THEME 1

Systems of informational security

Telecommunication systems department

Lecturer: assistant professor Persikov Anatoliy Valentinovich

SYSTEM DEVELOPMENT LIFE CYCLE

Information systems must meet the minimum security requirements.

These requirements are defined in the second mandatory security standard required by the FISMA legislation, FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems". The minimum security requirements cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of information systems and the information processed, stored, and transmitted by those systems:

1) access control
2) awareness and training
3) audit and accountability
4) certification, accreditation, and security assessments
5) configuration management
6) contingency planning
7) identification and authentication
8) incident response
9) maintenance
10) media protection
11) physical and environmental protection
12) planning
13) personnel security
14) risk assessment
15) systems and services acquisition
16) system and communications protection
17)system and information integrity

SYSTEM DEVELOPMENT LIFE CYCLE

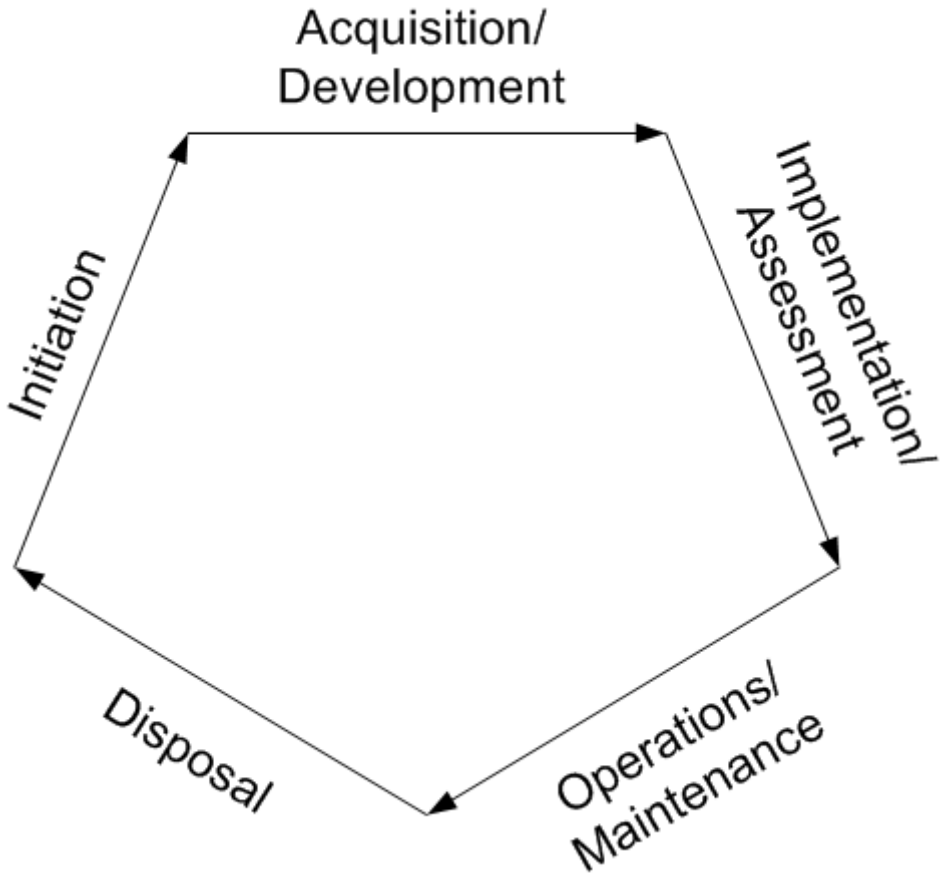
The **system development life cycle** (**SDLC**) is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal. There are many different SDLC models and methodologies, but each generally consists of a series of defined steps or phases.

Various SDLC methodologies have been developed to guide the processes involved, and some methods work better than others for specific types of projects. Regardless of the type of the life cycle used by an organization, information security must be integrated into the SDLC to ensure appropriate protection for the information that the system is intended to transmit, process, and store.

Security is most useful and cost-effective when such integration begins with a system development or integration project initiation, and is continued throughout the SDLC through system disposal.

A number of laws and directives require integrating security into the SDLC, including the **Federal Information Security Management Act** (FISMA) and **Office of Management and Budget** (OMB) **Circular** A-130, Appendix III.

SYSTEM DEVELOPMENT LIFE CYCLE



INITIATION PHASE

All information technology (IT) projects have a starting point, what is commonly referred to as the **initiation phase**.

During the initiation phase, the organization establishes the need for a particular system and documents its purpose. The information to be **processed**, **transmitted**, or **stored** is typically evaluated, as well as who is required access to such information and how (in high-level terms). In addition, it is often determined whether the project will be an independent information system or a component of an already-defined system. A **preliminary risk assessment** is typically conducted in this phase, and **security planning documents are initiated** (system security plan).

Once these tasks have been completed and a need has been recognized for a **new** or **enhanced IT product** or **service**, several processes must take place before the project is approved, to include clearly defining project goals and defining high-level information security requirements. Typically, during this phase, the organization defines high-level information security policy requirements as well as the enterprise security system architecture.

DEVELOPMENT/ACQUISITION PHASE

During this phase, the system is **designed**, **purchased**, **programmed**, **developed**, or otherwise **constructed**. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle.

During the first part of the development/acquisition phase, the organization should simultaneously define the system's security and functional requirements. These requirements can be expressed as technical features (e.g., access control), assurances (e.g., background checks for system developers), or operational practices (e.g., awareness and training). During the last part of this phase, the organization should perform developmental testing of the technical and security features/functions to ensure that they perform as intended prior to launching the implementation and integration phase.

IMPLEMENTATION PHASE

In the implementation phase, the organization **configures** and **enables system security features**, tests the functionality of these features, installs or implements the system, and finally, obtains a formal authorization to operate the system.

Design reviews and system tests should be performed before placing the system into operation to ensure that it meets all required security specifications. In addition, if new controls are added to the application or the support system, additional acceptance tests of those new controls must be performed.

This approach ensures that new controls meet security specifications and do not conflict with or invalidate existing controls.

The results of the design reviews and system tests **should be fully documented**, updated as new reviews or tests are performed, and maintained in the official organization records.

OPERATIONS/MAINTENANCE PHASE

An effective security program demands **comprehensive** and **continuous understanding of program and system weaknesses**. In the operation and maintenance phase, systems and products are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced.

During this phase, the organization should continuously monitor performance of the system to ensure that it is consistent with pre-established user and security requirements, and needed system modifications are incorporated.

