Security Controls Derivation

Sarah Storms

Lockheed Martin – Centralized Super Computer Facility

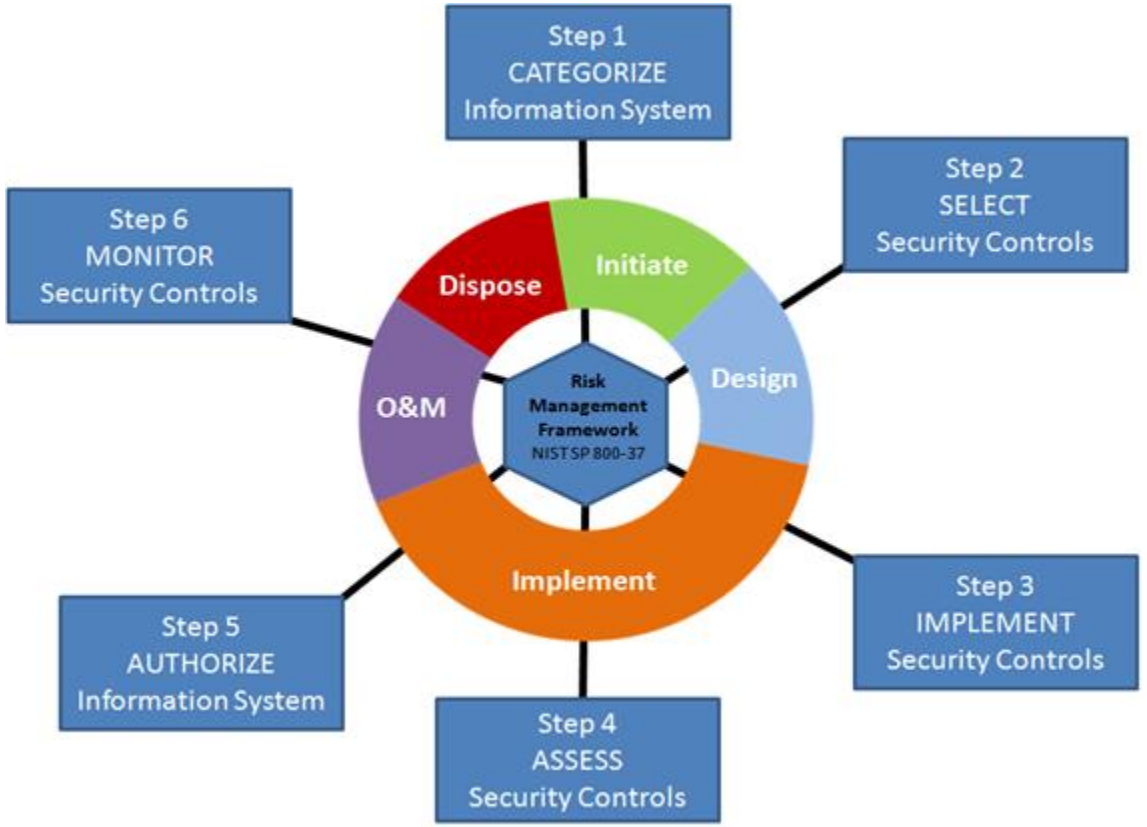
Outline

- Intelligence Community Directive ICD 503
- Risk Management Framework
- NIST SP 800-53
- CNSSI 1253
- IASD
- Security Control Overlays

Intelligence Community Directive (ICD) 503

- Released by Office of the Director of National Intelligence 15 September 2008
- Establishes Intelligence Community (IC) policy for information technology systems security risk management, certification and accreditation
- Rescinded and replaced the Director of Central Intelligence Directive (DCID) 6/3 Policy
- Directive to use “more holistic and strategic process for the risk management of IT systems”
  - Risk Management Framework

