise risk profile. OMB Circular A-123 includes four Enterprise risk objective categories: Strategic, Operational, Reporting, and Compliance. Circular A-123 notes that agencies have discretion when there is overlap between these categories and may find it useful to include additional subcategories to facilitate communication on a narrower topic.
2. As shown in Table 1, the DOC has developed 10 categories of Enterprise risk that are common across its bureaus.

Table 1: Crosswalk of A-123 and DOC Risk Categories

A-123 Objective Category	**DOC Risk Category**
Strategic Objectives	Strategic Risk Reputation Risk Political Risk
Operational Objectives	Operational Risk Safety and Security Risk COOP/Disaster Recovery Risk Technology Risk
Reporting Objectives	Financial Risk
Compliance Objectives	Compliance and Regulatory Risk Fraud Risk

b. **NOAA Enterprise Risk Management Framework**

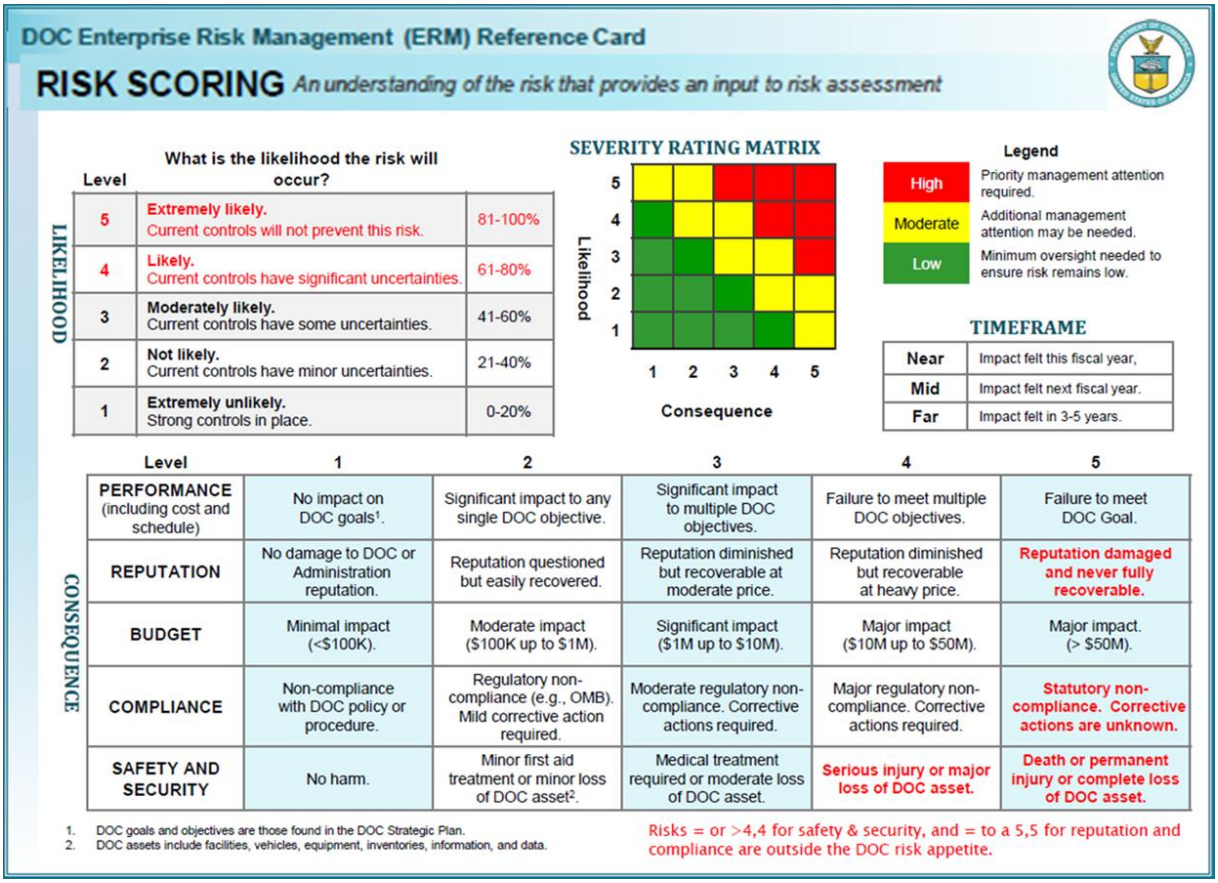
NOAA has established a framework for ERM. NESDIS aims to align its RM process with NOAA's ERM to support the bottom-up approach in managing risk across the Enterprise. For more information, please refer to the NOAA Framework for Enterprise Risk Management document.