For configuration management (CM) and control, it is important to document the proposed or actual changes in the security plan of the system. Information systems are typically in a constant state of evolution with upgrades to hardware, software, firmware, and possible modifications to the surrounding environment where the system resides. Documenting information system changes and assessing the potential impact of these changes on the security of a system is an essential part of continuous monitoring, and key to avoiding a lapse in the system security accreditation.

.

DISPOSAL PHASE

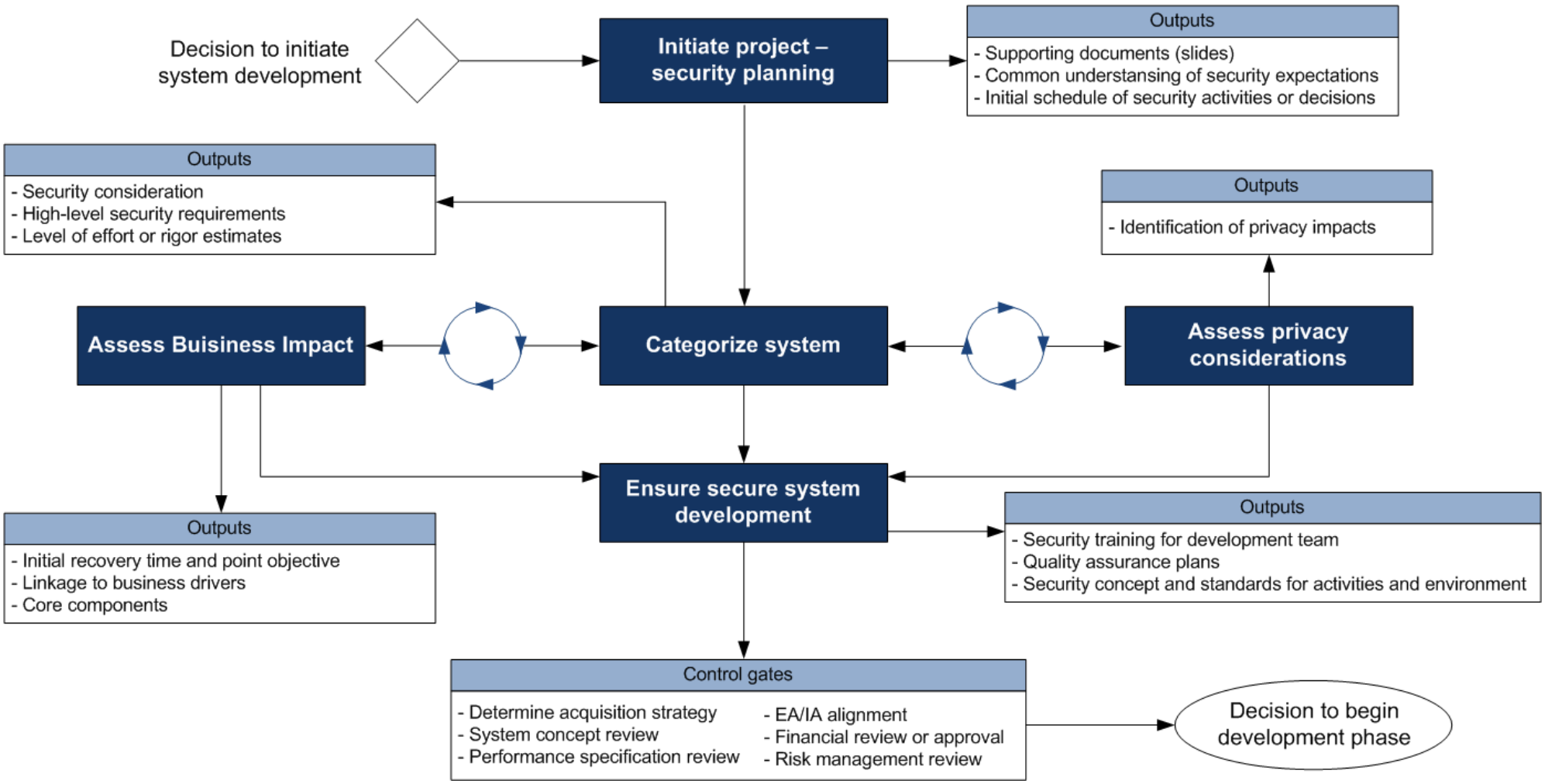
The disposal phase of the system life cycle refers to the process of preserving (if applicable) and discarding system information, hardware, and software.

This step is extremely important because during this phase, information, hardware, and software are moved to another system, archived, discarded, or destroyed. If performed improperly, the disposal phase can result in the unauthorized disclosure of sensitive data.

When archiving information, organizations should consider the need and methods for future retrieval. While electronic information is relatively easy to store and retrieve, problems can arise if the technology used to create the records is no longer available in the future as a result of obsolescence or incompatibility with new technologies. Additionally, the organization should consider what measures must be taken for the future use of data that has been encrypted, such as taking appropriate steps to ensure the secure long-term storage of cryptographic keys. It is equally important to consider legal requirements for records retention when disposing of information systems.

The removal of information from a storage medium, such as a hard disk or tape, is called **sanitization**. There are four categories of media sanitization: disposal, clearing, purging, and destroying.

INITIATION PHASE: DETAILS



INITIATION PHASE: DETAILS

During this first phase of the development life cycle, security considerations are key to diligent and early integration thereby ensuring that threats, requirements, and potential constraints in functionality and integration are considered.

At this point, security is looked at more in terms of business risks with input from the IT security office. For example, an agency may identify a political risk resulting from a prominent website being modified or made unavailable during a critical business period resulting in decreased trust by citizens.

Key security objectives for this phase include:

- Initial delineation of business requirements in terms of confidentiality, integrity, and availability.
- Determination of information categorization and identification of known special handling requirements to transmit, store or create information such as personally identifiable information.
- Determination of any privacy requirements.

Early planning and awareness will result in cost and timesaving through proper risk management planning. Security discussions should be performed as part of (not separately from) the development project to ensure solid understandings among project personnel of business decisions and their risk implications to the overall development project.

INITIATION PHASE: DETAILS

General types of control gates for this phase may include:

- An information system security categorization review of identified information types, resulting impact levels, and final Security Categorization.
- A System concept review that verifies that the concept is viable, complete, achievable, and in line with organizational mission objectives and budgetary constraints.
- An enterprise architecture alignment that harmonizes IT vision, standards, business requirements, as well as security alignment with current and imminent security services.
- A performance specification review that ensures the initial system design has addressed all currently identified specified security requirements.
- A risk management review that conforms to the recommended NIST risk management framework guidelines to reduce ambiguity in managing system risk.
- A financial review that verifies the system will be aligned with CPIC artifacts and guidance while balancing the cost implications associated with risk management.

