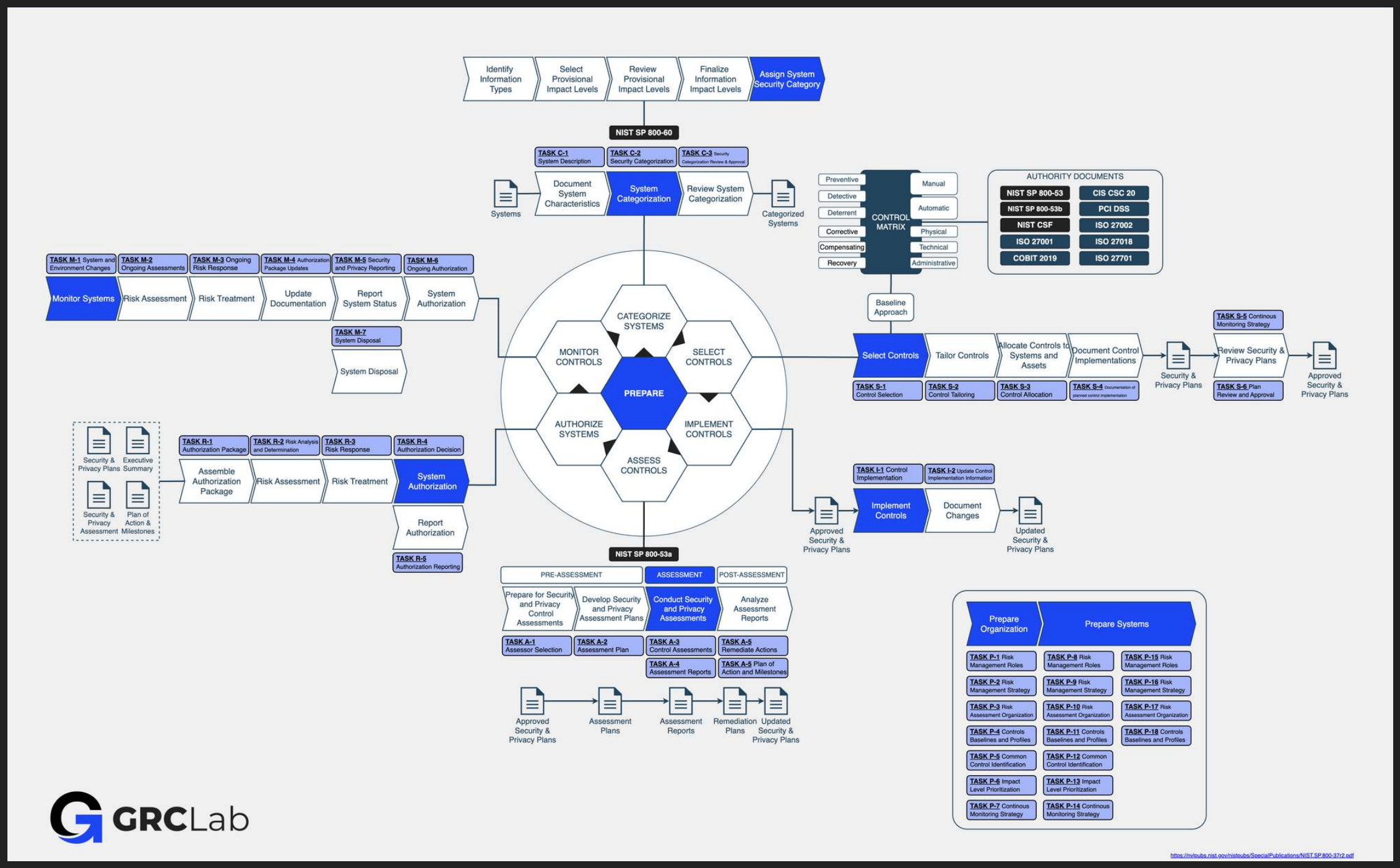
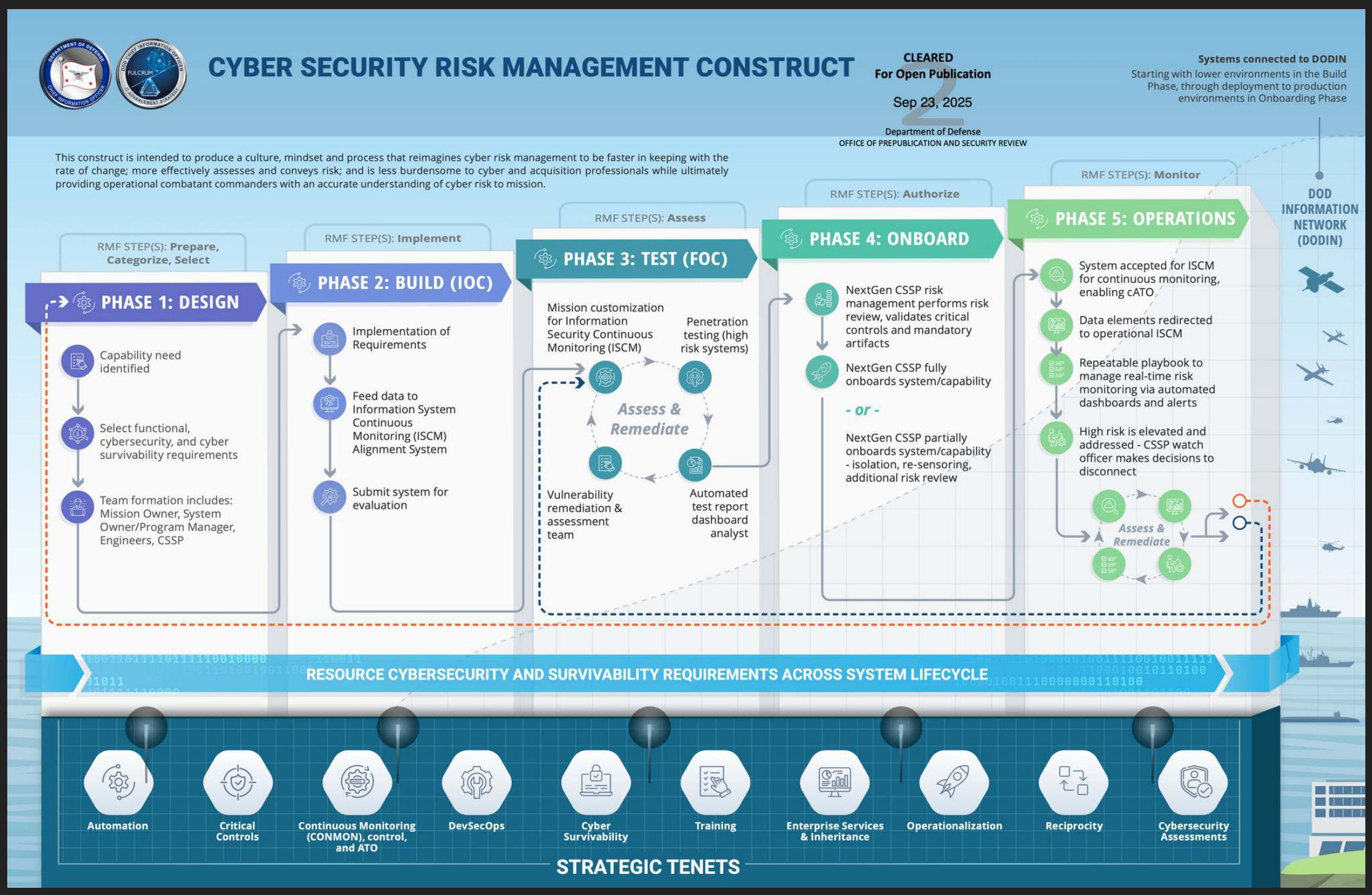

Identify Information Types
Select Provisional Impact Levels
Review Provisional Impact Levels
Finalize Information Impact Levels
Assign System Security Category
NIST SP 800-60
TASK C-1 System Description
TASK C-2 Security Categorization
TASK C-3 Security Categorization Review & Approval
Systems
Document System Characteristics
System Categorization
Review System Categorization
Categorized Systems
Preventive
Detective
Deterrent
Corrective
Compensating
Recovery
CONTROL MATRIX
Manual
Automatic
Physical
Technical
Administrative
AUTHORITY DOCUMENTS
NIST SP 800-53
CIS CSC 20
NIST SP 800-53b
PCI DSS
NIST CSF
ISO 27002
ISO 27001
ISO 27018
COBIT 2019
ISO 27701
TASK M-1 System and Environment Changes
TASK M-2 Ongoing Assessments
TASK M-3 Ongoing Risk Response
TASK M-4 Authorization Package Updates
TASK M-5 Security and Privacy Reporting
TASK M-6 Ongoing Authorization
Monitor Systems
Risk Assessment
Risk Treatment
Update Documentation
Report System Status
System Authorization
TASK M-7 System Disposal
System Disposal
CATEGORIZE SYSTEMS
MONITOR CONTROLS
SELECT CONTROLS
PREPARE
AUTHORIZE SYSTEMS
IMPLEMENT CONTROLS
ASSESS CONTROLS
Baseline Approach
Select Controls
Tailor Controls
Allocate Controls to Systems and Assets
Document Control Implementations
TASK S-1 Control Selection
TASK S-2 Control Tailoring
TASK S-3 Control Allocation
TASK S-4 Documentation of planned control implementation
Security & Privacy Plans
TASK S-5 Continous Monitoring Strategy
Review Security & Privacy Plans
TASK S-6 Plan Review and Approval
Approved Security & Privacy Plans
Security & Privacy Plans