NOAA's ERM is based on the DOC ERM Framework described in the DOC Enterprise Risk Management Guidebook. There are six phases in this to identify, assess, and respond to risks. These components are outlined in Figure 3.

1. **Organize**: In the Organize phase, personnel are identified to fulfill key roles and responsibilities. Organizational objectives and goals are considered, and "tone at the top" is established for implementing ERM. NESDIS Leadership sets objectives to meet the NESDIS mission, strategic plan, and goals and requirements of applicable laws and regulations. Leadership defines these objectives in specific and measurable terms to enable management to identify, analyze, and respond to risks in achieving those objectives.
2. **Identify and Score**: Risk identification and scoring are fundamental to ERM. Risk identification begins by thinking about uncertain events or conditions that have the potential to impact NESDIS goals and objectives.

Figure 3: DOC ERM Framework Methodology

Once risks have been identified, the next step is to score the risks using a risk scoring card. Both DOC and NOAA have developed risk management reference cards that provide guidelines to identifying and scoring risks (Figure 4 and Figure 5).



DOC Enterprise Risk Management (ERM) Reference Card

RISK SCORING *An understanding of the risk that provides an input to risk assessment*

Level	What is the likelihood the risk will occur?	
5	**Extremely likely.** Current controls will not prevent this risk.	81-100%
4	**Likely.** Current controls have significant uncertainties.	61-80%
3	**Moderately likely.** Current controls have some uncertainties.	41-60%
2	**Not likely.** Current controls have minor uncertainties.	21-40%
1	**Extremely unlikely.** Strong controls in place.	0-20%

LIKELIHOOD

SEVERITY RATING MATRIX

Legend

High	Priority management attention required.
Moderate	Additional management attention may be needed.
Low	Minimum oversight needed to ensure risk remains low.

TIMEFRAME

Near	Impact felt this fiscal year,
Mid	Impact felt next fiscal year.
Far	Impact felt in 3-5 years.