INITIATION PHASE: DETAILS

Security planning should begin in the project initiation phase by:

- identifying key security roles for the system development;
- ensuring all key stakeholders have a common understanding, including security implications, considerations, and requirements;
- outlining initial thoughts on key security milestones including time frames or development triggers that signal a security step is approaching.

This early involvement will enable the developers to plan security requirements and associated constraints into the project. It also reminds project leaders that many decisions being made have security implications that should be weighed appropriately, as the project continues.

Expected outputs are:

- Meeting minutes or supporting documentation, such as slides.
- Common understanding of security expectations.
- Initial schedule of security activities or decisions.

INITIATION PHASE: DETAILS

Security categorization provides a vital step towards integrating security into the government agencies' business and information technology management functions and establishes the foundation for security standardization among information systems. Security categorization starts with the identification of what information supports which government lines of business, as defined by the EA. Subsequent steps focus on the evaluation of security in terms of confidentiality, integrity, and availability. The result is strong linkage between

Expected outputs are:

- essential to the security categorization process is documenting the research, key decisions, and supporting rationale driving the information system, security categorization (this is included in the System Security Plan);
- initial level of rigor can be derived from applying the resulting security categorization to the minimal security controls.

INITIATION PHASE: DETAILS

An **assessment of system impact** on the agency lines of business correlates specific system components with the critical business services that are provided. That information is then used to characterize the business and mission consequences of a disruption to the system's components. An initial draft of this product early in the lifecycle alerts system stakeholders to key IT and security decisions. This task should also take into account the availability impact level identified during the security categorization task.

Expected outputs are:

- Identification of lines of business this system supports and how they will be impacted?
- What core system components are needed to maintain minimal functionality?
- How long can the system be down before the business is impacted? (Initial idea of the needed Recovery Time Objective)
- What is the business tolerance for loss of data? (Initial idea of the needed Recovery Point Objective)

INITIATION PHASE: DETAILS

Assess Privacy Impact. When developing a new system it is important to directly consider if the system will transmit, store, or create information that may be considered privacy information. This typically is identified during the security categorization process when identifying data types.

Once identified as a system under development that will likely handle privacy information, the **system owner should work towards identifying and implementing the necessary steps to enable proper safeguards and security controls**.

INITIATION PHASE: DETAILS

Many organizations have employed either a **one** or **two-step model** to address privacy considerations.

The **one-step model** requires all systems on the agency's system inventory develop a privacy impact assessment that outlines criteria for privacy information determination and documents security controls employed to properly protect the information.

In contrast, the **two step model** differentiates by processing all systems through a threshold analysis, which is focused on whether a privacy impact assessment should be performed. A positive answer would then result in the execution of a more detailed evaluation of privacy data and proper security controls in the form of a privacy impact assessment.

The resulting document of either process would then be incorporated into the system security plan and maintained appropriately.

Expected outputs are: Privacy Impact Assessment providing details on where and to what degree privacy information is collected, stored or created within the system.

INITIATION PHASE: DETAILS

Ensure Use of Secure Information System Development Processes

Primary responsibility for application security, during early phases, lies in the hands of the development team who has the most in-depth understanding of the detailed workings of the application and ability to identify security defects in functional behavior and business process logic. They are the first level of defense and opportunity to build in security. It is important that their role not be assumed or diminished. Communicating and providing expectations is key to planning and enabling an environment that protects down to the code level.

Considerations to plan for include:

Secure Concept of Operations (CONOPS) for Development. A concept of operations document for secure development should be established for the environment and a contingency plan should be in place for the code repository as source code is the predominant work product of software and system development and should be preserved in the event of interruption to the development environment.

INITIATION PHASE: DETAILS

Standards and Processes. System development should occur with standard processes that consider secure practices and are documented and repeatable. To accomplish this, appropriate security processes for the assurance level required by the system should be determined and documented. Thus, systems with a high assurance requirement may need additional security controls built into the development process.

Security Training for Development Team. Additional security training may be needed for key developers to understand the current threats and potential exploitations of their products as well as training for secure design and coding techniques. This enables the developers to create more secure designs and empowers them to address key issues early in the development processes.

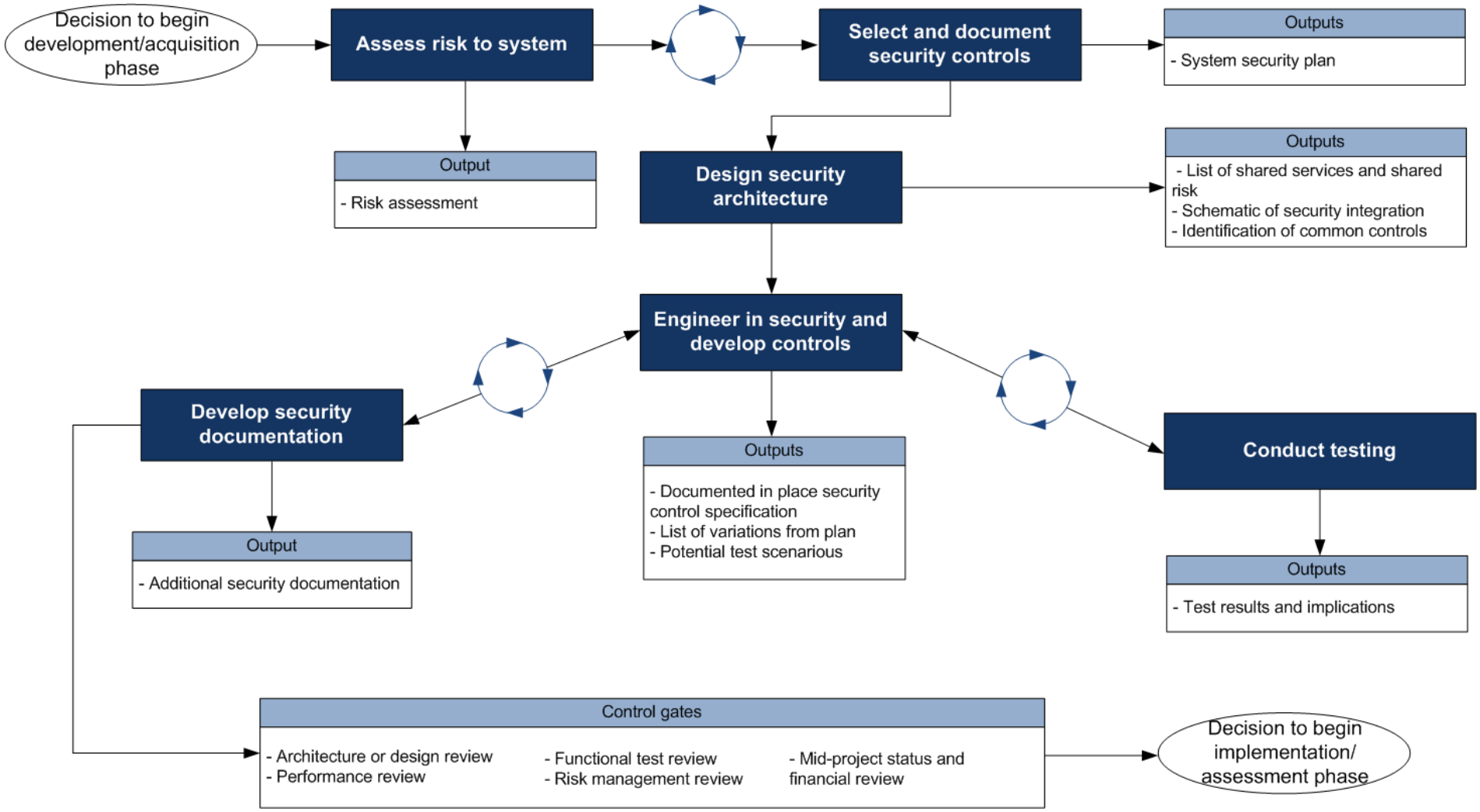
Quality Management. Quality management, which includes planning, assurance and control, is key to ensuring minimal defects within and proper execution of the information system. This reduces gaps or holes that are sometimes left open for exploitation or misuse (whether intentional or not) causing vulnerabilities in the system.