Executive Summary
Security & Privacy Assessment
Plan of Action & Milestones
TASK R-1 Authorization Package
TASK R-2 Risk Analysis and Determination
TASK R-3 Risk Response
TASK R-4 Authorization Decision
Assemble Authorization Package
Risk Assessment
Risk Treatment
System Authorization
Report Authorization
TASK R-5 Authorization Reporting
TASK I-1 Control Implementation
TASK I-2 Update Control Implementation Information
Approved Security & Privacy Plans
Implement Controls
Document Changes
Updated Security & Privacy Plans
NIST SP 800-53a
PRE-ASSESSMENT
ASSESSMENT
POST-ASSESSMENT
Prepare for Security and Privacy Control Assessments
Develop Security and Privacy Assessment Plans
Conduct Security and Privacy Assessments
Analyze Assessment Reports
TASK A-1 Assessor Selection
TASK A-2 Assessment Plan
TASK A-3 Control Assessments
TASK A-4 Assessment Reports
TASK A-5 Remediate Actions
TASK A-5 Plan of Action and Milestones
Approved Security & Privacy Plans
Assessment Plans
Assessment Reports
Remediation Plans
Updated Security & Privacy Plans
Prepare Organization
Prepare Systems
TASK P-1 Risk Management Roles
TASK P-2 Risk Management Strategy
TASK P-3 Risk Assessment Organization
TASK P-4 Controls Baselines and Profiles
TASK P-5 Common Control Identification
TASK P-6 Impact Level Prioritization
TASK P-7 Continous Monitoring Strategy
TASK P-8 Risk Management Roles
TASK P-9 Risk Management Strategy
TASK P-10 Risk Assessment Organization
TASK P-11 Controls Baselines and Profiles
TASK P-12 Common Control Identification
TASK P-13 Impact Level Prioritization
TASK P-14 Continous Monitoring Strategy
TASK P-15 Risk Management Roles
