From Chaos to Clarity: Embedding Security into the SDLC

Felicia Nicastro

Security Testing Services Practice

SQS USA

Celebrating a decade of guiding security professionals.

SECURE360 conference

Session Description

- This session will focus on the security testing requirements which have been derived from the NIST 800-64 Standard. It will also tie in requirements from the OWASP Testing Guide v4 and Industry Best Practices.
- Through each of the phases of the SDLC, the control gates, entry and exit criteria, as well as the short and long term goals for implementing a mature security testing process as part of the SDLC will be included.
- The purpose is to provide an overall security testing process an organization can implement that focuses on conducting security testing through the SDLC.
- This trend has been surfacing over the past few years and is also referred to as embedding security testing into the SDLC or also known as the “Shift Left” approach.

Key Learning Points

- Learn how to integrate security testing into the SDLC
- Leverage NIST 800-64 in order to ensure thorough security testing
- Learn what tests need to be performed during the SDLC

Chaos!

- If only we could get developers and QA teams to develop, test and implement secure code!
- How do we accomplish this?

Clarity!

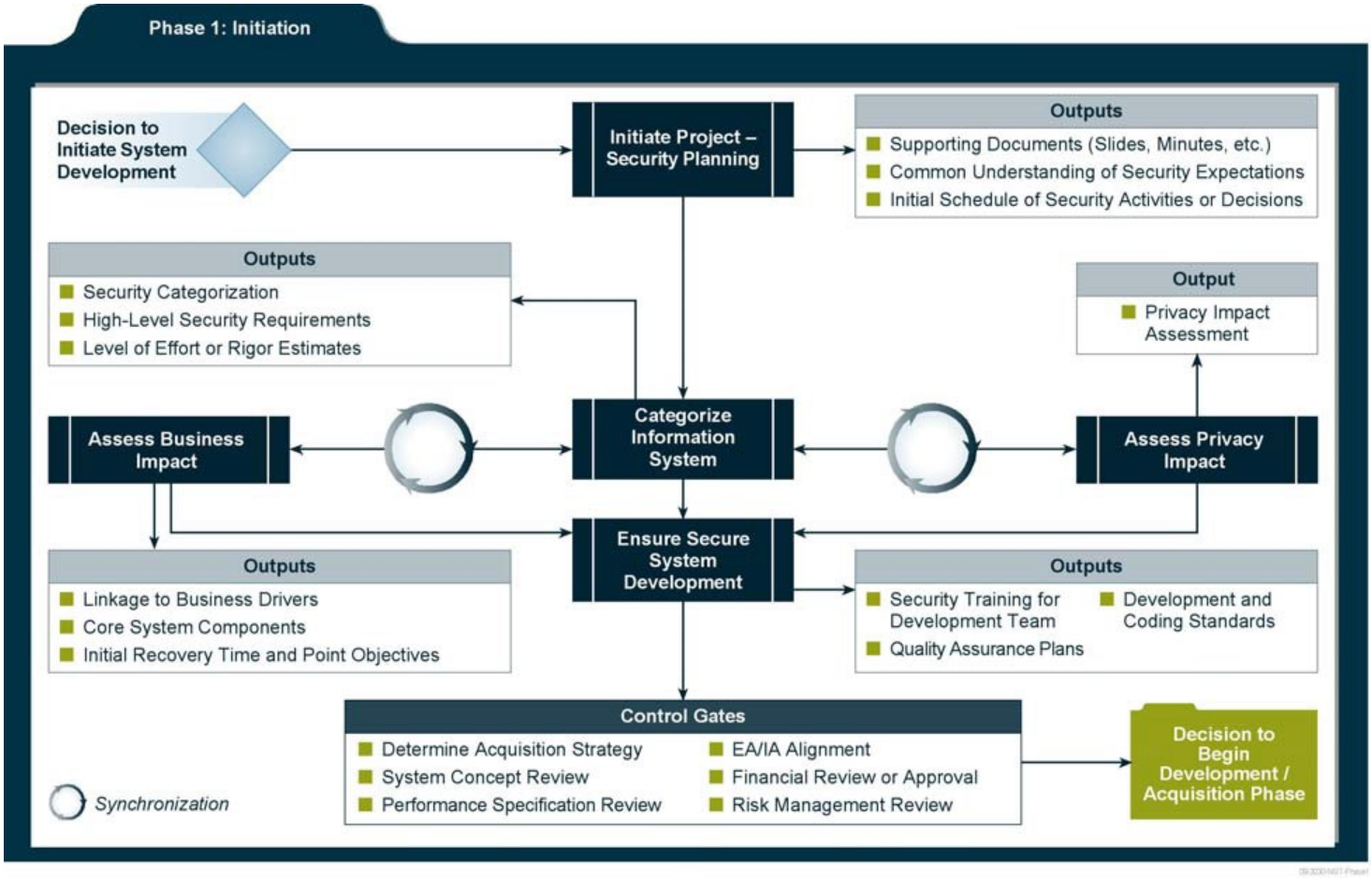
- Why embedding security testing into the Software Development Lifecycle of course!!
- So…how do we do that?

