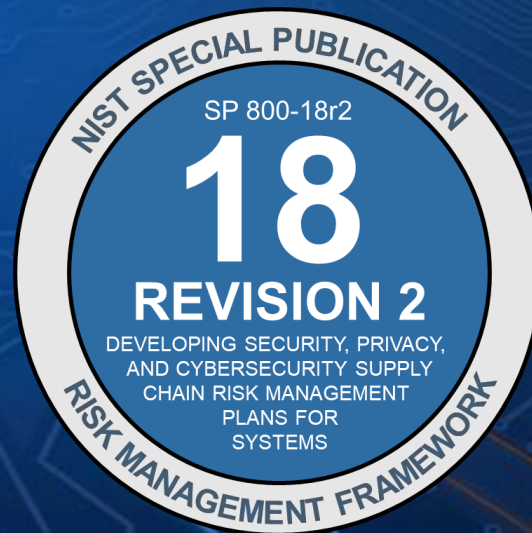


Special Publication (SP) 800-18r2: An Updated Approach to Developing System Plans

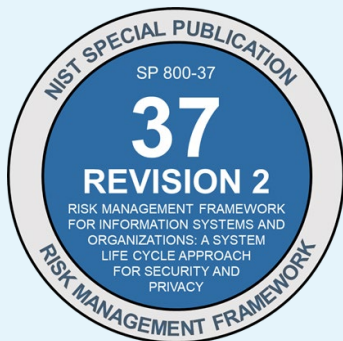
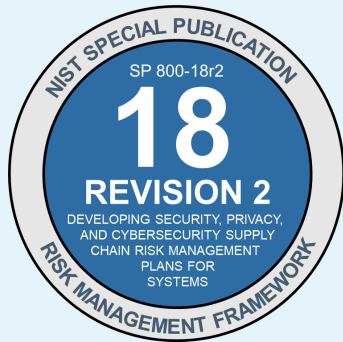


Presented by:
Jeremy Licata (NIST)
NIST Risk Management Framework (RMF) Team
Computer Security Division (CSD)

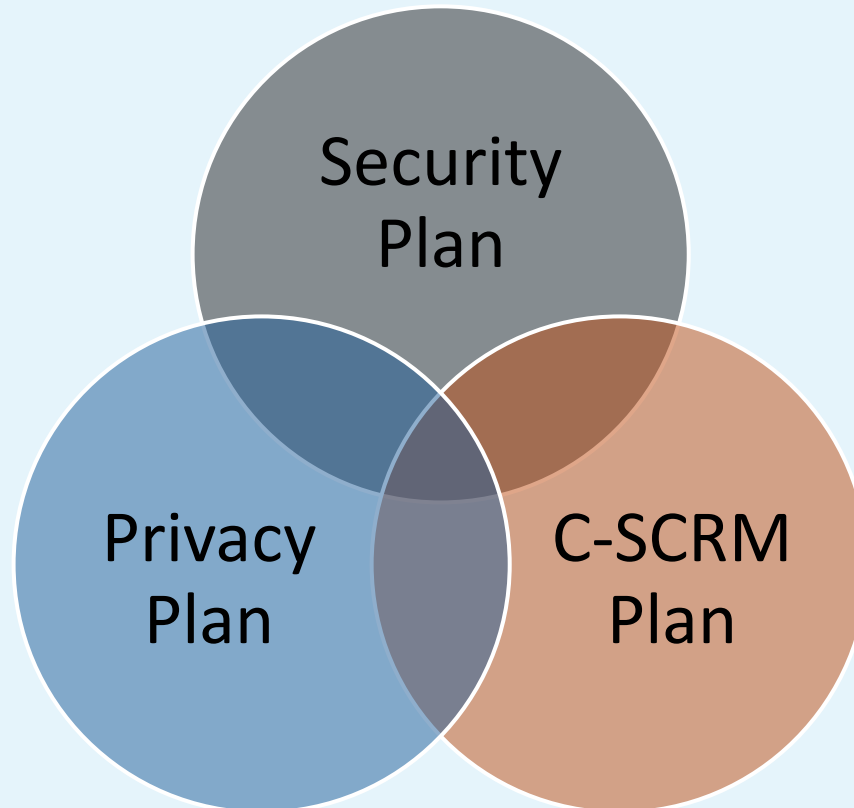
DISCLAIMER: any mention of entities, equipment, materials, or services throughout this talk is for information only; it does not imply recommendation or endorsement by NIST, nor is it intended to imply best available solution for any given purpose.

