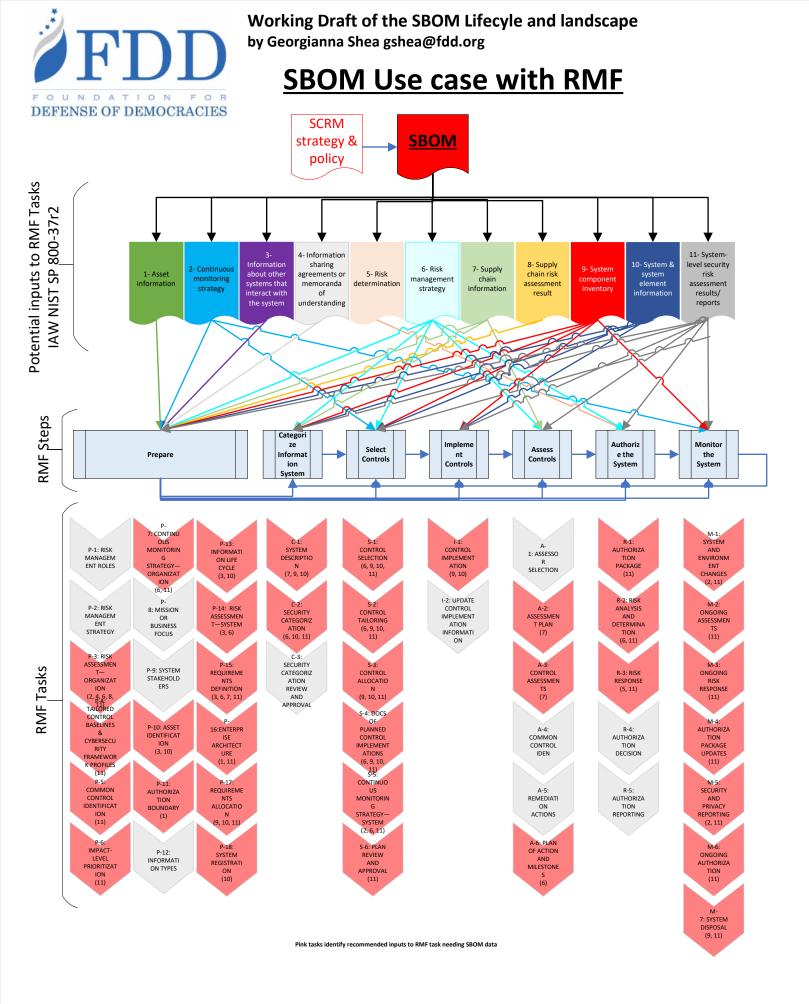


## Working Draft of the SBOM Lifecyle and landscape by Georgianna Shea gshea@fdd.org

**SBOM Risk** Integrate with SBOM **SBOM Mgmt** Validate SBOM **QC SBOMs** Requirements **Business Processes** Assessment - SBOM Analysis - Risk Mgmt - Contracted - Quality Control - Continuous (Use case next Regs meet? \*generation and Each Monitoring page) - SDLC - Integrity Check - SW Entity - Vulnerability - Asset Mgmt use including: - Tamper capabilities Resolution Exploitability Frequency, - SCRM detection - security - Contractor eXchange (VEX) - Procurement Depth, Known - Standardized posture, and Provision - Environment Unknowns, **Process** Naming - Foreign - Ingest Susceptibility - Vuln Mgmt Distribution and - Frequency, Ownership, --- directly (local VE)) Delivery, Access - Cyber Defense Depth, Known Control, or --- custom - Versioning Operations/SOCs Control, and **Consume SBOM** Unknowns,, and Influence - Configuration Accommodation scripts - Disposal Accommodation - Technical Debt - Store - Mapped of Mistakes. Mgmt of Mistakes enterprise -Export control -- ... dependencies Mgmt **Operationalizing SBOM Tooling** 