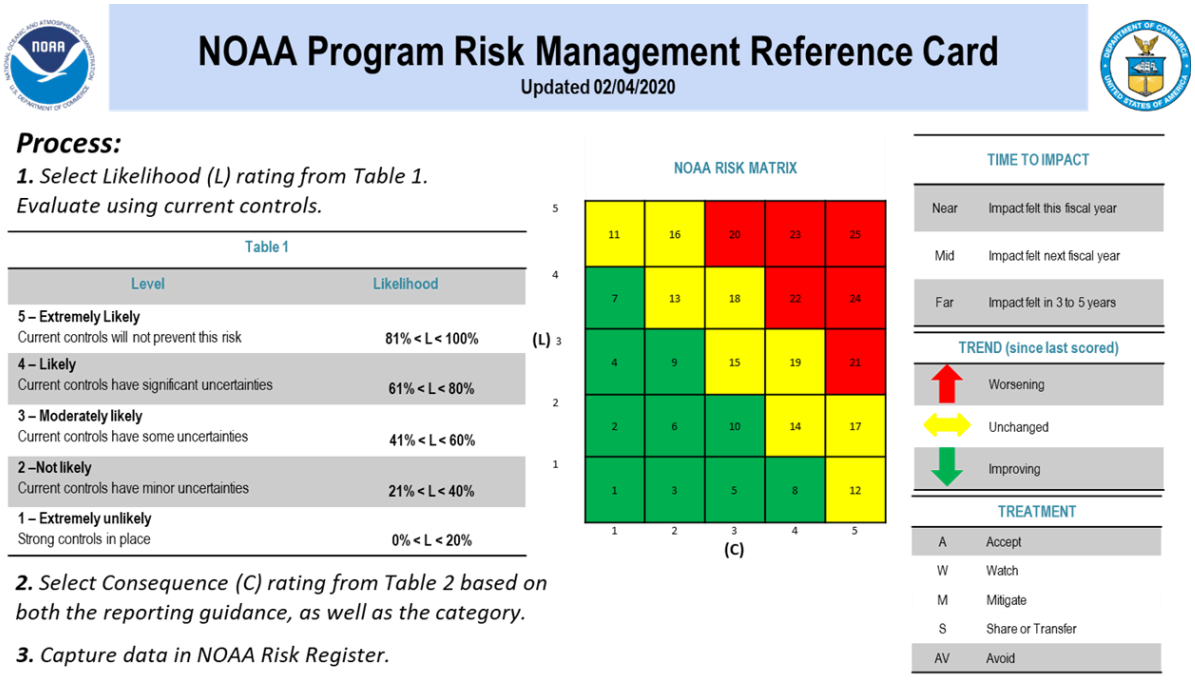
CONSEQUENCE

Level	1	2	3	4	5
PERFORMANCE (including cost and schedule)	No impact on DOC goals[1].	Significant impact to any single DOC objective.	Significant impact to multiple DOC objectives.	Failure to meet multiple DOC objectives.	Failure to meet DOC Goal.
REPUTATION	No damage to DOC or Administration reputation.	Reputation questioned but easily recovered.	Reputation diminished but recoverable at moderate price.	Reputation diminished but recoverable at heavy price.	**Reputation damaged and never fully recoverable.**
BUDGET	Minimal impact (<$100K).	Moderate impact ($100K up to $1M).	Significant impact ($1M up to $10M).	Major impact ($10M up to $50M).	Major impact. (> $50M).
COMPLIANCE	Non-compliance with DOC policy or procedure.	Regulatory non-compliance (e.g., OMB). Mild corrective action required.	Moderate regulatory non-compliance. Corrective actions required.	Major regulatory non-compliance. Corrective actions required.	**Statutory non-compliance. Corrective actions are unknown.**
SAFETY AND SECURITY	No harm.	Minor first aid treatment or minor loss of DOC asset[2].	Medical treatment required or moderate loss of DOC asset.	**Serious injury or major loss of DOC asset.**	**Death or permanent injury or complete loss of DOC asset.**

1. DOC goals and objectives are those found in the DOC Strategic Plan.
2. DOC assets include facilities, vehicles, equipment, inventories, information, and data.

Risks = or >4,4 for safety & security, and = to a 5,5 for reputation and compliance are outside the DOC risk appetite.

Figure 4: DOC ERM Reference Card



NOAA Program Risk Management Reference Card

Updated 02/04/2020

Process:

1. *Select Likelihood (L) rating from Table 1. Evaluate using current controls.*

Table 1

Level	Likelihood
5 – Extremely Likely Current controls will not prevent this risk	81% < L < 100%
4 – Likely Current controls have significant uncertainties	61% < L < 80%
3 – Moderately likely Current controls have some uncertainties	41% < L < 60%
2 –Not likely Current controls have minor uncertainties	21% < L < 40%
1 – Extremely unlikely Strong controls in place	0% < L < 20%

2. *Select Consequence (C) rating from Table 2 based on both the reporting guidance, as well as the category.*

3. *Capture data in NOAA Risk Register.*

NOAA RISK MATRIX

TIME TO IMPACT

Near	Impact felt this fiscal year
Mid	Impact felt next fiscal year
Far	Impact felt in 3 to 5 years

TREND (since last scored)

	Worsening
	Unchanged
	Improving

TREATMENT

A	Accept
W	Watch
M	Mitigate
S	Share or Transfer
AV	Avoid

Figure 5: NOAA Program Risk Management Reference Card

Both DOC and NOAA reference cards use a standard 5×5 risk matrix, also known as a “heat map” or “probability and impact diagram”, to score risks. NESDIS must develop a similar reference card to manage its risk and to elevate risks to NOAA. When scoring risks, most Risk Owners use professional judgment to determine the likelihood and consequence of risk events. Scoring considers the likelihood, L, of a risk event occurring in a timeframe and the consequence, C, of the event should it occur. Pairing the likelihood of occurrence with the consequence yields a relative characterization of severity, a key consideration when selecting a RM strategy. As shown in Figure 4, the likelihood of risk occurrence is classified as follows.