SP 800-18r2 Revision Objectives

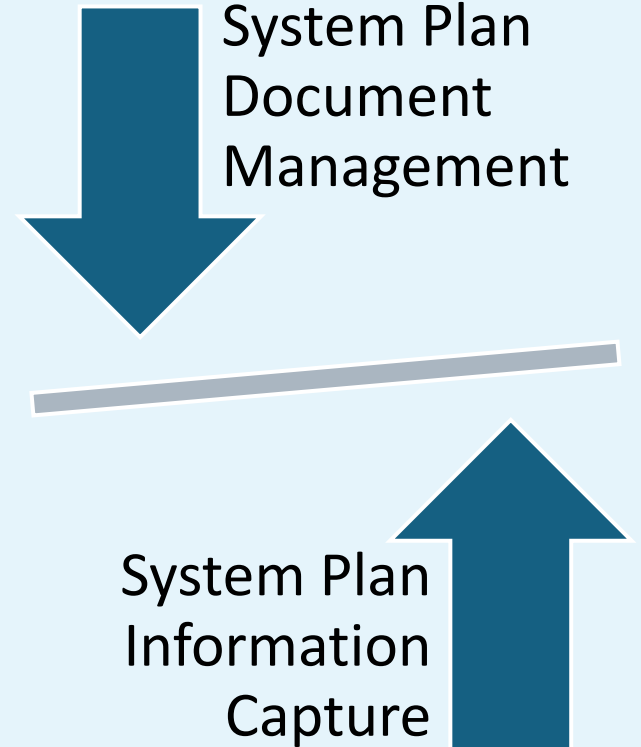
Align



System



Process



System Plan Descriptions



System Security Plan

- Describes system security requirements
- Includes controls to protect confidentiality, integrity, & availability
- Identifies system authorization boundary, purpose, security categorization, operational status & environment, and responsible individuals for security

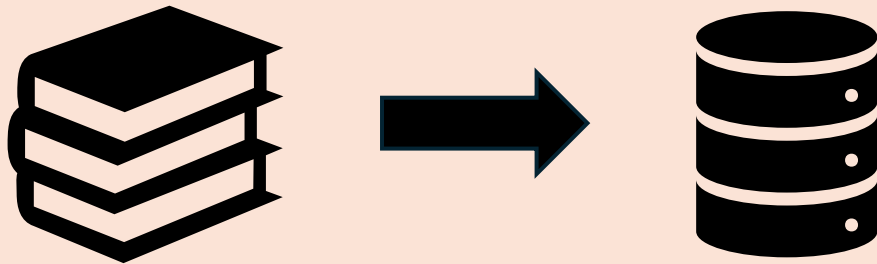
System Privacy Plan

- Describes system privacy risk management requirements
- Includes controls to address privacy engineering objectives predictability, manageability, & disassociability
- Aligns objectives with organization mission, risk tolerance, & privacy goals

C-SCRM Plan

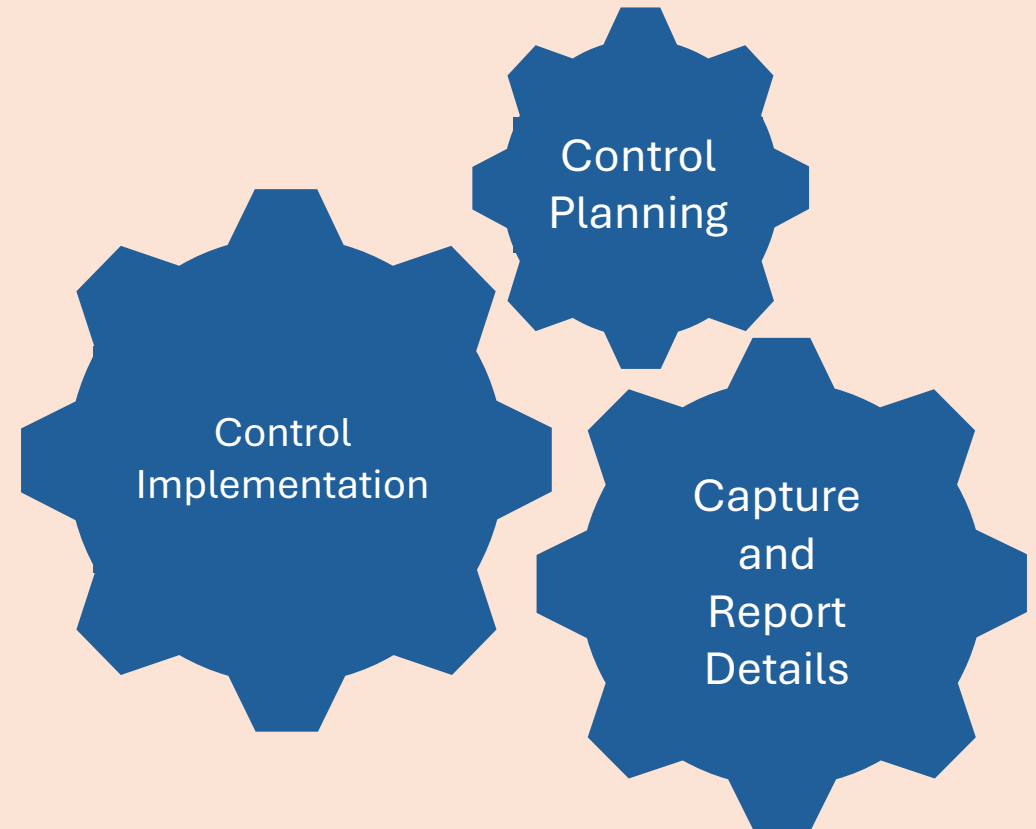
- Describes system's cybersecurity supply chain risk management requirements
- Includes controls to manage, implement, and monitor the supply chain
- Draws from organizational C-SCRM strategy to address risks at system level for components & services

