

Building Solutions for a Better Tomorrow



Baked-in Security and the System Development Life Cycle (SDLC)



Overview

- What is the SDLC?
- Why Integrate Security into the SDLC?
- Roles and Responsibilities
- Security in the SDLC



What is the SDLC?

“The SDLC is a mandatory process used to standardize the development of software.”



Why Integrate Security into the SDLC?

FISMA – States that the Office of Management and Budget (OMB) shall oversee the implementation of government-wide policies, principles, standards, and guidelines for Federal government computer security programs.

OMB Circular A-130, Appendix III – A document produced by OMB that gives NIST the responsibility to develop information security guidance and Federal Information Processing Standards (FIPS) documents.



Why Integrate Security into the SDLC?

Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*

- Mandatory security standard that specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements.
- **This standard mandates the use of the security controls found in NIST SP 800-53**



Why Integrate Security into the SDLC?

- **SA-3 Life-Cycle Support**
- “The organization manages the information system using a system development life cycle methodology that includes information security considerations.”

This is a security control directly related to the requirement to follow a SDLC from NIST SP 800-53, Revision 2.



Roles and Responsibilities

- Chief Information Officer (CIO)
- Contracting Officer & Technical Representative
- Information Technology Investment Board
- Information System Security Officer
- Program Manager/Data Owner
- Privacy Officer



Roles and Responsibilities (Continued)

Chief Information Officer (CIO)

- The CIO is responsible for the organization's information system planning, budgeting, investment, performance and acquisition. As such, the CIO provides advice and assistance to senior organization personnel in acquiring the most efficient and effective information system to fit the organization's enterprise architecture
- The CIO is most often the Designated Approval Authority (DAA) for FISMA systems.
- Others may be designated to act as the DAA for systems under their area of responsibility.



Roles and Responsibilities (Continued)

Contracting Officer

Has authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

Contracting Officer Technical Representative (COTR)

Qualified employee appointed by the Contracting Officer to act as their technical representative in managing the technical aspects of a particular contract.

Information Technology Investment Board (or equivalent)

Responsible for managing the capital planning and investment control process defined by the Clinger-Cohen Act of 1996 (Section 5).



Roles and Responsibilities (Continued)

Information System Security Officer (ISSO)

- The ISSO is responsible for ensuring the systems information is secure throughout the SDLC.
- May be designated to act as the Certifying Authority during the Certification & Accreditation process.



Roles and Responsibilities (Continued)

Program Manager (Data Owner)

- Represents programmatic interests during the acquisition process. The system owner, who has been involved in strategic planning initiatives of the acquisition, plays an essential role in security and is, ideally, intimately aware of functional system requirements.
- Has a personal and direct interest in ensuring that the information system functions as intended and provides users the level of confidentiality, availability, and integrity defined in the specifications or requirements documents.



Roles and Responsibilities (Continued)

Privacy Officer

- Responsible for ensuring that the service or system being procured or developed meets existing privacy policies regarding protection, dissemination, (information sharing and exchange) and information disclosure.
- Should remain involved throughout the life-cycle of the system to ensure that system data confidentiality is maintained at the appropriate level.



Security in the SDLC Process

SDLC Phases

- Initiation
- Development/Acquisition
- Implementation
- Operational/Maintenance
- Disposition

<i>SDLC Phases</i>	Initiation	Development/ Acquisition	Implementation		Operational/ Maintenance	Disposition
<i>Security NIST SP 800-37 Phases</i>	Initiation		Certification	Accreditation	Continuous Monitoring	



Initiation Phase ***(Security: Initiation Phase)***



Initiation Phase

Overview

During the initiation phase, the need for a system is expressed and the purpose of the system is documented.