A. High Risk: High risks are expected to occur with severe impacts, if realized. They are denoted in the upper right-hand (red) region of the DOC ERM Reference Card. These risks require priority management attention.
B. Moderate Risk: Moderate risks may occur, and impacts would be significant, but are not catastrophic. They are denoted in the middle (yellow) region of the DOC ERM Reference Card. These risks may require additional management attention.
C. Low Risk: Low risks are not likely to occur, or potential impacts are not expected to be significant. They are denoted in the lower left-hand (green) region of the NESDIS Risk Scorecard. In this case, minimum management oversight is required to ensure that the risk likelihood remains low.

3. **Assess**: In the Assess phase, risk owners/responders analyze and document key information on a risk including root causes, NESDIS mission(s) impacted, and the potential positive or negative outcomes in a risk profile template. This analysis validates and verifies preliminary assumptions about the risk. Full risk assessments are resource intensive, and the risks targeted for assessment must first be selected. It is common practice to select risks based on their severity (determined by their score on the 5×5 risk matrix), with high severity risks given highest priority (i.e., risks that score in the “red” range on the 5×5 risk matrix). The decision to further assess a risk should also consider organizational concerns, available resources, the initial identification of key controls, and the immediacy of the area considered, as well as regulatory mandates and new or revised regulatory requirements.
4. **Treat**: For each of the risks identified, a response is determined, subject to management approval. Table 2 shows a range of possible responses for dealing with risks.

Table 2: Risk Responses for Dealing with Risks

Response	Description
Accept	Accepting the risk by informed decision. Accepting risk implies an organization is comfortable that the potential impact of the risk lies within an acceptable range. Accepting risk frequently occurs when the cost of taking action outweighs the cost of the risk should it occur. Accepting risk may also occur when mitigation depends on an outside

Response	Description
	organization and no further action can be taken without support from that organization.
Avoid	Avoiding a risk entails a decision that eliminates the risk as a factor for the organization. Some risks may be avoided by not starting or continuing the activity that gives rise to risk.
Escalate/ Elevate	A risk is usually escalated (or elevated) to the appropriate level of the organization that matches the objective that would be affected if the risk occurred. Escalation is the action taken when the risk or the proposed response exceeds the authority of the Office/Program.
Mitigate	Mitigating a risk requires management action to reduce the likelihood and/or the consequence of the risk, which often requires applying internal controls.
Research	Researching the risk to get more information to better assess for a future date.
Transfer	Transferring all or part of the risk to another party. Transferring does nothing to the risk itself. It merely moves liability associated with risk to another party. Risk transfer may involve payment of a risk premium to the party taking on the risk.
Watch	Watching the risk or acknowledging the existence of a risk while pursuing the activity. This involves tracking the risk over time to make sure the severity does not change. If the situation begins to deteriorate, a change in response may be enacted.

Selecting the appropriate risk response often involves balancing cost and benefit. When selecting options, NESDIS Leadership and Risk Owners should consider the values and perceptions of stakeholders and appropriate ways to communicate response decisions. If the risk response impacts risk elsewhere in the organization or stakeholders, those potentially impacted should be involved in risk response decisions.

5. **Monitor**: Effective monitoring of both risks and controls is essential to the success of ERM. The objective of monitoring is to collect accurate, timely, and relevant risk information and to present it in a clear and easily understood manner to NESDIS Leadership responsible for managing risk. Monitoring is used to detect changes in the internal and external environment and alert for potential needed action. Monitoring should encompass all aspects of the RM process to:
    - Identify emerging risks;
    - Ensure risk responses and any associated controls are effective and efficient in both design and operation;
    - Obtain further information to improve risk assessment;
    - Analyze and learn lessons from events (including near misses, changes, trends, successes, and failures); and

- Detect changes in the risk criteria and the risk itself that require revision of risk priority and treatment.

An Enterprise risk profile is an aggregation of the prioritized risks across the Enterprise to assist leadership in decision-making. While risks have importance within projects and programs based on their context, simply aggregating risks from across the organization does not indicate that those risks are at the Enterprise level. Senior leadership must evaluate and prioritize risk to the organization as a whole to ensure risks in areas between organizational units are captured.

