



# **CYBER SECURITY RISK MANAGEMENT CONSTRUCT**

**CLEARED For Open Publication** 

Systems connected to DODIN

DOD **INFORMATION** 

**NETWORK** 

(DODIN)

Starting with lower environments in the Build Phase, through deployment to production environments in Onboarding Phase

Sep 23, 2025

Department of Defense OFFICE OF PREPUBLICATION AND SECURITY REVIEW

RMF STEP(S): Authorize

**PHASE 4: ONBOARD** 

NextGen CSSP risk

NextGen CSSP fully

artifacts

- or -

management performs risk

onboards system/capability

onboards system/capability

NextGen CSSP partially

- isolation, re-sensoring,

additional risk review

review, validates critical

controls and mandatory

This construct is intended to produce a culture, mindset and process that reimagines cyber risk management to be faster in keeping with the rate of change; more effectively assesses and conveys risk; and is less burdensome to cyber and acquisition professionals while ultimately providing operational combatant commanders with an accurate understanding of cyber risk to mission.

RMF STEP(S): Prepare, Categorize, Select

## PHASE 1: DESIGN



Capability need



Team formation includes: Mission Owner, System Owner/Program Manager, Engineers, CSSP

RMF STEP(S): Implement

### PHASE 2: BUILD (IOC)



Feed data to Information System Continuous Monitoring (ISCM) Alignment System



Submit system for evaluation

RMF STEP(S): **Assess** 

### PHASE 3: TEST (FOC)

Mission customization for Information Security Continuous Monitoring (ISCM)

Penetration testing (high risk systems)



Vulnerability remediation & assessment team

Automated test report dashboard analyst

### **PHASE 5: OPERATIONS**

RMF STEP(S): Monitor



System accepted for ISCM for continuous monitoring, enabling cATO



Data elements redirected to operational ISCM



Repeatable playbook to manage real-time risk monitoring via automated dashboards and alerts



High risk is elevated and addressed - CSSP watch officer makes decisions to disconnect



#### RESOURCE CYBERSECURITY AND SURVIVABILITY REQUIREMENTS ACROSS SYSTEM LIFECYCLE



Critical **Automation** 



Controls



**Continuous Monitoring DevSecOps** (CONMON), control, and ATO









& Inheritance











Cybersecurity Assessments

STRATEGIC TENETS

Survivability