- System Categorization
- Preliminary Security Risk Assessment



Initiation Phase (Continued)

System Categorization

To determine the overall impact level of the information system –

1. Determine the different types of information that are processed, stored, or transmitted by the information system (e.g., information management, budget & finance, IT infrastructure maintenance, etc.).
2. Use the impact levels in FIPS 199, the recommendations of NIST Special Publication 800-60 Volume II, and possibly the BRM to categorize the system's confidentiality, integrity, and availability of each information type as low, moderate, or high impact.
3. Determine the information system security categorization; that is, the highest impact level for each security objective (confidentiality, integrity, availability) from among the categorizations for the information types associated with the information system.
4. Determine the overall impact level of the information system from the highest impact level among the three security objectives in the system security categorization.



Initiation Phase (Continued)

System Categorization (continued)

Find the information types that the information system will process, store, or transmit, by referring to **NIST SP 800-60, Volume II**

If information type is not listed in NIST SP 800-60 refer to the:

Federal Business Reference Model (BRM):

<http://www.whitehouse.gov/omb/egov/a-3-brm.html>



Initiation Phase (Continued)

System Categorization (continued)

Categorize the System Using FIPS 199

Security Objective	Low	Moderate	High
<p>Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]</p>	<p>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p>Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]</p>	<p>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p>Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]</p>	<p>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>



Initiation Phase (Continued)

System Categorization (continued)

The system categorization establishes the overall impact level at which to protect your system (e.g., High, Medium, or Low).

Example Information Types –

Information Type	Confidentiality	Integrity	Availability
IT Infrastructure Maintenance	Low	Moderate	Low
Official Information Dissemination	Low	Low	Low
System Maintenance	Low	Moderate	Low
IT Security	Low	Moderate	Low
Information Management	Low	Moderate	Low
System Development	Low	Moderate	Low



Initiation Phase (Continued)

