Guide to Conducting Risk Assessments

Overview of NIST Special Publication 800-30, Revision 1

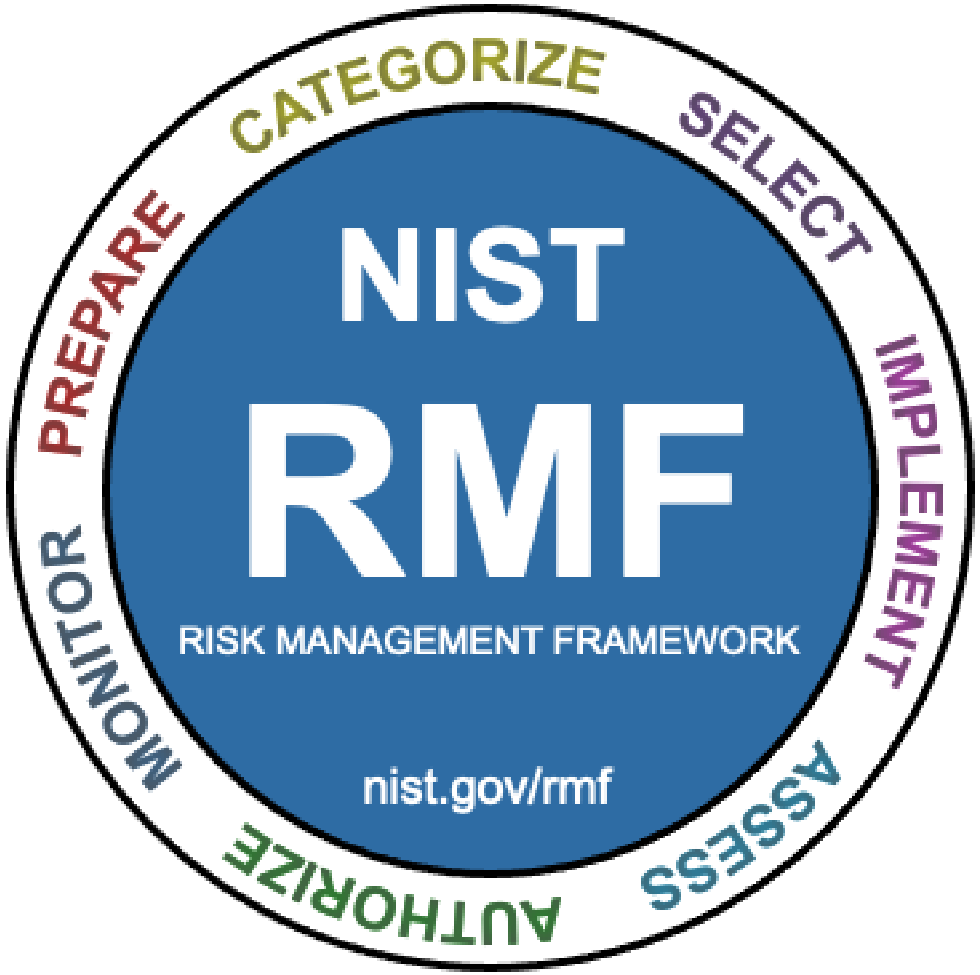
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Risk Management Framework (RMF) Team
sec-cert@nist.gov

Risk Management Framework Overview

The RMF provides a ***structured, yet flexible process*** for managing ***cybersecurity and privacy risk to information & systems*** that includes system categorization, control selection, implementation, assessment, authorization, and continuous monitoring.