## Working Draft of the SBOM Lifecyle and landscape by Georgianna Shea gshea@fdd.org

Potential inputs to RMF Tasks IAW NIST SP 800-37r2

		ef NIST SP 800-37r2	Asset Information		Info on systems that interact with the system	Info sharing agreements	Risk determination	Risk management strategy	Supply chain information	Supply chain risk assessment result	System component inventory	System & system element & info	Security
sk#	Task -1 RISK MANAGEMENT ROLES	Inputs using SBOM data			system			strategy	information	result	inventory	& info	-
	-2 RISK MANAGEMENT												
	STRATEGY												
p.:	RISK ORGANIZATIO	Risk management strategy     system-level security and privacy risk assessment results											
	ASSESSMENT—ORGANIZATIO	system-level security and privacy risk assessment results     supply chain risk assessment results											
	l"	•information sharing agreements or memoranda of understanding		X		Х		Х		x			×
		•security and privacy information from continuous monitoring											
-	4 ORGANIZATIONALLY-	organization- and system-level risk assessment results											
bert	TAILORED CONTROL	organization- and system-level risk assessment results											
	BASELINES AND												×
	CYBERSECURITY												
-	FRAMEWORK PROFILES -5 COMMON CONTROL	organization- and system-level security and privacy risk		-									
P	IDENTIFICATION	organization- and system-level security and privacy risk assessment results											×
p.,	-6 IMPACT-LEVEL	organization- and system-level risk assessment results											×
	PRIORITIZATION												^
p.	7 CONTINUOUS MONITORING STRATEGY—ORGANIZATION	Risk management strategy     organization- and system-level risk assessment results						x					×
p.,	-8 MISSION OR BUSINESS FOCUS												
	9 SYSTEM STAKEHOLDERS												
P-1	ASSET IDENTIFICATION	system information     information about other systems that interact with the system			x							x	
P-1	11 AUTHORIZATION BOUNDARY		Х										
P-1	12 INFORMATION TYPES												
P-1	INFORMATION LIFE CYCLE	•information about other systems that interact with the system			x							х	
P-1	4 RISK ASSESSMENT—SYSTEM	system element information     information about other systems that interact with the system											
1	M31516—31315M	information about other systems that interact with the system     irisk management strategy			x			Х					
P-1	REQUIREMENTS DEFINITION	organization- and system-level risk assessment results											
		•information about other systems that interact with the system			×			x	x				х
		supply chain information     risk management strategy											
P-1	6 ENTERPRISE ARCHITECTURE	organization- and system-level risk assessment results	x										
		asset information	X										Х
P-1	7 REQUIREMENTS ALLOCATION	Organization- and system-level risk assessment results     wastem element information.									v	Ü	x
		system element information     system component inventory									Х	Х	×
	18 SYSTEM REGISTRATION	•system information										X	
	-1 SYSTEM DESCRIPTION	•system elements											
		system element information     system component inventory							×		x	x	
		system component inventory     system element supply chain information											
C-	-2 SECURITY CATEGORIZATION	•Risk management strategy											
		<ul> <li>organization- and system-level risk assessment results</li> </ul>						×				x	X
_	-3 SECURITY CATEGORIZATION	•system elements											
C-	REVIEW AND APPROVAL												
	1 CONTROL SELECTION	organization- and system-level risk assessment results											
		•system element information											
		•system component inventory						х			Х	х	×
		system elements     risk management strategy											
	-2 CONTROL TAILORING	organization- and system-level risk assessment results											
		•system element information											
		•system component inventory						×			X	х	×
		system elements     risk management strategy											
S-:	3 CONTROL ALLOCATION	organization- and system-level risk assessment results											
S-4		•system elements											