INITIATION PHASE: DETAILS

Secure Environment. The system development environment should meet minimum FISMA compliance criteria as expressed in SP 800-53. This is to include workstations, servers, network devices, and code repositories. Development environments must be accredited as would any other operational system or environment. A secure development environment lends itself to developing secure software and systems.

Secure Code Practices and Repositories. Special attention should be placed upon code repositories with an emphasis on systems that support distributed code contribution with check-in/check-out functionality. Role-based access should apply to accessing the code repository, and logs should be reviewed regularly as part of the secure development process. Code should be developed in accordance with standard practices. A necessary part of the aforementioned CONOPS is the establishment and retention of secure coding patterns and components. Secure coding patterns embody code level examples and accompanying documentation that illustrate how to meet specific functional requirements while simultaneously achieving security mandates. These patterns can then be reused by developers to ensure that all software components are developed in an assured fashion, having been vetted and adopted by the organization.

DEVELOPMENT/ACQUISITION PHASE: DETAILS



DEVELOPMENT/ACQUISITION PHASE: DETAILS

Key security activities for this phase include:

- conduct the risk assessment and use the results to supplement the baseline security controls;
- analyze security requirements;
- perform functional and security testing;
- prepare initial documents for system certification and accreditation; and
- design security architecture.

Security analysis of complex systems will need to be iterated until consistency and completeness is achieved.

DEVELOPMENT/ACQUISITION PHASE: DETAILS

General types of control gates for this phase may include:

- An **Architecture/Design Review** that evaluates the planned system design and potential integration with other systems as well as incorporation of shared services and common security controls, such as authentication, disaster recovery, intrusion detection, or incident reporting.
- A **System Performance Review** that evaluates whether the system is delivering, or capable of delivering, to the documented expectation of the owner and whether the system behaves in a predictable manner if it is subjected to improper use. (For example, the ability of the system to maintain availability and data integrity at the expected extreme resource loads.)
- A **System Functional Review** that ensures functional requirements identified are sufficiently detailed and are testable.
- **Mid-Project Status & Financial Review** is important to detect major shifts in planned level of effort to ensure cost-benefit ratios are monitored and effective decisions are continued.
- A **follow-on review of risk management decisions** may be needed if, due to the aforementioned reviews, the system and/or its security controls and/or its requirements change.

DEVELOPMENT/ACQUISITION PHASE: DETAILS

Assess Risk to System

Organizations should consult NIST SP 800-30, **Risk Management Guide for Information Technology Systems**, for guidance on conducting risk assessments.

The **purpose of a risk assessment** is to evaluate current knowledge of the system's design, stated requirements, and minimal security requirements derived from the security categorization process to determine their effectiveness to mitigate anticipated risks.

Results should show that specified security controls provide appropriate protections or highlight areas where further planning is needed. To be successful, participation is needed from people who are knowledgeable in the disciplines within the system domain (e.g., users, technology experts, operations experts).

The security risk assessment should be conducted before the approval of design specifications as it may result in additional specifications or provide further justification for specifications.

DEVELOPMENT/ACQUISITION PHASE: DETAILS

In addition to considering the security perspective of the system being developed/ acquired, **organizations should also consider how the system might affect other systems to which it will be directly or indirectly connected**.

This may mean that there are inherited common controls to leverage or additional risks that need to be mitigated. In these cases, an enterprise review may be needed to provide a more comprehensive view of threats and vulnerabilities.

Expected outputs are: A refined risk assessment based on a more mature system design that more accurately reflects the potential risk to the system, known weaknesses in the design, identified project constraints, and known threats to both business and IT components. In addition, previous requirements are now transitioning into system specific controls.

DEVELOPMENT/ACQUISITION PHASE: DETAILS

Select and Document Security Controls

The selection and documentation of security controls corresponds to step 2 in the NIST Risk Management Framework.

The selection of security controls consists of three activities:

1) the **selection of baseline security controls** (including common security controls);
2) the **application of security control tailoring guidance** to adjust the initial security control baseline;
3) and the **supplementation of the tailored baseline** with additional controls based on an assessment of risk and local conditions.

An organization-wide view is essential in the security control selection process to ensure that adequate risk mitigation is achieved for all mission/business processes and the information systems and organizational infrastructure supporting those processes.

DEVELOPMENT/ACQUISITION PHASE: DETAILS

The security control selection process should include an analysis of laws and regulations, such as FISMA, OMB circulars, agency-enabling acts, agency-specific governance, FIPS and NIST Special Publications, and other legislation and federal regulations that define applicable specifics to the security controls selected.

As with other aspects of security, **the goal should be cost-effective implementation** that meets the requirements for protection of an organization's information assets. In each situation, a balance should exist between the system security benefits to mission performance and the risks associated with operation of the system.