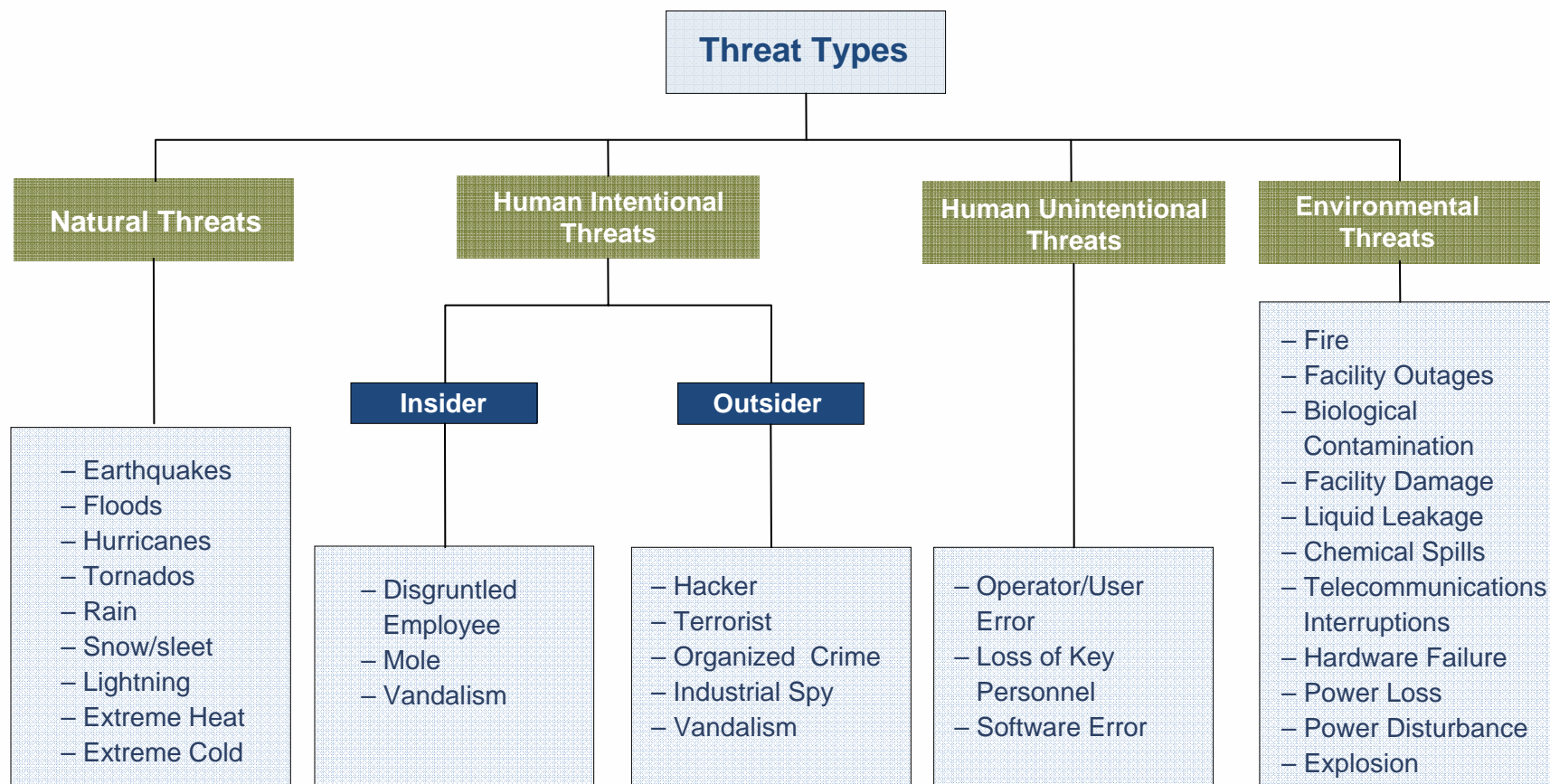
Preliminary Security Risk Assessment

- Used to determine the threats to the system environment, laws, and regulations that apply; identify personnel; and to plan and conduct security-related activities.
- Refer to NIST SP 800-30 for qualitative risk assessment method and NIST SP 800-53, Revision 2, for security controls related to the system's potential threat environment.
- Should result in an initial description of the basic security needs of the system.



Initiation Phase (Continued)

Preliminary Security Risk Assessment





Development/Acquisition Phase (Security: Initiation Phase)



Development/Acquisition Phase

Overview

During this phase the system's security requirements analysis and planning are completed. The system is also designed, purchased, programmed, developed, or otherwise constructed.

- Risk Assessment
- Security Functional Requirements
- Security Assurance Requirements
- Cost Considerations and Reporting
- Security Planning
- Security Control Development
- Developmental Security test and Evaluation
- Other Planning Components



Development/Acquisition Phase (continued)

Requirements Analysis; Risk Assessment (NIST SP 800-30)

- Used to identify the system's protection requirements through the use of a formal risk assessment process.
- Generates essential information needed to complete the system security plan.
- The risk assessment includes the following:
 1. Identification of threats to and vulnerabilities in the information system
 2. The potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on agency assets or operations (mission, functions, image, or reputation) should there be a threat of exploitation
 3. Identification and analysis of security controls for the information system
- Consider potential inheritance of vulnerabilities by other systems.



Development/Acquisition Phase (continued)

Security Functional Requirements Analysis

- May include two sources of system security requirements:
 - **System security environment** (Enterprise security policy & enterprise security architecture)
 - **Security functional requirements**
- Analysis should include laws and regulations such as:
 - Privacy Act
 - FISMA
 - OMB circulars
 - Agency enabling acts
 - NIST Special Publications and FIPS documents
 - Other legislation and federal regulations
- More than one risk assessment may be required as this phase of the SDLC progresses



Development/Acquisition Phase (continued)

Security Assurance Requirements Analysis (NIST SP 800-23)

This analysis should address the developmental activities required and assurance needed to produce the desired level of confidence that the information security will work correctly and effectively. Some considerations follow:

- Common criteria
- Validation testing for cryptographic modules and algorithms
- Third-party evaluations
- Accreditation of a system to operate in a similar situation
- Test and evaluation procedures
- Test and evaluation under the auspices and review of an independent organization



Development/Acquisition Phase (continued)

Cost Considerations and Reporting (OMB Memorandum 00-07)

- Anticipate the cost of security throughout the system's life cycle:
 - Consider what it will cost to mitigate vulnerabilities noted during the previous functional and assurance analysis
 - Consider the results of the previous risk assessments
- Include the security costs in the agency's "Capital Asset Plan" as part of the Exhibit 300 submission. (OMB Circular A-11, Part 3)
- Include the system security cost as part of the overall percentage of funding on the Exhibit 53, Agency Information Technology Investment Portfolio.
- Ensure the cost for security can be aggregated into the agency's annual FISMA report along with the fall budget submission.