Plan Elements



Shift focus from documenting sections to defining data elements for consistent content standards in data collection

Automate



System Plan Elements

- Each Plan Element is derived from RMF Tasks

A single RMF Task within a single RMF Step

System Plan Element	Source RMF Task(s)	System Plan Element Overview
System Name and Identifier	P-18, System Registration	Identify the system name and unique system identifier.

Multiple RMF Tasks within a single RMF Step

System Plan Element	Source RMF Task(s)	System Plan Element Overview
System Categorization	C-2, Security Categorization C-3, Security Categorization Review and Approval	Categorize information types by their impact level for each security objective (i.e., confidentiality, integrity, availability). The system security category reflects the high-water mark of the security category of all designated subsystems.

System Plan Elements

Multiple RMF Tasks across multiple RMF Steps

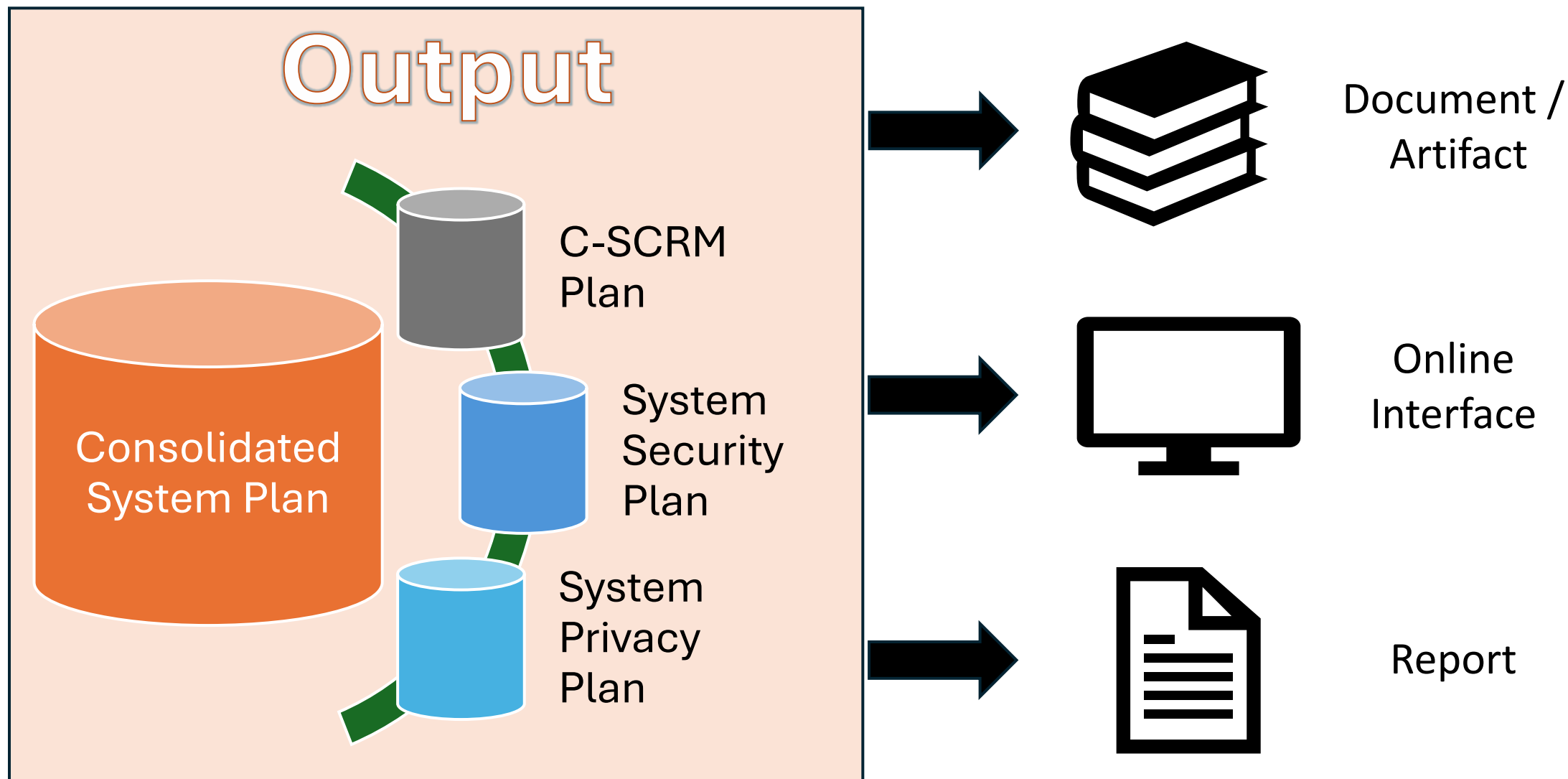
System Plan Element	Source RMF Task(s)	System Plan Element Overview
System Plan Change Records	I-2, Update Control Implementation Information A-5, Remediation Actions A-6, Plan of Action and Milestones R-3, Risk Response M-1, System and Environmental Changes M-3, Ongoing Risk Response M-4, Authorization Package Updates M-7, System Disposal	Provide a method for recording system plan changes over the course of the system life cycle.

