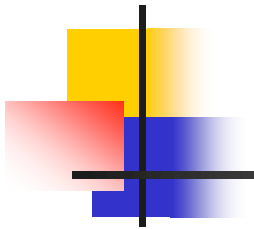


CSE 543
Information Assurance and Security

IA Certification & Accreditation (C&A)

Professor Stephen S. Yau

What Is IA C&A?

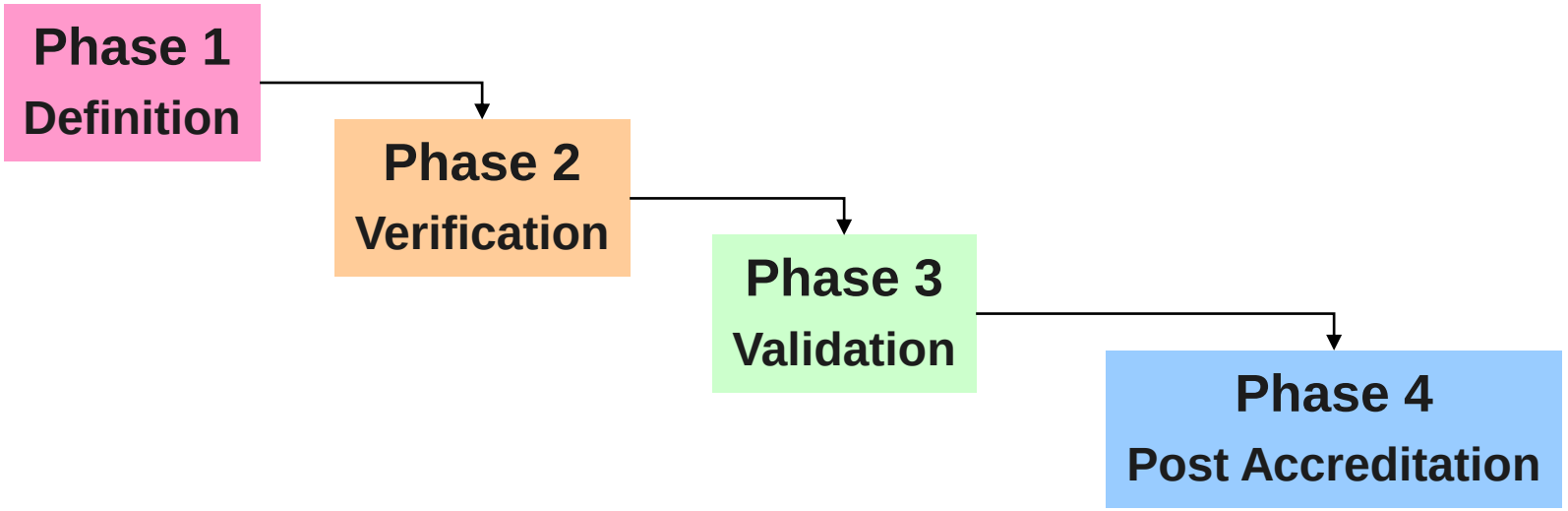
- IA Certification
  - ***Comprehensive evaluation*** of technical and non-technical ***security features*** of IT system and other safeguards made in support of accreditation process to establish the extent that a particular design and implementation ***meets specified security requirements***
- IA Accreditation
  - ***Formal declaration*** by the ***Designated Approving Authority (DAA)*** that an ***IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk***

Two Key Players

- ***Designated Approving Authority (DAA):***
  - Official with authority to ***formally assume responsibility for operating a system or network at an acceptable level of risk***
- ***Certification Authority (CA):***
  - Official responsible for ***performing comprehensive evaluation and issuing certificate for a particular design and implementation that meet specified security requirements***
- Critical to make sure **DAA and CA *independent of implementation team*** to ensure fairness

Certification and Accreditation (C&A) Process

- ***DoD Information Technology Security Certification and Accreditation Process (DITSCAP):***
  - Tailorable, scalable, predictable, understandable, relevant, effective, evolvable, repeatable, responsive



C&A Process (cont.)

- ***Repeatable process*** that ***addresses security threats and vulnerabilities*** with appropriate combination of security measures
- Covers ***entire system's life-cycle*** -- from creation to maintenance until system decommission

Phase 1: Definition

- Define ***mission, system functions, and requirements (especially security)***
- Define ***information category and classification***
- Prepare ***system architecture description***
- Identify ***principal C&A roles & responsibilities***
- Draft ***overall C&A document***
  - ***System Security Authorization Agreement (SSAA)***
- Agreement among all principals on methods for implementing security requirements
  - ***Approve SSAA***

System Security Authorization Agreement (SSAA)

- A formal agreement among DAA, CA, IT system user representative, and program manager.
- Used throughout entire ***DITSCAP*** to guide actions, document decisions, specify Information Technology Security (ITSEC) requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational system security
- Return ***DITSCAP*** to the initial phase for re-design.

Phase 2: Verification

- ***System architecture analysis***
- ***Software design analysis***
- ***Network connection rule compliance***
- ***Integrity analysis***
- ***Life cycle management analysis***
- Establishment of ***security requirement validation procedures***
- ***Vulnerability evaluation***

Phase 3: Validation

- ***Security test and evaluation***
- ***Penetration testing*** (exploitation, insider/outsider)
- ***Compliance evaluation*** (requirements, integration)
- ***System management analysis***
- ***Contingency plan evaluation***
- ***Site accreditation survey***
- ***Risk management review***
- ***Develop certification report and recommendation for accreditation***
- ***Generate declaration of accreditation***
- ***Exceptions:*** Under certain situations, some policies may be waived to continue operation

Phase 4: Post Accreditation

- ***Review configuration and security management***
- Follow system changes
  - Change requests to a system must be ***reviewed and approved by DAA and CA***
  - Determine if a system with the requested changes will continue to support ***organization's mission and architecture***
  - If change requests are approved, they invalidate the SSAA requirement, and ***DITSCAP*** must go back to Phase I; otherwise, continue to operate as it is

Phase 4: Post Accreditation (cont.)

- Conduct ***risk management review***
  - Assess if risk to system is being maintained at an acceptable level
- Conduct ***compliance validation for any changes of configuration***
- ***Maintain documentation***
- ***Monitor compliance***

Reference

- DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Available at:

  http://www.sans.org/reading_room/whitepapers/country/ditscap-dods-answer-secure-systems_669