6. **Report**: Reporting is a critical component in the communication of risk information across the organization. NESDIS must provide dashboards and reports that highlight the risks to help facilitate strategic conversations on how to address them. NESDIS must also communicate and elevate (when appropriate) risk information to NOAA's Office of Performance, Risk, and Social Science (PRSS). NOAA is required to provide updated risk information to the DOC Office of Performance, Evaluation and Risk Management (OPERM) in accordance with OMB's A-123 Circular.

c. **ERM Tool**

Using an ERM tool will provide consistency and standardization in managing risks at all levels. Considering the significance of ERM, NESDIS will evaluate and, if feasible, implement an ERM tool to automate the RM process to the degree most appropriate and to ensure universal access by all stakeholders.

d. **Risk Management Process Requirements**

NESDIS will:

[REQ-005] Create a NESDIS RM scorecard aligned with the NOAA RM scorecard to provide guidance to NESDIS Offices/Programs.

[REQ-006] Provide risk acceptability criteria and elevation guidelines to be applied when escalating risks from Office/Programs to the Enterprise level.

[REQ-007] Establish a risk escalation function to escalate risks to NOAA's PRSS.

[REQ-008] Identify, procure, and configure an appropriate ERM tool to support ERM.

[REQ-024] Use the ERM tool to create and maintain a NESDIS Risk Inventory that contains the recommended risk information to be collected and maintained for each risk.

NESDIS Offices/Programs and projects will:

[REQ-009] Define and implement a comprehensive RM process that incorporates the RM functions described in this PR.

[REQ-010] Develop an RMP that defines how the ERM functions will be implemented in accordance with the ERM process described in this PR.

[REQ-011] Establish RM board(s) to govern RM activities.

[REQ-012] Establish and maintain NESDIS and lower-level risk inventories with recommended risk data to be collected and maintained per risk.

[REQ-013] Provide risk information to support the milestone reviews described in the program/project documents such as the Project Management Plan (PMP) and the Systems Engineering Plan (SEP).

[REQ-014] Establish risk communication protocols including the frequency and content of reporting.

[REQ-015] Provide RM training to effectively carry out RM responsibilities.

3.3. Risk Management Plan

a. An RMP is a document that describes how RM is accomplished in an organization. It is a tailorable document that captures current and evolving RM strategy, and its relationship with the overall project management effort throughout the life cycle of the system. It identifies the RM roles and responsibilities and provides the basis for implementing and communicating risk information.
b. The RMP may be a separate document (if the project is of sufficient size or complexity) or part of other project planning documents.
c. The RMP is baselined and updated in accordance with the requirements of NESDIS-PR-1223.1, Project Milestones Procedural Requirements.
d. The RMP is a controlled document and shall be reviewed by the PM throughout the project life cycle.
e. RMP requirements:
NESDIS Offices/Programs and projects will:

[REQ-016] Determine the appropriate level within the system structure at which the RMP is to be developed, taking into account factors such as the size and complexity of the project.

[REQ-017] Ensure that the RMP is consistent with higher-level RMPs and the project plan.

[REQ-018] Baseline and update the RMP per NESDIS-PR-1223.1, NESDIS Project Milestones Procedural Requirements.

3.4. Information Technology Risk Management

a. Information systems are subject to serious threats that can have adverse effects on organizational operations and assets, individuals, other organizations, and the Nation. These threats aim to exploit both known and unknown vulnerabilities to systems and compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems.
b. IT 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.

c. IT RM requirements:

[REQ-019] Develop policy and procedures to communicate the NESDIS-specific procedures for performing baseline and annual risk assessments.

[REQ-020] Develop policy and procedures to communicate the NESDIS-specific procedures for assessing supply chain risk assessments.

3.5. Opportunity Management

a. Traditional RM addresses the negative effects on one or more Enterprise objectives. Opportunity management helps to identify and understand possible ways in which objectives can be achieved more successfully.

b. The DOC ERM Framework and NOAA ERM Framework do not address opportunity management. Therefore, NESDIS has enhanced these frameworks to address opportunities.

c. An opportunity is defined as a risk that would have a positive effect on one or more Enterprise objectives. A benefit is an opportunity that has been realized, i.e., the probability of occurrence of the opportunity has reached 100%.

d. Table 3 provides a range of possible responses for dealing with opportunities.