Risk Management Framework Steps



Essential activities to **prepare** the organization to manage security and privacy risks

Categorize the system and information processed, stored, and transmitted based on an impact analysis

Select the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)

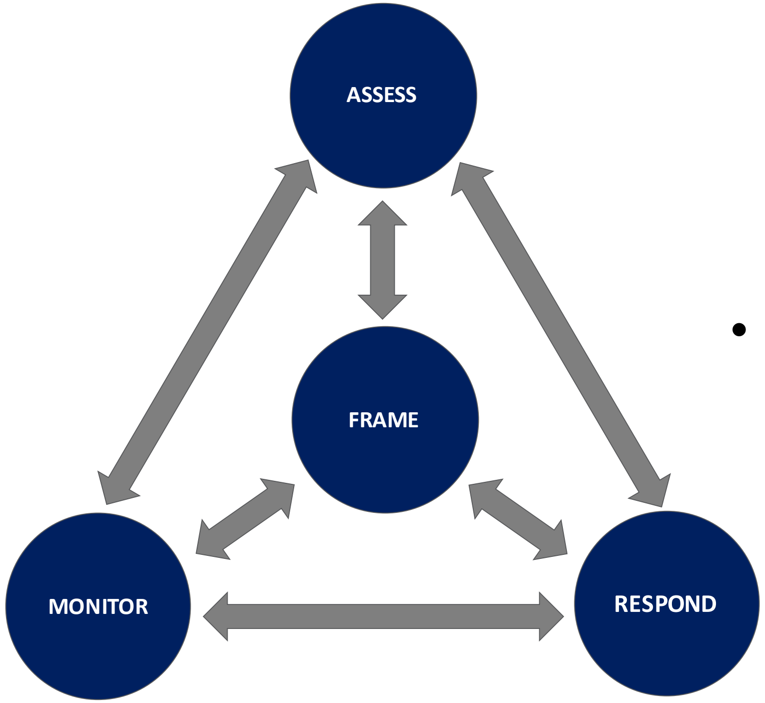
Implement the controls and document how controls are deployed

Assess to determine if the controls are in place, operating as intended, and producing the desired results

Senior official makes a risk-based decision to **authorize** the system (to operate)

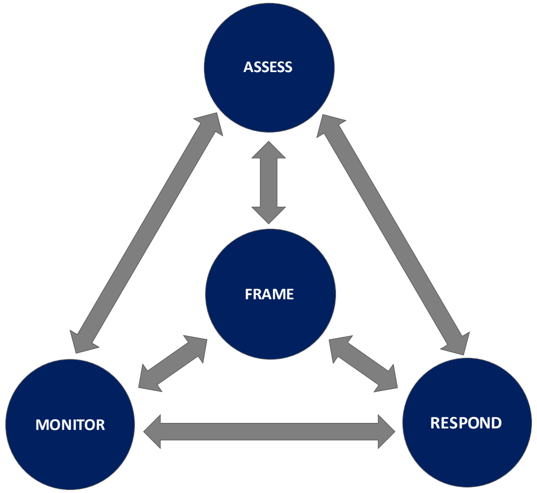
Continuously **monitor** control implementation and risks to the system

Risk **Management** and Risk **Assessment**



- ***Risk assessment*** is a key component of a holistic risk management process (as defined in NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and System View*)

- Risk management processes include:
  - Framing Risk
  - ***Assessing Risk***
  - Responding to Risk
  - Monitoring Risk



Framing

Establishing the context for how organizations manage information security risk

Assessment

Identify threat sources & events, vulnerabilities, determine risk (impact & likelihood) & uncertainty

RISK

Response

Develop risk response strategy (accept, reject, mitigate, share/transfer risk) & courses of action

Monitoring

Verify implementation, determine effectiveness of risk mitigation measures, identify changes