Let’s count the ways…

- NIST 800-64 is a great start
- OWASP v4 has guidance as well
- Education of developers, QA teams
- Security testing teams working alongside developers

- For example….

SDLC Phase 1: Initiation



Initiate Security Planning

- Key Security Roles
- Sources of Security Requirements
- Understanding between stakeholders
- Document initial security milestones
- Outline of security requirements and expectations documented

Categorize the Information System

- Establishes foundation for security standardization
- Three levels (low, moderate, or high) of potential impact should there be a breach of security (a loss of confidentiality, integrity, or availability)
- Assists in defining appropriate security controls

Assess Business Impact

- Expected outputs are to identify:
  - lines of business supported and how they will be impacted
  - core system components
  - length of time the system can be down before the business is impacted
  - business tolerance for loss of data

Assess Privacy Impact

- Is the system going to transmit, store, or create information that may be considered Private?
- Defined during Security Categorization
- Output: Privacy Impact Assessment

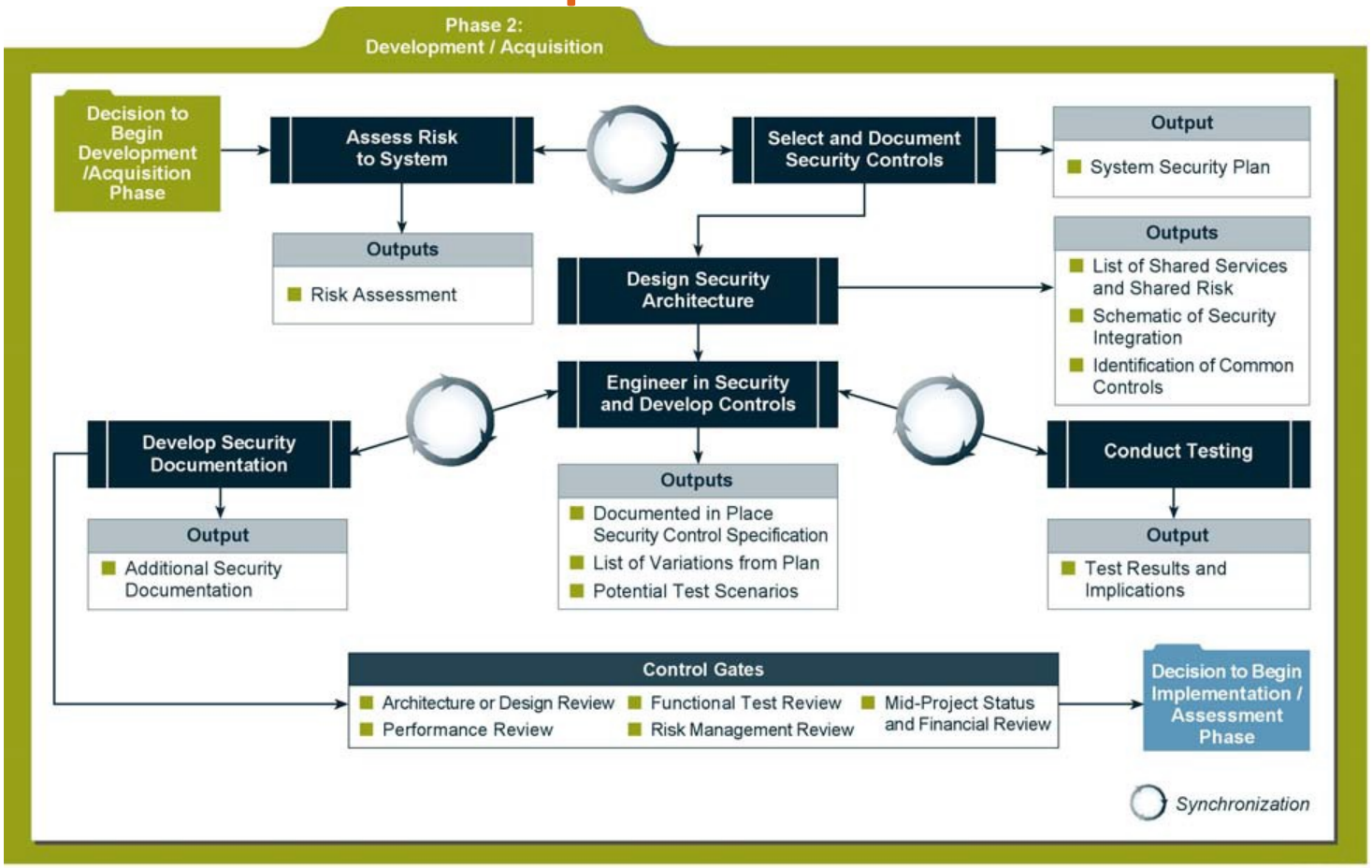
Ensure Use of Secure Information System Development Processes