Table 3: Responses for Dealing with Opportunities

Response	Description
Accept	Accepting the opportunity acknowledges its existence, but no proactive action is taken. This is appropriate when it is not possible or cost effective to address the opportunity in any other way, or for low-priority opportunities.
Enhance	This is used to increase the probability and/or impact of an opportunity. Early enhancement of an opportunity is more effective than improving the benefit after the opportunity is realized.
Escalate/ Elevate	An opportunity is usually escalated to the appropriate level of the organization that matches the objective that would be affected if the opportunity occurred. Escalation is the action taken when the opportunity or the proposed response exceeds the authority of the Office/Program.
Exploit	This response is appropriate for high-priority opportunities where the organization wants to ensure that the opportunity is realized. This strategy seeks to increase the probability of occurrence of the opportunity to 100%.
Research	Research involves researching the opportunity to get more information to better assess for a future date.
Share	This response involves sharing all or part of the opportunity with another party so that the third party shares some of the benefit if the opportunity occurs.

Response	Description
Watch	This is for watching the opportunity or acknowledging the existence of an opportunity while pursuing the activity. If the situation begins to improve, a change in response may be enacted.

e. Opportunity management requirements:

[REQ-025] NESDIS will create a NESDIS Opportunity Management Scorecard to provide guidance on managing opportunities.

[REQ-026] NESDIS will actively manage opportunities to improve its ability to accept and pursue opportunities.

3.6. Tailoring Guidelines

a. RM requirements tailoring is the process used to seek relief from the requirements of this PR consistent with project objectives, allowable risk, and constraints.

b. The tailoring process should occur at the beginning of a project but may occur at any time in the project's life cycle. It results in changes to the implementation of requirements depending on the timing of the request.

c. The results of tailoring will be documented in the Requirements Matrix (Appendix C) and submitted to OSAAP along with supporting rationale.

d. The results of the tailoring will be documented in the next revision of the RMP, along with supporting rationale and documented approvals from the requirement owner.

e. Tailoring requirements:

[REQ-021] Requests for tailoring are submitted through the NESDIS configuration change management process.

[REQ-022] The results of tailoring are documented in the Requirements Matrix (Appendix C) and submitted to OSAAP for approval along with supporting rationale.

[REQ-023] The results of the tailoring will be documented in the next revision of the RMP.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A: Glossary

Acceptable Risk: An identified risk that is understood and agreed to by the program/project, organization, Governing Council, Enterprise and other stakeholders(s) sufficient to achieve the defined success criteria utilizing the approved resources.

Analysis of Risk: An evaluation of all identified risks either qualitatively and/or quantitatively to estimate the likelihood of occurrence, consequence of occurrence, timeframe when mitigation actions are needed, classification into sets of related risks, and priority ranking.

Baseline: An agreed-to set of requirements, designs, budgets, schedules, or documents that will have changes controlled through a formal approval and monitoring process.

Benefit: A benefit is an opportunity that has been realized.

Concern: A candidate risk with insufficient or immature information to analyze or define mitigation options.

Consequence/Impact: the severity, importance, or significance as it relates to the cause of the event and what naturally follows (including timeframe or condition). It refers to the magnitude of harm that can be expected to result from the occurrence of the event.

Issue: An event or incident of impact to the organization that is currently occurring and that requires attention. An issue may have been a risk that was realized or identified.

Likelihood: the quantitative and/or qualitative probability of the occurrence of threat events initiating, and that the identified deficiency will result in an adverse impact.

NESDIS Office(s): A term used in the widest sense to include NESDIS Headquarters elements, NESDIS Operations and Acquisitions offices, the Center for Satellite Applications and Research (STAR), and the National Centers for Environmental Information (NCEI).

Opportunity: A risk that would have a positive effect on one or more objectives.

Organizational Element: Refers to the Offices or equivalent units that comprise the NESDIS organization, including their respective Divisions, Branches or groups under them.

Process: A set of activities used to convert inputs into desired outputs to generate expected outcomes and satisfy a purpose.