Key Terms in Risk Assessment

Risk

Risk Assessment

Threat

Vulnerability

Impact

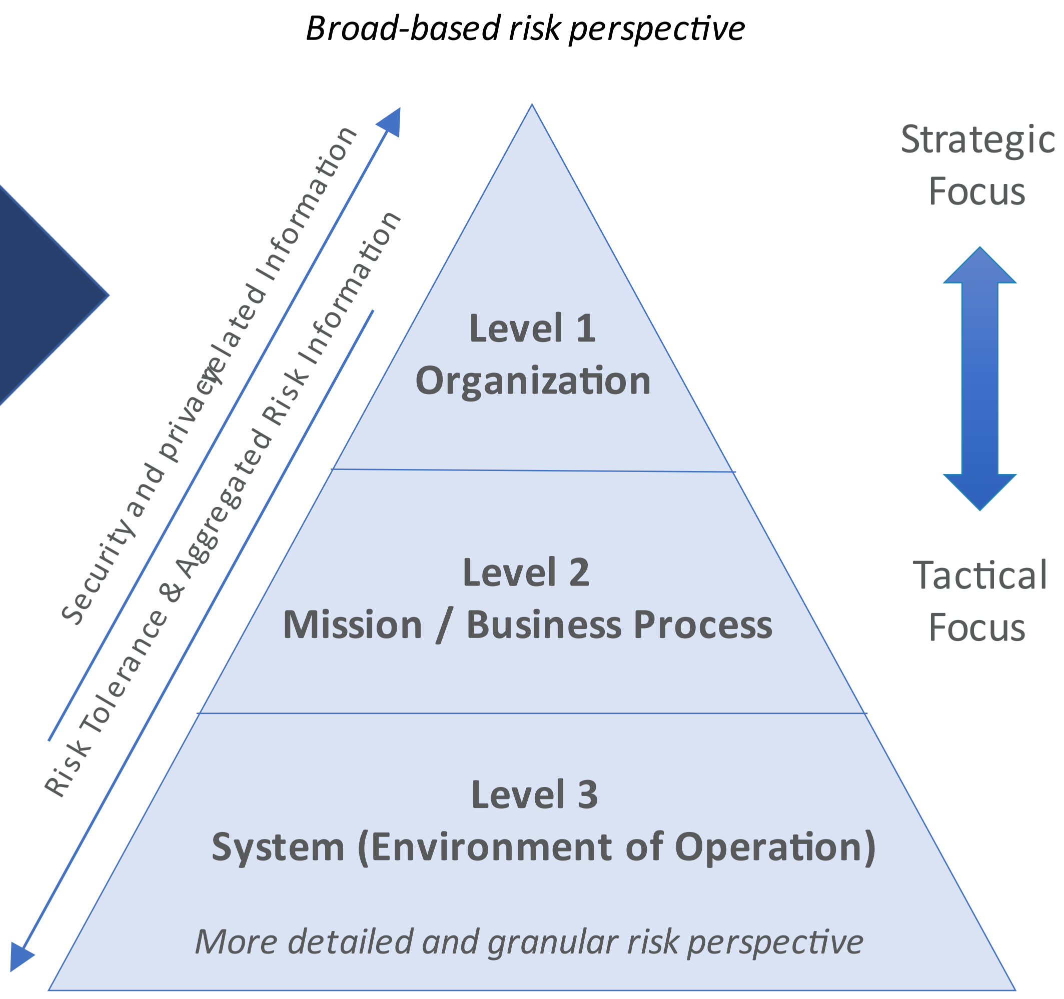
Likelihood

Organization-Wide Risk Assessment

Level 1: Support organization-wide strategies/policies/procedures

Level 2: Support determination of mission/business process protection, inform decisions on use of systems

Level 3: Focused on individual systems, can be conducted during each step of the RMF



Broad-based risk perspective
Security and privacy-related Information
Risk Tolerance & Aggregated Risk Information
Level 1
Organization
Level 2
Mission / Business Process
Level 3
System (Environment of Operation)
More detailed and granular risk perspective
Strategic Focus
Tactical Focus