- Secure Concept of Operations (CONOPS) for Development
- Standards and Processes
- Security Training for Development Team
- Quality Management
- Secure Environment
- Secure Code Practices and Repositories

- Phase 1 sets the foundation on which the remainder of the SDLC is built upon
- Like a house without a solid foundation it will falter and fail

- Now is when the fun begins…

SDLC Phase 2: Development / Acquisition



Assess Risk to System

- NIST 800-30 – Guidance for Risk Assessments
- Purpose is to:
  - evaluate current knowledge of the system's design
  - stated requirements, and
  - minimal security requirements from the security categorization process
- Results should show specified security controls provide protections or highlight areas where further planning is needed

Select and Document Security Controls

- Made up of 3 activities:
  - the selection of baseline security controls
  - the application of security control tailoring guidance to adjust the initial security control baseline
  - supplementation of the tailored baseline with additional controls based on an assessment of risk and local conditions

Design Security Architecture

- Minimal security requirements as well as requirements and constraints determined early in the process should provide the architects with a set of assumptions and constraints to build around
- Can provide the most value in lowering the total cost of ownership by planning the systems core components in a secure way
- Outputs include:
  - Schematic of security integration providing details on where, within the system, security is implemented and shared.
  - Security architectures should be graphically depicted and detailed to the extent the reader can see where the core security controls are applied and how.
  - Identification of common controls used by the system

Engineer in Security and Develop Controls

- Security controls are implemented
- Applying security controls in development should be considered carefully and planned logically
- Intent is to integrate the controls so challenges with system performance are known early
- Output includes:
  - Implemented controls with documented specification for inclusion into the security plan
  - List of security control variations resulting from development decisions and tradeoffs
  - Potential assessment scenarios to test known vulnerabilities or limitations

Develop Security Documentation

- System Security Plan is most important
- Others include:
  - Configuration management plan
  - Contingency plan (including a BIA)
  - Continuous monitoring plan
  - Security awareness, training and education plan
  - Incident response plan
  - Privacy impact assessment (PIA)