Program: A strategic investment that has defined goals, objectives, architecture, funding levels, and a management structure that supports one or more projects.

Project: A specific investment that has defined goals, objectives, requirements, lifecycle cost, a beginning, and an end. A project yields products or services that directly address NESDIS'

strategic needs. In this document, the term ‘project’ applies in the widest sense to include projects, programs, portfolios, and major initiatives.

Requirement: A statement that identifies a system, product, or process characteristic or constraint. A requirement statement must be clear, correct, feasible to obtain, unambiguous in meaning, and able to be validated at the level of the system structure at which it is stated.

Requirements Management: A process used to gather, analyze, decompose, verify, validate, track, and manage changes to requirements.

Risk: The combination of a) the probability (qualitative or quantitative) that an organization will experience an undesired event such as cost overrun, schedule slippage, safety mishap, or failure to achieve a needed technological breakthrough; and b) the consequences, impact, or severity of the undesired event were it to occur.

Risk Acceptance: Determination that the consequences of an identified risk, should they occur, are acceptable without further mitigation. No further resources are expended in managing this risk except periodic review (every six months) to ensure assumptions or circumstances have not changed.

Risk Assessment: Determination of perceived acceptability or severity of a risk following analysis of the risk (e.g., analysis indicates a schedule slip of 1 week; assessment determines if a 1 week slip is acceptable or catastrophic)

Risk Control: An activity that utilizes the status and tracking information to make a decision about a risk or risk mitigation effort, including resource allocation. Risk control is comprised of four decisions; continue as planned, re-plan, invoke a contingency plan, or close the risk.

Risk Elevation: The process of raising risk visibility by reporting the risk to a higher level in the organization. This is done either to raise the awareness and visibility of a risk, calling attention to adverse changes in consequence, likelihood of occurrence or timeframe, or to request resources that are not available to handle the risk at the lower level. Risks are elevated to one or more levels above the level at which it is initially owned and mitigated.

Risk Escalation: The process of increasing the visibility of a concern to a risk, or a risk to an issue.

Risk Identification: A continuous effort to capture, acknowledge and document risks as they are found.

Risk Inventory: A record of information on identified risks.

Risk Management (RM): RM is an organized, systematic decision making process that efficiently identifies, analyzes, plans, tracks, controls, communicates, and documents risk to increase the likelihood of achieving goals.

Risk Mitigation: The reduction of an identified risk by reducing the consequences, likelihood, or by delaying the projected time of occurrence (i.e. to allow time to mitigate, or beyond time which impacts the tasks being performed).

Risk Owner: The NESDIS Office/Program owning individual risk items and handling plan implementation to directly support the risk process with a pre-established minimum level of commitment.

Risk Register: A record of information on identified risks.

Risk Response (Handling Strategy): Establishes the proper course of action for dealing with a particular risk. Resulting actions are to watch, accept, research, or mitigate.

Risk Tracking: An activity to capture, compile, and report risk attributes and metrics which determine whether or not risks are being mitigated effectively and whether risk mitigation plans are being implemented correctly.

Success Criteria: The minimum set of measures that establish the accomplishment of predefined goals and objectives for a given activity or undertaking. Within the practice of risk management it usually refers to the establishment of goals and objectives for risk mitigation activities.

Share: The act of allocating authority, responsibility, and accountability for a risk to another person or organization.

System: The combination of elements that function together to produce the capability required to meet a need. The elements include all hardware, software, equipment, facilities, personnel, processes, and procedures needed for this purpose.

Tailoring: The process used to seek relief from in the implementation of PR requirements consistent with program or project objectives, allowable risk, and constraints.

Watch: The monitoring of an identified risk and its attributes for early warning of critical changes in consequences, likelihood, timeframe, or other indications that might reveal a risk event is imminent (Sub-Category of Accept).