Three Levels of Organization-Wide Risk Management

NIST SP 800-30, Revision 1: Organization

Chapter 1 - Introduction

Chapter 2 – Process overview and terminology

Chapter 3 – Risk assessment process activities

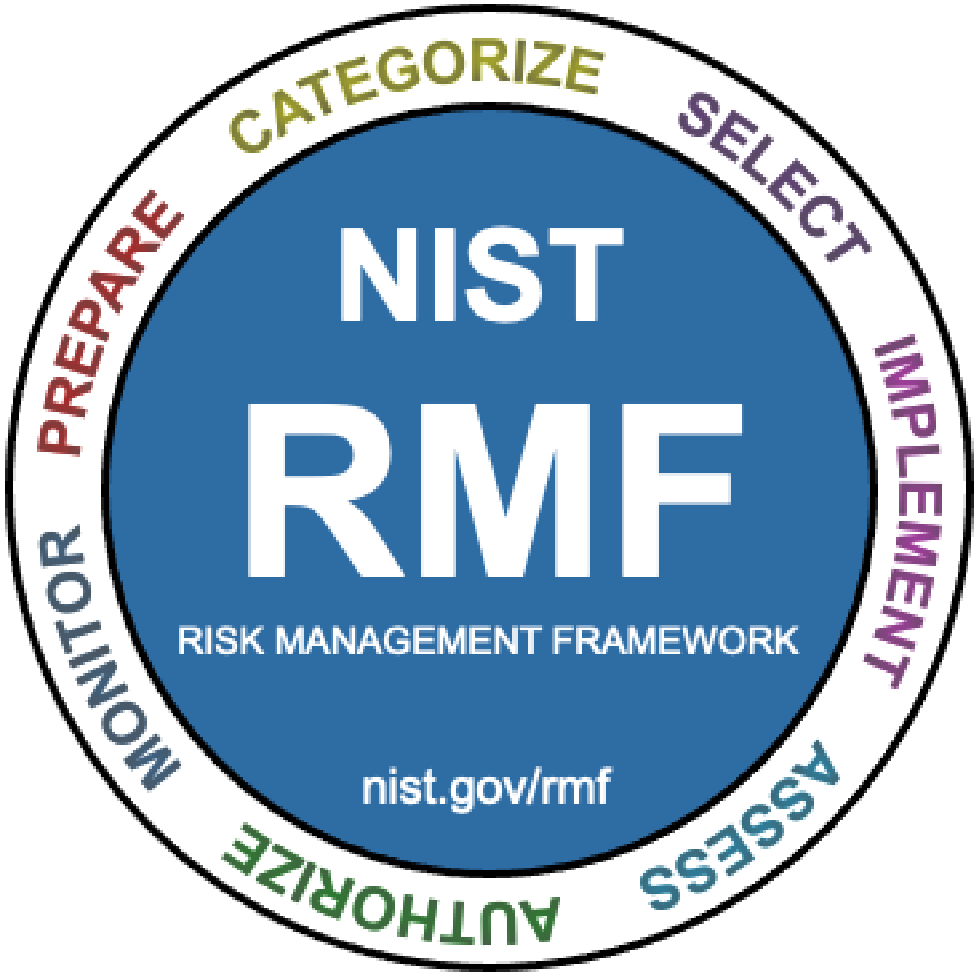
Supporting appendices, including:

- Threat sources and threat events
- Vulnerabilities and predisposing conditions
- Likelihood of threat occurrence
- Impact
- Risk and uncertainty
- Prioritization of risks

Risk Assessment Goal

- Determination of risk
  - What is the degree of potential harm?
  - How likely would such harm occur?

Risk Management Framework Steps



Essential activities to **prepare** the organization to manage security and privacy risks

Categorize the system and information processed, stored, and transmitted based on an impact analysis

Select the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)