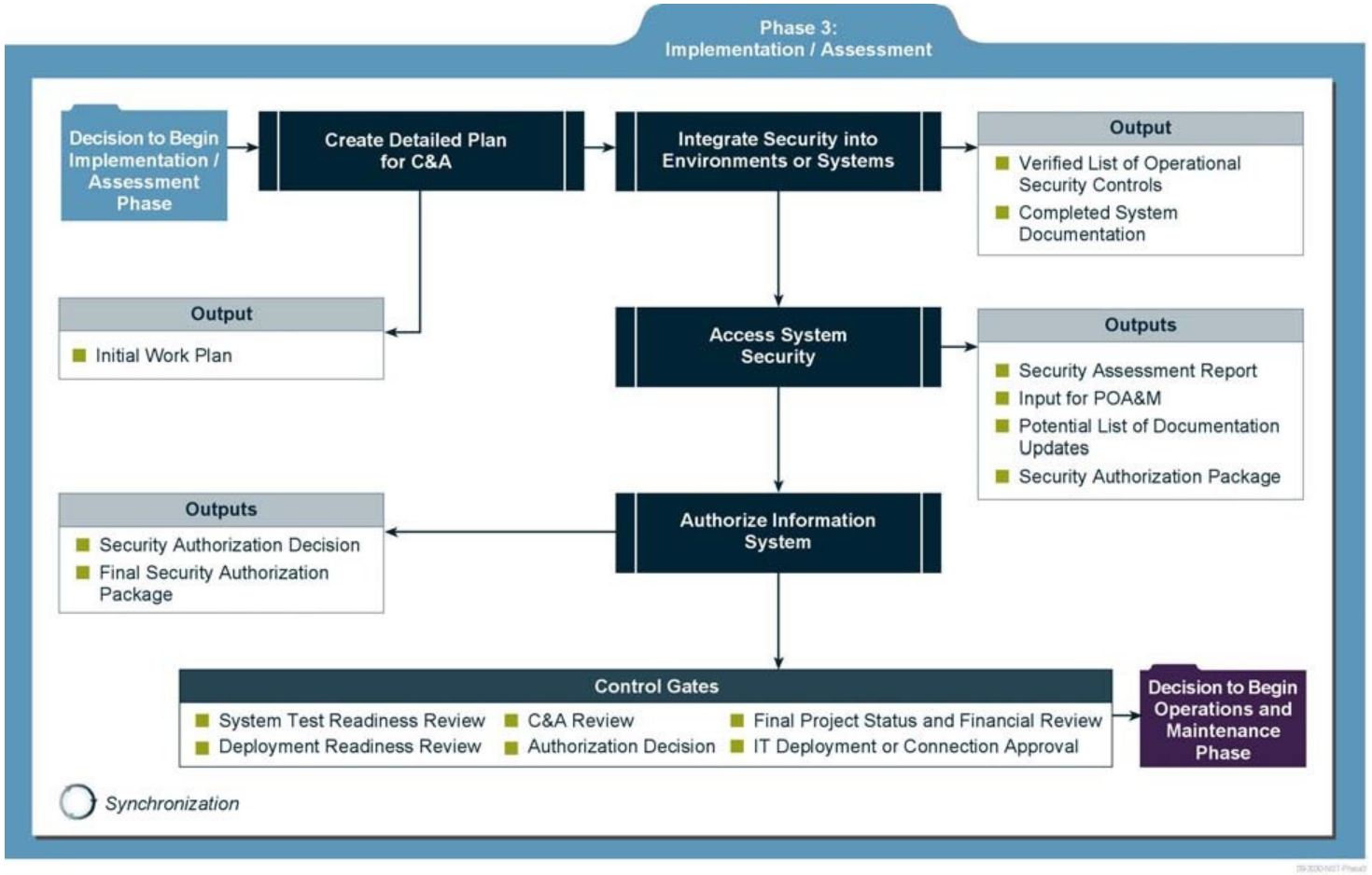
Conduct Testing (Developmental, Functional, and Security)

- The process focuses on:
  - Specificity - testing must be scoped to test the relevant security requirement as it is intended for use in its environment
  - Repeatability - testing must be capable of the execution of a series of tests against an information system more than once (or against similar systems in parallel) and yield similar results each time
  - Iteration - each system will be required to execute functional tests in whole or in part a number of successive times in order to achieve an acceptable level of compliance with the requirements of the system
- Functional testing should be automated to the degree possible, and the test cases will be published, in detail, to ensure that the test process is repeatable and iterative

- Now that the development and testing is completed, we move on to the next phase…

- Plus, look at all the security functions we've already performed!