Expected Output is: System Security Plan - specification of security controls that identify which, where, and how security controls will be applied.

DEVELOPMENT/ACQUISITION PHASE: DETAILS

Design Security Architecture

With the increase in shared service providers and the centralization of some key security services within agencies, it is becoming more important to plan these services and understand how they will be integrated into the system.

An enterprise alignment of the system should ensure that the initiative fits the agency's future plans and does not conflict or unnecessarily provide redundant services. In addition, as the system matures and more decisions are made as to services utilized, the EA should be reviewed for optimal integration.

At the system level, security should be architected and then engineered into the design of the system. This may be accomplished by zoning or clustering services either together or distributed for either redundancy or additional layers of protection. Security designing at the system level should take into consideration services obtained externally, planned system interconnections, and the different orientations of system users (e.g., customer service versus system administrators).

DEVELOPMENT/ACQUISITION PHASE: DETAILS

Another example would be a **system auditing strategy** that should be developed to enable an accurate trace or reconstruction of all priority and high-risk work flows. The audit strategy should include various audit records from several different components including (but not limited to) the Web application, databases, mainframe, and Web servers. The goal should not be to capture as much audit information as possible but to capture only what is needed to provide enough information to investigate potential security breaches and system failures.

Expected outputs are:

- **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.
- **Listing of shared services** and **resulting shared risk**.
- **Identification of common controls** used by the system.

DEVELOPMENT/ACQUISITION PHASE: DETAILS

Engineer in Security and Develop Controls

During this stage, security controls are implemented and become part of the system rather than applied at completion. Applying security controls in development should be considered carefully and planned logically.

For new information systems, the security requirements identified and described in the respective system security plans are now designed, developed, and implemented. The system security plans for operational information systems may require the development of additional security controls to supplement in-place controls or the modification of controls that are deemed to be less than effective.

During this task, decisions are made based on integration challenges and trade-offs. It is important to document the major decisions and their business/technology drivers. In cases where the application of a planned control is not possible or advisable, compensating controls should be considered and documented.

Expected outputs are:

- 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.

DEVELOPMENT/ACQUISITION PHASE: DETAILS

Develop Security Documentation

While the most prominent document is the **System Security Plan**, documentation supporting it may include:

- configuration management plan;
- contingency plan (including a Business Impact Assessment);
- continuous monitoring plan;
- security awareness, training and education (SATE) plan;
- incident response plan;
- privacy impact assessment (PIA).

Development of these documents should consider the maturity of the security services being documented. In some cases, these documents may contain only known requirements, common controls, and templates. Filling in these documents should begin as early as possible during the project.

Expected output is: additional security documentation supporting the system security plan.

DEVELOPMENT/ACQUISITION PHASE: DETAILS

Conduct Testing (Developmental, Functional and Security)

Systems being developed or undergoing software, hardware, and/or communication modification(s) must be tested and evaluated prior to being implemented.

The **objective of the test and evaluation process** is to validate that the developed system complies with the functional and security requirements. Testing of security controls is based on technical security specifications for those controls supplemented by the assessment procedures detailed in NIST SP 800-53A, **Guide for Assessing the Security Controls in Federal Information System**s.

The process focuses on specificity, repeatability, and iteration. For specificity, the testing must be scoped to test the relevant security requirement as it is intended for use in its environment. For repeatability, the testing process 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. For 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. To achieve this, functional testing will 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.

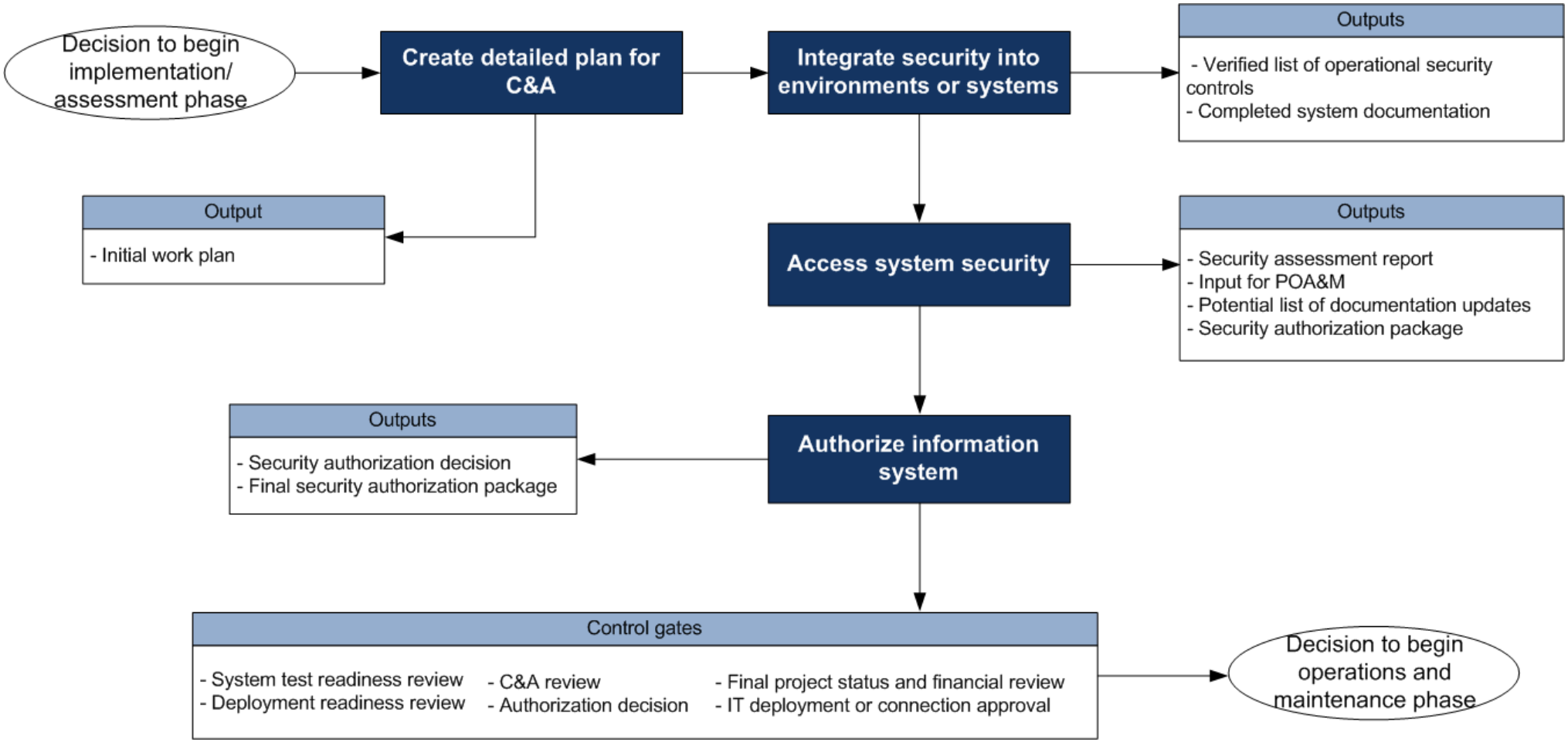
DEVELOPMENT/ACQUISITION PHASE: DETAILS

The use of automated testing tools and integration of the **NIST Security Content Automation Protocol (SCAP)** should be accomplished prior to the commencement of security control test and evaluation activities. Any security functionality not tested during the functional or automated testing will be carefully examined to ensure compliance with the requirements during the explicit security control test and evaluation.