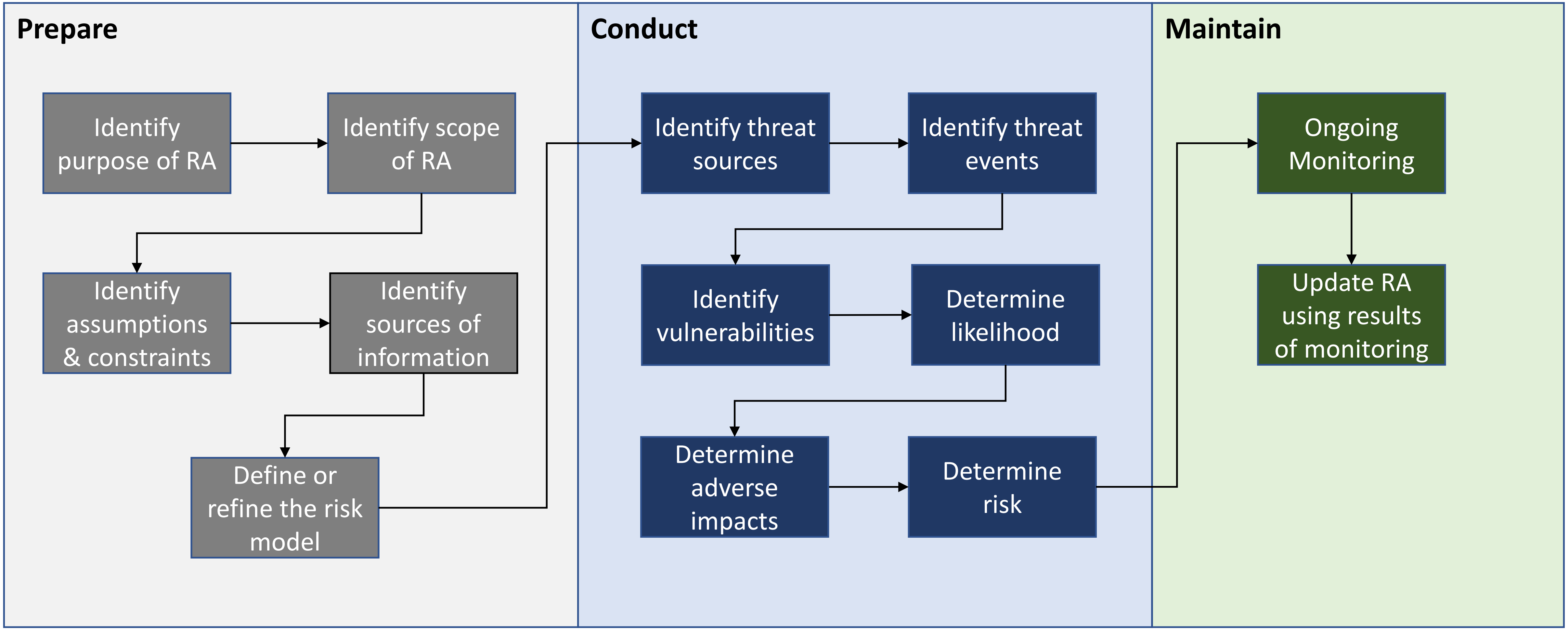
Implement the controls and document how controls are deployed

Assess to determine if the controls are in place, operating as intended, and producing the desired results

Senior official makes a risk-based decision to **authorize** the system (to operate)

Continuously **monitor** control implementation and risks to the system

Risk Assessment (RA) Process



Prepare

Identify purpose of RA

Identify scope of RA

Identify assumptions & constraints

Identify sources of information

Define or refine the risk model

Conduct

Identify threat sources

Identify threat events

Identify vulnerabilities

Determine likelihood

Determine adverse impacts

Determine risk

Maintain

Ongoing Monitoring

Update RA using results of monitoring

Assessment Approaches

Quantitative

- Based on numbers where proportionality of values is maintained in and out of the context of the assessment; higher degree of repeatability
- Qualitative-like subjective interpretations may still be involved
- Benefits may be outweighed by costs in time, effort, and tools

Qualitative

- Based on non-numerical levels such as low, moderate, and high
- Results typically easier to convey to decision makers
- Extra work required to ensure repeatability and reproducibility

Semi-Quantitative

- Based on scales or representative numbers whose values/proportions are not maintained in other contexts, e.g., 0-15, 16-35, 35-70, 71-85, 86-100)
- Expert judgment needed to assign values appropriately/reduce subjectivity

STAY IN TOUCH

CONTACT US

nist.gov/RMF

sec-cert@nist.gov

@NISTcyber