SDLC Phase 3: Implementation / Assessment



Create a Detailed Plan for C&A

- To ensure proper testing and reduce the likelihood of scope creep, the security accreditation boundary should be clearly delineated. This forms the basis for the test plan to be created and approved
- Output - Initial Work Plan: A planning document that identifies key players, project constraints, core components, scope of testing, and level of expected rigor. The certification package should be close to completion, and any initial agency-specified conformance reviews initiated

Integrate Security into Established Environments or Systems

- Integration and acceptance testing occur after information system delivery and installation
- Security control settings are enabled in accordance with manufacturers' instructions, available security implementation guidance, and documented security specification

Assess System Security

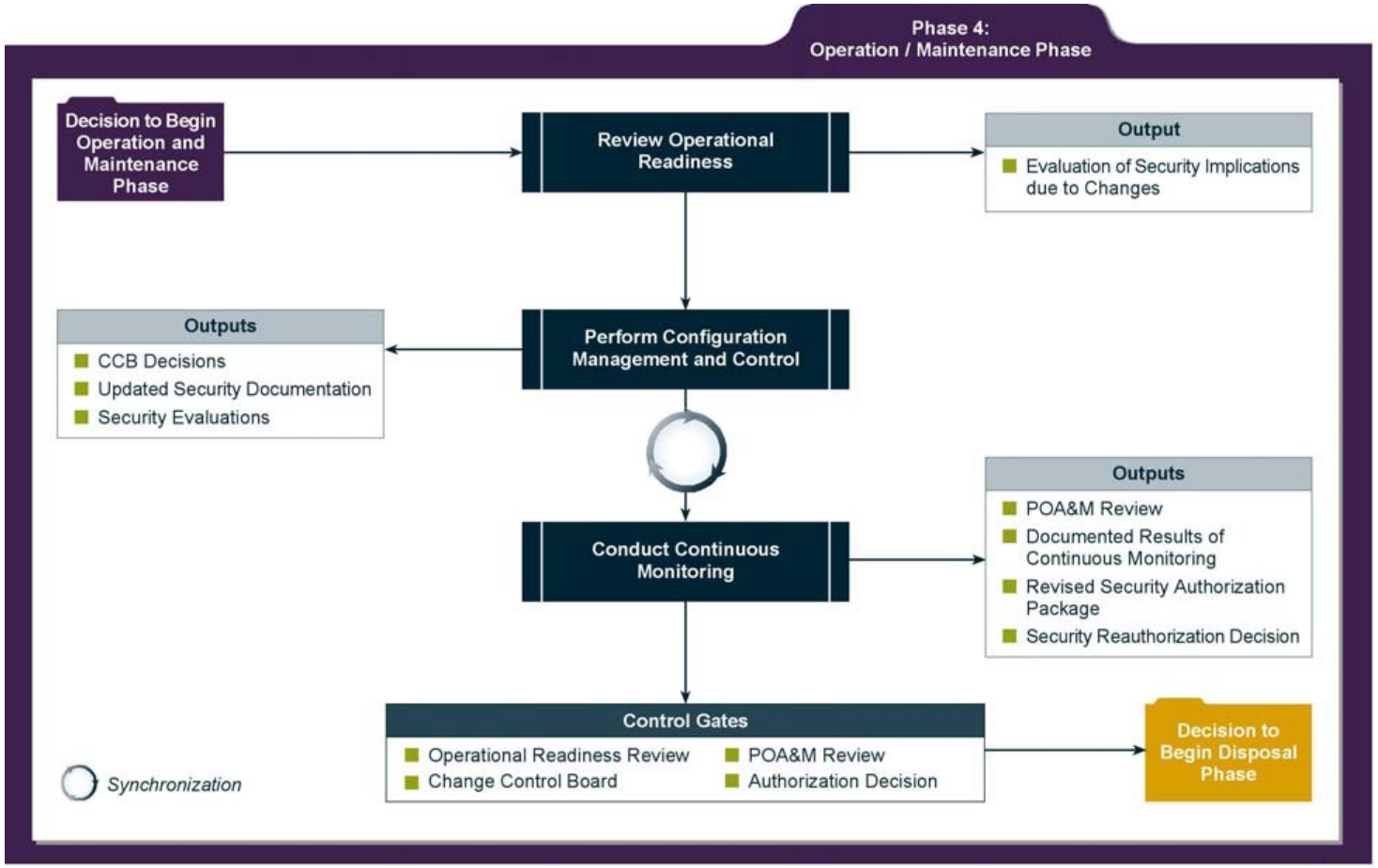
- Systems being developed or undergoing software, hardware, and/or communication modification(s) **must be formally assessed prior** to being granted formal accreditation
- A security certification must be conducted to assess the extent to which the controls are implemented, operating as intended, and producing the desired outcome
- Periodic testing and evaluation of the security controls in an information system must be conducted
- Security certification may uncover and describe actual vulnerabilities in the information system