- System Type v. System Information Type
- System Overview v. Authorization Boundary Description
 - Diagrams (subsystems, data flows, network connections, key internal boundaries)
- System Component Inventory
 - “hardware, firmware, software” ≠ subsystem
 - Automate (ITAM, GRC, SOAR, SIEM)
- Control Implementation Details
 - Achieving control outcomes: Who? What? Where? When? Why? How?
 - Provide reference to specific operational procedures
 - Prepared for system use and can inform assessment plan
- Control Implementation Status v. Control Assessment Status
- System Plan Approval v. System Authorization Decision

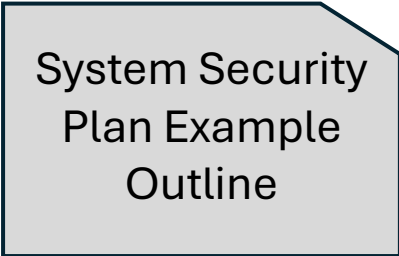
Combining Plan Elements

- System Status
 - Plan Approval
 - System Authorization Decision
 - System Operational Status
 - under development / operational / undergoing significant modification / disposal
- Control Implementation Details
 - Control implementation status
 - (planned / partially implemented / fully implemented)
 - Control assessment status
 - “satisfied” / “other than satisfied”

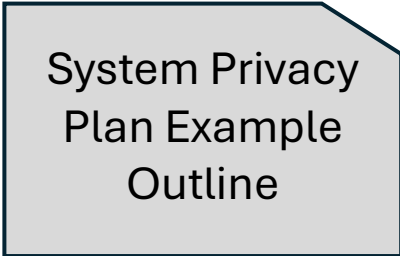
Sharing System Plans



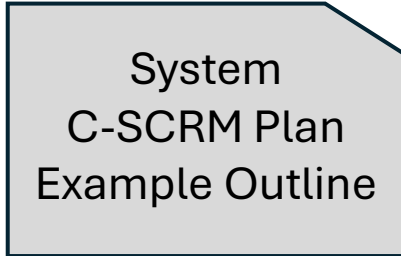
- Demonstrate how the plan elements may be combined



System Security
Plan Example
Outline

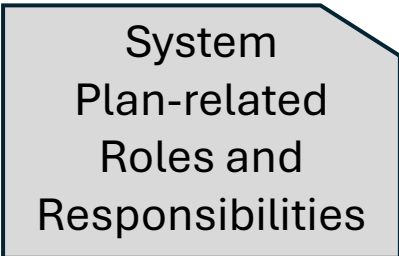


System Privacy
Plan Example
Outline



System
C-SCRM Plan
Example Outline

- Identify system plan-specific responsibilities for common system roles based on SP 800-37, Appendix D



System
Plan-related
Roles and
Responsibilities

Q&A and Open Discussion



**NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY**
U.S. DEPARTMENT OF COMMERCE



nist.gov/rmf



sec-cert@nist.gov



nist.gov/cyber