Only test or “stub” data should be used during system development. Absolutely no operational, security-relevant, or personally identifiable information (PII) should reside within any system or software during development.

Expected output is: documentation of test results, including any unexpected variations discovered during testing.

IMPLEMENTATION / ASSESSMENT PHASE: DETAILS



IMPLEMENTATION / ASSESSMENT PHASE: DETAILS

Implementation/Assessment is the third phase of the SDLC. During this phase, the system will be installed and evaluated in the organization's operational environment. Key security activities for this phase include:

- Integrate the information system into its environment;
- Plan and conduct system certification activities in synchronization with testing of security controls; and
- Complete system accreditation activities.

General types of control gates for this phase may include:

- System Test Readiness Review
- C&A Review
- Final Project Status and Financial Review
- Deployment Readiness Review
- Authorizing Official (AO) Decision
- IT Deployment or Connection Approval.

IMPLEMENTATION / ASSESSMENT PHASE: DETAILS

Create a Detailed Plan for C&A

Because the Authorizing Official (AO) is responsible for accepting the risk of operating the system, the AO can advise the development team if the risks associated with eventual operation of the system appear to be unacceptable. Specifications can impose excessive burden and costs if the acceptable residual risks are not known. The involvement of the AO is required for this determination of acceptable residual risks. It is easier to incorporate requirement changes during the planning stage of a system acquisition than during the solicitation, source selection, or contract administration stages.

The development team and the AO should also discuss the forms of evidence that the AO needs to make a decision. This evidence may include system test results and other data. In addition, the acquisition initiator and the accrediting official should discuss how changes to the system and its environment would be addressed. The possibility of establishing a security working group should be discussed. Such a group may consist of personnel such as users, program managers, and application sponsors; system, security, or database administrators; security officers or specialists, including the C&A representatives; and system or application analysts.

IMPLEMENTATION / ASSESSMENT PHASE: DETAILS

To ensure proper testing and reduce the likelihood of scope creep during testing, the security accreditation boundary should be clearly delineated. This will form the basis for the test plan to be created and approved prior to implementation performance.

At this point, the certification package should be close to completion, and any agency-specified initial review for conformance has commenced.

Expected output is: 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.

IMPLEMENTATION / ASSESSMENT PHASE: DETAILS

Integrate security into established environments or systems

System integration occurs at the operational site when the information system is to be deployed for operation. 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.

Expected outputs are:

- Verified list of operational security controls.
- Completed System Documentation.

IMPLEMENTATION / ASSESSMENT PHASE: DETAILS

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. The objective of the security assessment process is to validate that the system complies with the functional and security requirements and will operate within an acceptable level of residual security risk. Testing of security controls is based on the assessment procedures detailed in NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems.

Prior to initial operations, a security certification must be conducted to assess the extent to which the controls are implemented, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In addition, periodic testing and evaluation of the security controls in an information system must be conducted to ensure continued effectiveness.

Expected output is: Security Accreditation Package, which includes the Security Assessment Report, the POA&M, and the updated System Security Plan.

IMPLEMENTATION / ASSESSMENT PHASE: DETAILS

Authorize the information system

OMB Circular A-130 requires the security authorization of an information system to process, store, or transmit information. This authorization (also known as security accreditation), granted by a senior agency official, 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 (including mission, function, image, or reputation).

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.

IMPLEMENTATION / ASSESSMENT PHASE: DETAILS

An authorizing official relies primarily on:

(i) the completed system security plan;

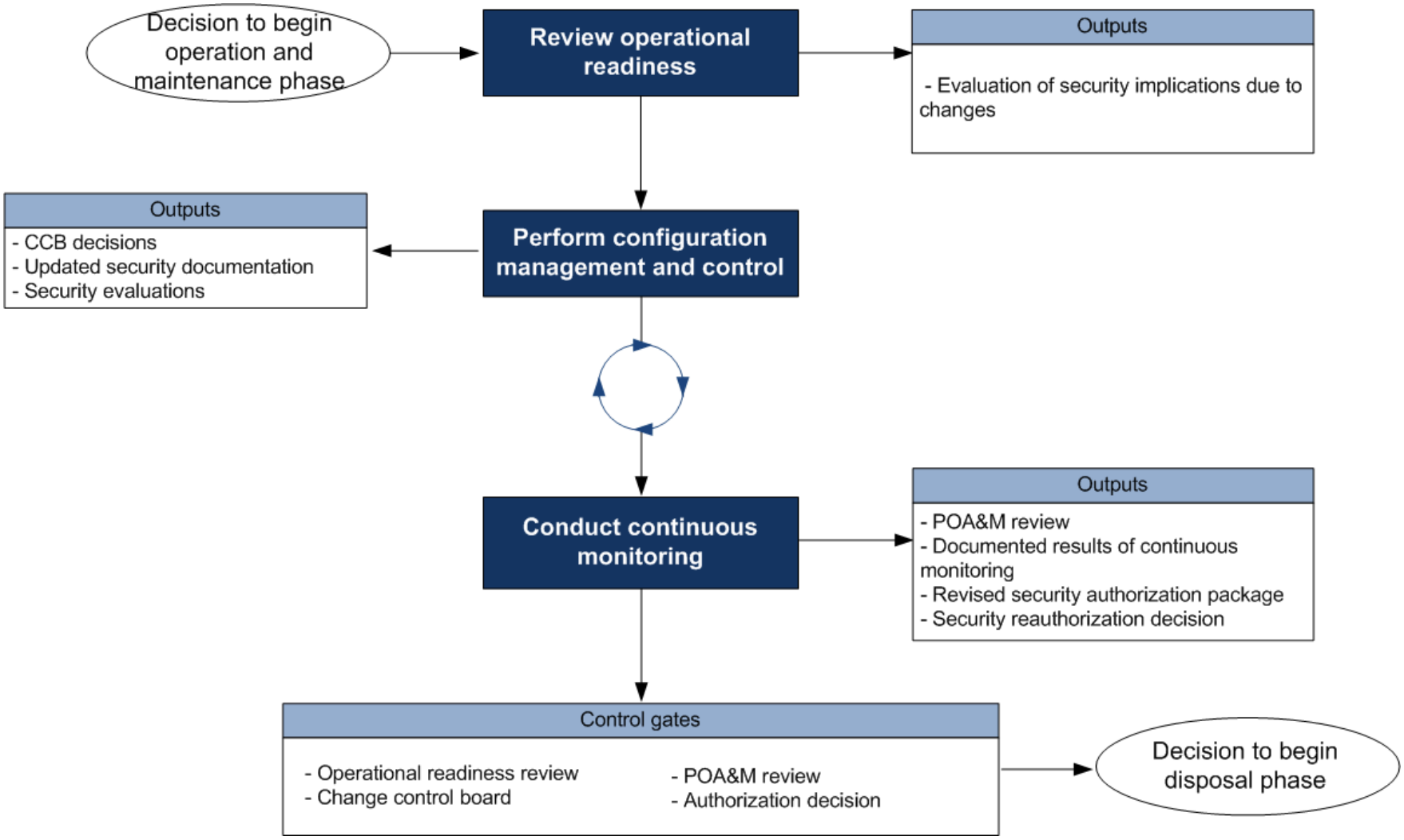
(ii) the security test and evaluation results; and