Authorize the Information System

- This security accreditation is based on the verified effectiveness of security controls to some agreed-upon level of assurance and an identified residual risk to agency assets or operations
- The security authorization decision is a risk-based decision that depends heavily, but not exclusively, on the security testing and evaluation results produced during the security control verification process

- A lot of assessing and certifying just occurred
- Makes us feel more comfortable launching into operations now!

SDLC Phase 4: Operations / Maintenance



Review Operational Readiness

- When systems transition into production, unplanned changes can occur
- Depending on changes, a modified test of the security controls should be performed
- This review analyzes those changes, performs additional testing if needed, and confirms systems readiness for production
- This step is not always needed

Perform Configuration Management and Control

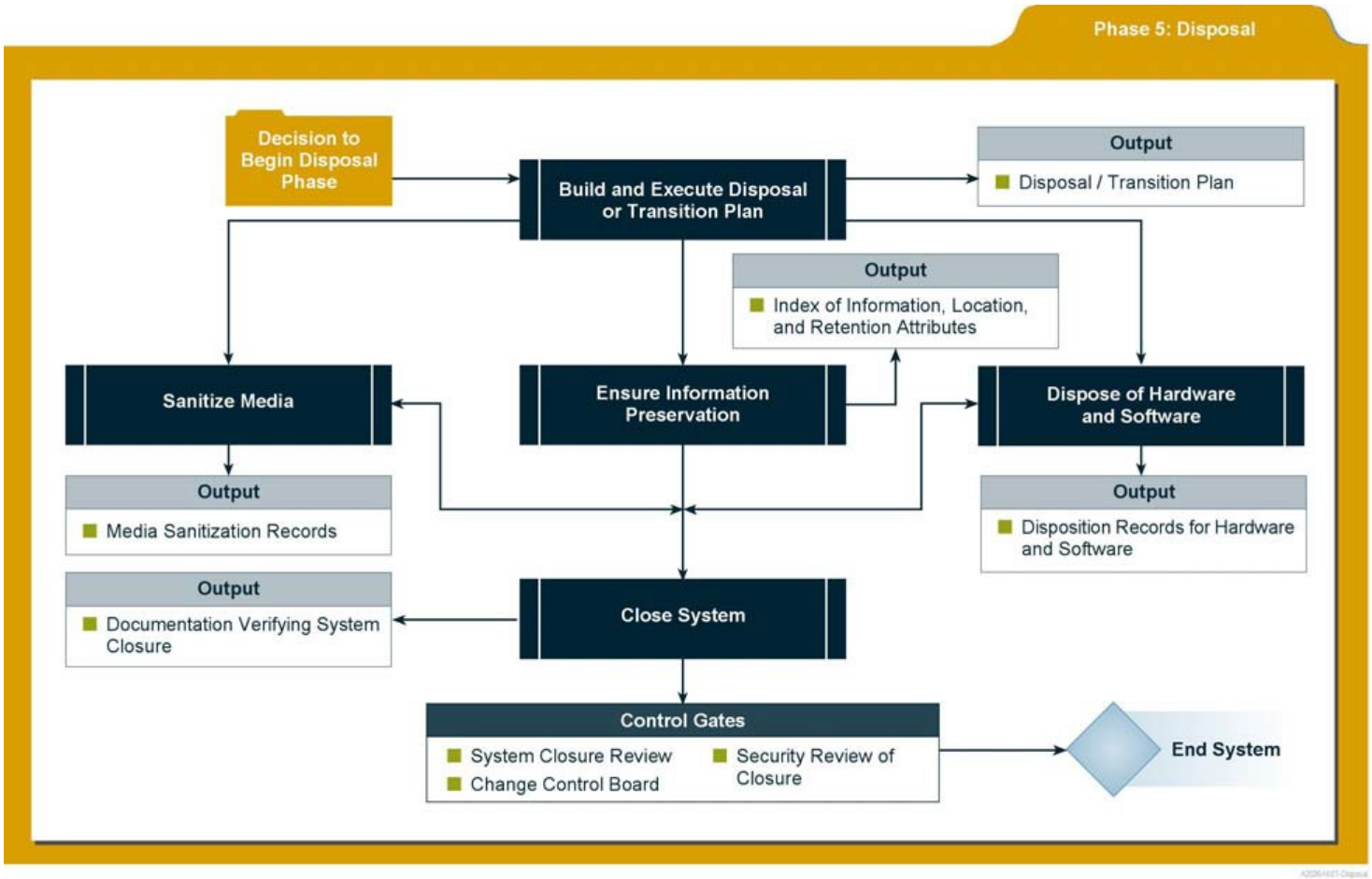
- Configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently for controlling and maintaining an accurate inventory of any changes to the system.
- Output includes:
  - Change Control Board (CCB) decisions
  - Updated security documentation
  - Security evaluations of documented system changes