Appendix B: Acronyms

AA	Assistant Administrator
AoA	Analysis of Alternatives
CITR	Commerce Information Technology Requirement
ConOps	Concept of Operations
COOP	Continuity of Operations
DOC	Department of Commerce
DUS/O	Deputy Under Secretary for Operations
ERB	Enterprise Risk Board
ERM	Enterprise Risk Management
HQ	Headquarters
IT	Information Technology
NASA	National Aeronautics and Space Administration
NCEI	National Centers for Environmental Information
NESDIS	National Environmental Satellite, Data, and Information Service
NOAA	National Oceanic and Atmospheric Administration
OMB	Office of Management and Budget
OSAAP	Office of Systems Architecture and Advanced Planning
PR	Procedural Requirements
PRSS	Performance, Risks, and Social Science
REQ	Requirement
RM	Risk Management
RMP	Risk Management Plan
ROM	Rough Order of Magnitude
RqMB	Requirements Management Board
STAR	Satellite Applications and Research

Appendix C: Compliance Matrix

Section	REQ#	Requirement
2.1	001	OSAAP ensures compliance with this PR.
2.2	002	NESDIS Office Directors establish policies, processes, and procedures within their Office to execute the requirements of this PR.
2.3	003	The Project Manager allocates adequate resources to meet the requirements of this PR commensurate with the scope, size, and complexity of the project.
2.4	004	The NESDIS Authorizing Official's Designated Representative for Cybersecurity, acting on behalf of the Authorizing Official, is responsible for coordinating and carrying out the necessary activities required during the security accreditation for information systems in the project.
3.2	005	Create a NESDIS Risk Management Scorecard aligned with the NOAA Risk Management Scorecard to provide guidance to NESDIS Offices/Programs.
3.2	006	Provide risk acceptability criteria and elevation guidelines to be applied when escalating risks from Office/Programs to the Enterprise level.
3.2	007	Establish a risk escalation function to escalate risks to NOAA's Office of Performance, Risk, and Social Science (PRSS).
3.2	008	Identify, procure, and configure an appropriate Enterprise Risk Management tool to support ERM.
3.2	024	Use the ERM tool to create and maintain a NESDIS Risk Inventory that contains the recommended risk information to be collected and maintained for each risk.
3.2	009	Define and implement a comprehensive risk management process that incorporates the RM functions described in this PR.
3.2	010	Develop a Risk Management Plan (RMP) that defines how the ERM functions will be implemented in accordance with the ERM process described in this PR.
3.2	011	Establish Risk Management Board(s) to govern risk management activities.
3.2	012	Establish and maintain NESDIS and lower-level risk inventories with recommended risk data to be collected and maintained per risk.

Section	REQ#	Requirement
3.2	013	Provide risk information to support the milestone reviews described in the program/project documents such as the Project Management Plan (PMP) and the Systems Engineering Plan (SEP).
3.2	014	Establish risk communication protocols including the frequency and content of reporting.
3.2	015	Provide RM training to effectively carry out risk management responsibilities.
3.3	016	Determine the appropriate level within the system structure at which the RMP is to be developed, taking into account factors such as the size and complexity of the project.
3.3	017	Ensure that the RMP is consistent with higher level RMPs and the project plan.
3.3	018	Baseline and update the RMP per the NESDIS Project Milestones Procedural Requirements document, NESDIS-PR-1223.1.
3.4	019	Develop policy and procedures to communicate the NESDIS-specific procedures for performing baseline and annual risk assessments.
3.4	020	Develop policy and procedures to communicate the NESDIS-specific procedures for assessing supply chain risk assessments.
3.5	025	NESDIS will create a NESDIS Opportunity Management scorecard to provide guidance on managing opportunities.
3.5	026	NESDIS will actively manage opportunities to improve its ability to accept and pursue opportunities.
3.6	021	Requests for tailoring are submitted through the NESDIS configuration change management process.
3.6	022	The results of tailoring are documented in the Requirements Matrix (Appendix C) and submitted to OSAAP for approval along with supporting rationale.
3.6	023	The results of the tailoring will be documented in the next revision of the RMP.

Appendix D: Reference Documents

- SP-2012-3422 Version 1.0 NASA Risk Management Handbook.
- NPR 8000.4 Agency [NASA] Risk Management Procedural Requirements
- The Standard for Risk Management in Portfolios, Programs, and Projects, Project Management Institute, 2019.
- NIST SP 800-30 Revision 1 Guide for Conducting Risk Assessments
- NIST SP 800-37 Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems

END OF DOCUMENT