(iii) the POA&M for reducing or eliminating information system vulnerabilities, in making the security authorization decision to permit operation of the information system and to accept explicitly the residual risk to agency assets or operations.

Expected Outputs are:

- Security Authorization Decision, documented and transmitted from Authorizing Official to System Owner and ISSO;
- Final Security Authorization Package.

OPERATIONS AND MAINTENANCE PHASE: DETAILS



OPERATIONS AND MAINTENANCE PHASE: DETAILS

Operations and Maintenance is the fourth phase of the SDLC. In this phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced.

The system is monitored for continued performance in accordance with security requirements and needed system modifications are incorporated.

The operational system is periodically assessed to determine how the system can be made more effective, secure, and efficient.

Operations continue as long as the system can be effectively adapted to respond to an organization's needs while maintaining an agreed-upon risk level.

When necessary modifications or changes are identified, the system may reenter a previous phase of the SDLC.

OPERATIONS AND MAINTENANCE PHASE: DETAILS

Key security activities for this phase include:

- conduct an operational readiness review;
- manage the configuration of the system;
- institute processes and procedures for assured operations and continuous monitoring of the information system's security controls; and
- perform reauthorization as required.

General types of control gates for this phase may include:

- operational Readiness Review;
- change Control Board Review of Proposed Changes;
- review of POA&Ms;
- accreditation Decisions (Every three years or after a major system change).

OPERATIONS AND MAINTENANCE PHASE: DETAILS

Review operational readiness

Many times when a system transitions to a production environment, unplanned modifications to the system occur. If changes are significant, a modified test of security controls, such as configurations, may be needed to ensure the integrity of the security controls.

This step is not always needed; however, it should be considered to help mitigate risk and efficiently address last-minute surprises.

Expected output is: evaluation of security implications due to any system changes.

OPERATIONS AND MAINTENANCE PHASE: DETAILS

Perform Configuration Management and Control

An effective agency configuration management and control policy and associated procedures are essential to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment.

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. Changes to the hardware, software, or firmware of a system can have a significant security impact.

Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation.

OPERATIONS AND MAINTENANCE PHASE: DETAILS

These steps, when implemented effectively, provide vital input into the system's continuous monitoring capability. As such, it facilitates the agency's ability to identify significant changes that alter a system's security posture and control effectiveness to ensure proper assessment and testing occurs.

Expected outputs are:

- Change Control Board (CCB) decisions;
- Updated security documentation (System Security Plan, POA&M);
- Security evaluations of documented system changes.

OPERATIONS AND MAINTENANCE PHASE: DETAILS

Conduct continuous monitoring

The ultimate objective of continuous monitoring is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as the environment in which the system operates.

A well-designed and well-managed continuous monitoring process can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status information to appropriate organizational officials. This information can be used to take appropriate risk mitigation actions and make credible, risk-based authorization decisions regarding the continued operation of the information system and the explicit acceptance of risk that results from that decision.