Conduct Continuous Monitoring

- Objective is to determine if the security controls in the information system continue to be effective over time as changes occur in the system as well as the environment in which it operates
- Ongoing monitoring of security controls can be accomplished in a variety of ways:
  - security reviews, self-assessments, configuration management, antivirus management, patch management, security testing and evaluation, or audits
  - Automation should be leveraged where possible to reduce level of effort and ensure repeatability
- Don’t forget reaccreditation when significant changes have taken place!

- Wash, Rinse, Repeat!
- Operational tasks are never finished!
- Now what happens when it's time to dispose of the system?

SDLC Phase 5: Disposal



Build and Execute a Disposal/Transition Plan

- Should account for the disposal / transition status for all critical components, services, and information
- The plan identifies necessary steps, decisions, and milestones needed to properly close down, transition, or migrate a system or its information.
- Expected output:
  - Documented disposal/transition plan for closing or transitioning the system and/or its information

Ensure Information Preservation

- When preserving information, organizations should consider the methods that will be required for retrieving information in the future
- Technology used to retrieve the records may not be readily available in the future
- Legal requirements for records retention must be considered when disposing of systems
- Output includes:
  - Index of preserved information, and its location and retention attributes

Sanitize Media

- NIST 800-88 divides media sanitization into four categories: disposal, clearing, purging and destroying.
- The system owner categorize the information, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Then decide appropriate sanitization process.
- Output includes:
  - Media sanitization records

Dispose of Hardware and Software

- Hardware and software can be sold, given away, or discarded as provided by applicable law or regulation
- The disposal of software should comply with license or other agreements with the developer and with government regulations.
- Outputs include:
  - Disposition records for hardware and software. These records may include lists of hardware and software released (sold, discarded, or donated), and lists of hardware and software redeployed to other projects or tasks within the organization.

Closure of System

- The information system is formally shut down and disassembled at this point
- Output: Documentation verifying system closure, including final closure notification to the authorizing and certifying officials, configuration management, system owner, ISSO, and program manager


GAME
OVER