		•system element information									×	х	X
		•system component inventory											
	-4 DOCUMENTATION OF	organization- and system-level risk assessment results											
	PLANNED CONTROL	•system element information											
	IMPLEMENTATIONS	•system component inventory						×			Х	x	×
		system elements     risk management strategy											
S-	5 CONTINUOUS MONITORING	risk management strategy     risk management strategy											
	STRATEGY— SYSTEM	organizational continuous monitoring strategy		×				x					×
		organization- and system-level risk assessment results											
S-	- PLAN REVIEW AND APPROVAL	organization- and system-level risk assessment results											×
J.	-1 CONTROL IMPLEMENTATION	organization- and system-level risk assessment results											
	2 CONTROL IMPLEMENTATION	•system elements											
1-		•system element information									x	x	×
		•system component inventory											
	2 UPDATE CONTROL												
	IMPLEMENTATION												
	INFORMATION												
	-1 ASSESSOR SELECTION -2 ASSESSMENT PLAN	•supply chain information							X				
	-3 CONTROL ASSESSMENTS	supply chain information     supply chain information							X				
Α-	4 ASSESSMENT REPORTS												
	-5 REMEDIATION ACTIONS	Completed security and privacy assessment reports											×
٨	-6 PLAN OF ACTION AND	organization- and system-level risk assessment results     Undated security and privacy assessment reports		-									
24-	MILESTONES	Updated security and privacy assessment reports     organization- and system-level risk assessment results						х					×
		organizational risk management strategy											
	1 AUTHORIZATION PACKAGE	•security and privacy assessment reports											Х
R-	-2 RISK ANALYSIS AND DETERMINATION	risk management strategy     organization- and system-level risk assessment results						x					×
R-	-3 RISK RESPONSE	organization- and system-level risk assessment results     risk determination					75						
		organization- and system-level risk assessment results					Х						X
	4 AUTHORIZATION DECISION												
	-5 AUTHORIZATION REPORTING -1 SYSTEM AND ENVIRONMENT	Organizational continuous monitoring strategy											
ant-	CHANGES	Organizational continuous monitoring strategy security and privacy assessment reports		×									×
M-	-2 ONGOING ASSESSMENTS	Organizational continuous monitoring strategy and system level											
		continuous monitoring strategy		×									x
		•security and privacy assessment reports		^									^
No.	-3 ONGOING RISK RESPONS	organization- and system-level risk assessment results     Security and privacy assessment reports											
****	OTTOOTHS RESPONS	security and privacy assessment reports     system-level risk assessment results											Х
M-	4 AUTHORIZATION PACKAGE	Security and privacy assessment reports											
	UPDATES	•system-level risk assessment results											x
		Security and privacy assessment reports											^
M-	-5 SECURITY AND PRIVACY	organization- and system-level risk assessment results     Security and privacy assessment reports											
	REPORTING	•system-level risk assessment results		×									×
		organization- and system-level continuous monitoring strategy											
	6 ONGOING AUTHORIZATION	<ul> <li>organization- and system-level risk assessment results</li> </ul>		1			1	1	1				)

## DEFENSE OF DEMOCRACIES Potential inputs to RMF Tasks **IAW NIST SP 800-37r2** 4- Information Information 2- Continuous sharing 1- Asset about other agreements or information systems that strategy memoranda of interact with understanding the system 5,6,7,11 for RMF tasks Responsible P-1: RISK MANAGE MENT ROLES 1: ASSESS OR SELECTION PLANNED CONTROL IMPLEME NT. STBONS (GINT IND) GUIS MONITORI NG STRATEGY - SYSTEM CONTROL IMPLEME NTATION (9,20) SECURITY CATEGORIZ REVIEW AND APPROVAL S-6: PLAN REVIEW AND R-2: RISK ANALYSIS AND COMMON ATION (6, 11) REMEDIAT 1: ASSESSOR SELECTION UPDATE CONTROL RMF Tasks NTATION INFORMA TION A-5:

(2, 11)

## Working Draft of the SBOM Lifecyle and landscape by Georgianna Shea gshea@fdd.org