Risk Management Framework



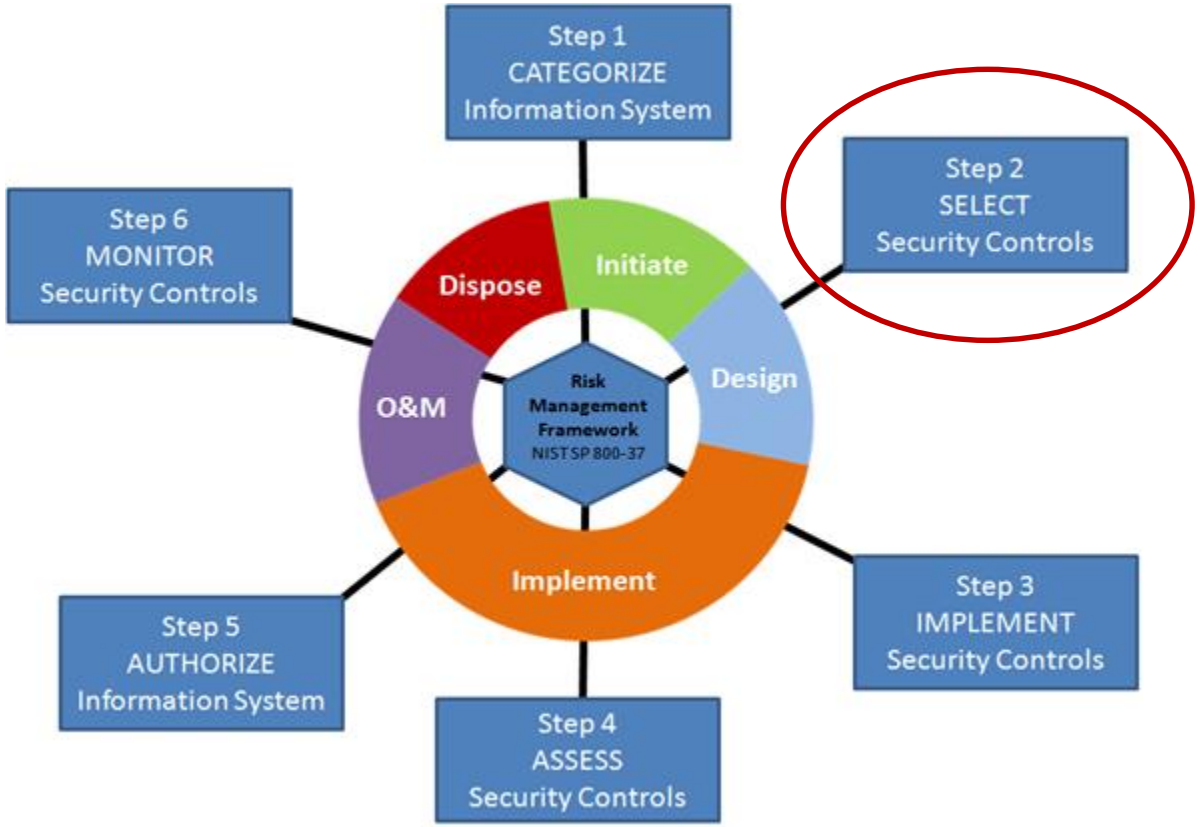
Risk Management Framework Steps

- Step 1 – Categorize Information System
  - Confidentiality
  - Integrity
  - Availability
- Step 2 - Select Security Controls
  - Common Controls
  - Hybrid Controls
  - System Controls
  - Critical Controls
  - Compensating Controls

Risk Management Framework Steps (cont.)

- Step 3 – Implement Security Controls
- Step 4 – Assess Security Controls
- Step 5 – Authorize Information System
- Step 6 – Monitor Security Controls

Risk Management Framework



Intelligence Community Standard 503-2

- Released in May 2010
- Designates CNSSI 1253 as standard for categorizing ISs and selecting baseline security controls for National Security Systems
- Designates NIST SP 800-53 as source for security and programmatic controls for NSS

Committee for National Security Systems Instruction (CNSSI) 1253

- “Security Categorization and Control Selection for National Security Systems (NSS)”
- Comprehensive set of security controls and enhancements that may be applied to any NSS
- Tailoring guidance
- Formatted and aligned with section numbering scheme used in NIST SP 800-53
- Companion document to NIST SP 800-53

National Institute Of Standards and Technology (NIST) Special Publication (SP) 800-53

- "Recommended Security Controls for Federal Information Systems and Organizations"
- Purpose of NIST SP 800-53
  - Facilitate consistent, comparable, and repeatable approach for selecting security controls
  - Provide recommendation for minimum security controls in accordance with FIPS 199
  - Provide stable, flexible catalog of security controls
  - Create foundation for development and assessment methods
  - Improve communication by providing common lexicon

Information Assurance Standards Document (IASD)

- Specific baseline set of control's deemed applicable to CSCF agency's NSS
- Employed CNSSI 1253 Table D-1 to determine baseline controls deemed applicable and assigned values to establish organizationally-specific parameters
- Does not replace CNSSI 1253 or NIST SP 800-53

Security Control Overlays

- Provide NSS community-level structured tailoring of security controls specific to a particular application of technology, protection level
- Examples include
  - Cross Domain Solution
    - Transfer*
    - Access
    - Multi-Level*
  - Intelligence*
  - Space
  - PII

* Applied to CSCF systems