TASK P-16 Risk Management Strategy
TASK P-17 Risk Assessment Organization
TASK P-18 Controls Baselines and Profiles
GRCLab
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf


CYBER SECURITY RISK MANAGEMENT CONSTRUCT
CLEARED
For Open Publication
Sep 23, 2025
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW
Systems connected to DODIN
Starting with lower environments in the Build Phase, through deployment to production environments in Onboarding Phase
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 identified
Select functional, cybersecurity, and cyber survivability requirements
Team formation includes: Mission Owner, System Owner/Program Manager, Engineers, CSSP
RMF STEP(S): Implement
PHASE 2: BUILD (IOC)
Implementation of Requirements
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)
Assess & Remediate
Vulnerability remediation & assessment team
Automated test report dashboard analyst
RMF STEP(S): Authorize
PHASE 4: ONBOARD
NextGen CSSP risk management performs risk review, validates critical controls and mandatory artifacts
NextGen CSSP fully onboards system/capability
- or -
NextGen CSSP partially onboards system/capability - isolation, re-sensoring, additional risk review
RMF STEP(S): Monitor
PHASE 5: OPERATIONS
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
Assess & Remediate
DOD INFORMATION NETWORK (DODIN)
RESOURCE CYBERSECURITY AND SURVIVABILITY REQUIREMENTS ACROSS SYSTEM LIFECYCLE
Automation
Critical Controls
Continuous Monitoring (CONMON), control, and ATO
DevSecOps
Cyber Survivability
Training
Enterprise Services & Inheritance
Operationalization
Reciprocity
Cybersecurity Assessments
STRATEGIC TENETS