OPERATIONS AND MAINTENANCE PHASE: DETAILS

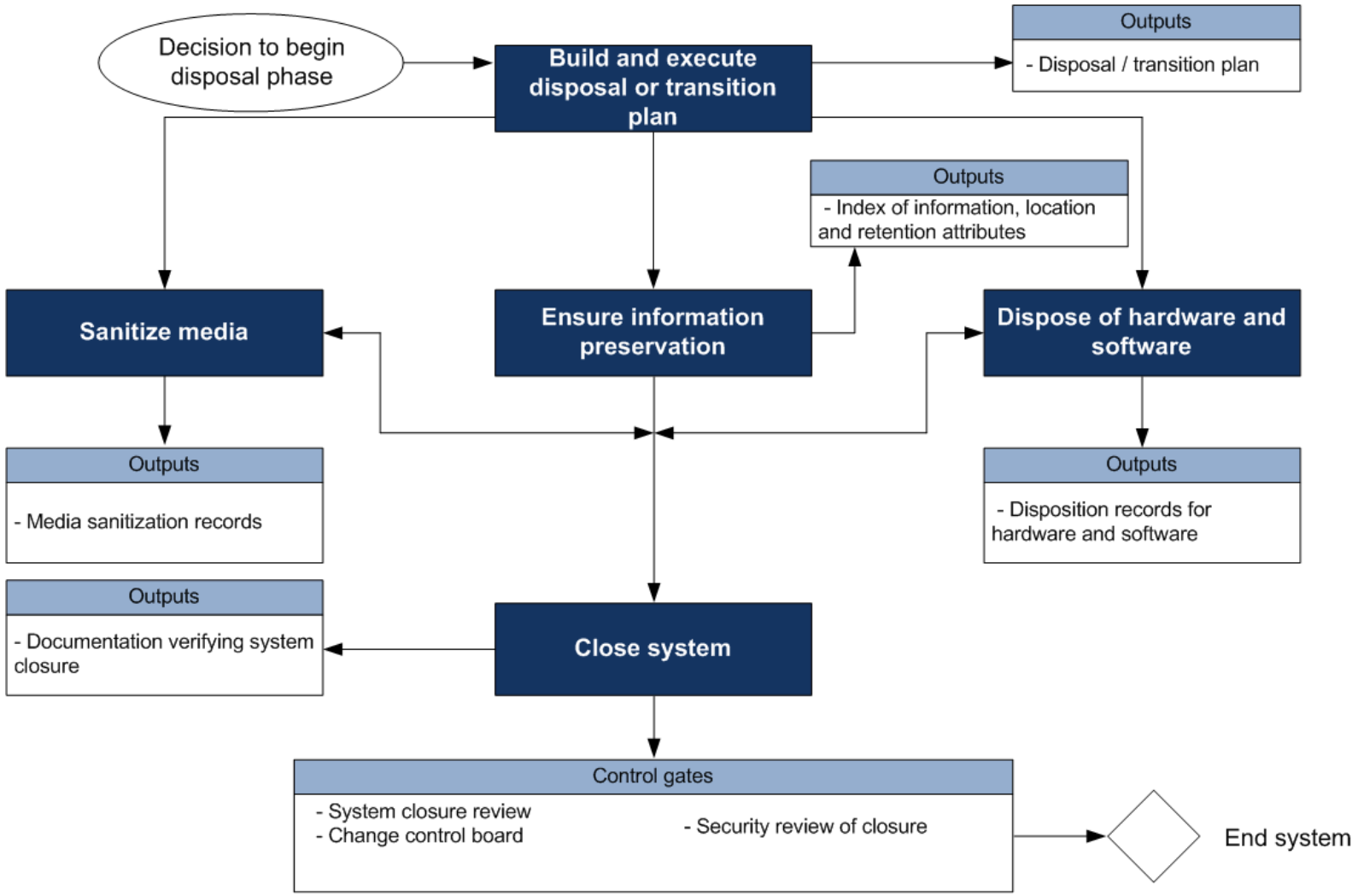
The ongoing monitoring of security control effectiveness can be accomplished in a variety of ways, including security reviews, self-assessments, configuration management, antivirus management, patch management, security testing and evaluation, or audits. Automation should be leveraged where possible to reduce level of effort and ensure repeatability.

Included as a part of continuous monitoring is reaccreditation which occurs when there are significant changes to the information system affecting the security of the system or when a specified time period has elapsed in accordance with federal or agency policy.

Expected outputs are:

- documented results of continuous monitoring;
- POA&M review;
- security reviews, metrics, measures, and trend analysis;
- updated security documentation and security reaccreditation decision, as necessary.

DISPOSAL PHASE: DETAILS



DISPOSAL PHASE: DETAILS

Disposal, the final phase in the SDLC, provides for disposal of a system and closeout of any contracts in place. Information security issues associated with information and system disposal should be addressed explicitly. When information systems are transferred, become obsolete, or are no longer usable, it is important to ensure that government resources and assets are protected.

Usually, there is no definitive end to a system. Systems normally evolve or transition to the next generation because of changing requirements or improvements in technology. System security plans should continually evolve with the system. Much of the environmental, management, and operational information should still be relevant and useful in developing the security plan for the follow-on system.

The disposal activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future, if necessary. Particular emphasis is given to proper preservation of the data processed by the system so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access.

DISPOSAL PHASE: DETAILS

Key security activities for this phase include:

- build and Execute a Disposal/Transition Plan;
- archive of critical information;
- sanitization of media; and
- disposal of hardware and software.

General types of control gates for this phase may include:

- System Closure Review;
- Change Control Board;
- Security Review of Closure.

DISPOSAL PHASE: DETAILS

Build and Execute a Disposal/Transition Plan

Building a disposal / transition plan ensures that all stakeholders are aware of the future plan for the system and its information. This plan should account for the disposal / transition status for all critical components, services, and information.

Much like a work plan, this plan identifies necessary steps, decisions, and milestones needed to properly close down, transition, or migrate a system or its information.

In many cases, disposed systems or system components have remained dormant but still connected to the infrastructure. As a result, these components are often overlooked, unaccounted for, or maintained at suboptimal security protection levels thus, providing additional and unnecessary risk to the infrastructure and all connected systems. A transition plan assists in mitigating these possible outcomes.

Expected output is: documented disposal/transition plan for closing or transitioning the system and/or its information.

DISPOSAL PHASE: DETAILS

Ensure Information Preservation

When preserving information, organizations should consider the methods that will be required for retrieving information in the future. The technology used to retrieve the records may not be readily available in the future (particularly if encrypted). Legal requirements for records retention must be considered when disposing of systems.

Expected output is: index of preserved information, and its location and retention attributes.

DISPOSAL PHASE: DETAILS

Sanitize Media

Based on the results of security categorization, the system owner should refer to NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, which specifies that, “the organization sanitizes information system digital media using approved equipment, techniques, and procedures.

The organization tracks, documents, and verifies media sanitization and destruction actions and periodically tests sanitization equipment/procedures to ensure correct performance.

The organization sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media.”

DISPOSAL PHASE: DETAILS

NIST SP 800-88, Guidelines for Media Sanitization, divides media sanitization into four categories: disposal, clearing, purging and destroying. It further suggests that 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 on the appropriate sanitization process. The selected process should be assessed as to cost, environmental impact, etc., and a decision made that best mitigates the risk to confidentiality and best satisfies other constraints imposed on the process.

Several factors should be considered along with the security categorization of the system confidentiality when making sanitization decisions. The cost versus benefit of a media sanitization process should be understood prior to a final decision. For instance, it may not be cost-effective to degauss inexpensive media such as diskettes.

Expected outputs are: media sanitization records

DISPOSAL PHASE: DETAILS

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. There is rarely a need to destroy hardware except for some storage media that contains sensitive information and that cannot be sanitized without destruction. In situations when the storage media cannot be sanitized appropriately, removal and physical destruction of the media may be possible so that the remaining hardware may be sold or given away. Some systems may contain sensitive information after the storage media is removed. If there is doubt whether sensitive information remains on a system, the ISSO should be consulted before disposing of the system. Also, the vendor may be consulted for additional disposal options or verification of risk.

Expected outputs are: 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.

DISPOSAL PHASE: DETAILS

Closure of System

The information system is formally shut down and disassembled at this point.

Expected output is: Documentation verifying system closure, including final closure notification to the authorizing and certifying officials, configuration management, system owner, ISSO, and program manager.

THANKS FOR ATTENTION