Development/Acquisition Phase (continued)

Security Planning

- FISMA requires system security plans for all networks, facilities, information systems or groups of systems to ensure adequate security is in place or planned.
- Refer to NIST SP 800-18, Guide for Developing Security Plans for Information Systems.
- Refer to NIST SP 800-53 for inclusion of the state of the implementation of required security controls to protect the information system's data.



Development/Acquisition Phase (continued)

Security Planning (Continued)

System security plan attachments may include –

- Configuration management plan
- Contingency plan
- Incident response plan
- Security awareness training plan
- Rules of behavior
- Risk assessment
- Security test and evaluation results
- System interconnection agreements
- Security authorizations/accreditations
- Plan of action and milestones



Development/Acquisition Phase (continued)

Security Control Development

The process for developing the security control baseline is as follows:

- From the catalog of security controls (NIST SP 800-53) select a provisional set of controls using the “high water mark” from the system categorization.

Information Type	Confidentiality	Integrity	Availability
IT Infrastructure Maintenance	Low	Moderate	Low
Official Information Dissemination	Low	Low	Low
System Maintenance	Low	Moderate	Low
IT Security	Low	Moderate	Low
Information Management	Low	Moderate	Low
System Development	Low	Moderate	Low



Development/Acquisition Phase (continued)

Security Control Development (Continued)

Tailor the provisional baseline of security controls by applying the “scoping guidance” found in NIST SP 800-53, page 18:

- Common security control related guidance
- Operational/environmental related considerations
- Physical Infrastructure related considerations
- Public access related considerations
- Technology related considerations
- Policy/regulatory related considerations
- Security objective related considerations



Development/Acquisition Phase (continued)

Security Control Development (Continued)

Example – Security objective-related considerations

Security controls related to “Confidentiality” and “Availability” may be downgraded to the “Low” level from the “Moderate” provisional level.

Information Type	Confidentiality	Integrity	Availability
IT Infrastructure Maintenance	Low	Moderate	Low
Official Information Dissemination	Low	Low	Low
System Maintenance	Low	Moderate	Low
IT Security	Low	Moderate	Low
Information Management	Low	Moderate	Low
System Development	Low	Moderate	Low

Confidentiality: AC-15, MA-3 (3), MP-2 (1), MP-3, MP-4, MP-5 (1) (2) (3), MP-6, PE-5, SC-4, SC-9

Integrity: SC-8

Availability: CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, MA-6, PE-9, PE-10, PE-11, PE-13, PE-13, PE-15, SC-6



Development/Acquisition Phase (continued)

Security Control Development, NIST SP 800-53, Rev. 2 (Continued)

CNT L NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
System and Services Acquisition				
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	SA-3	SA-3	SA-3
SA-4	Acquisitions	SA-4	SA-4 (1)	SA-4 (1)
SA-5	Information System Documentation	SA-5	SA-5 (1)	SA-5 (1) (2)
SA-6	Software Usage Restrictions	SA-6	SA-6	SA-6
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security Design Principles	Not Selected	SA-8	SA-8
SA-9	Outsourced Information System Services	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	Not Selected	Not Selected	SA-10
SA-11	Developer Security Testing	Not Selected	SA-11	SA-11



Development/Acquisition Phase (continued)

Developmental Security Test and Evaluation

- Security controls must be tested to ensure they are performing as intended prior system deployment.
- A test and evaluation plan must be developed for those controls that can be tested before the systems is deployed.
- Controls that cannot be tested such as those non-technical in nature, management and operational, may be tested at a later date.
- May provide important insight to developers regarding the state of security of the system.



Development/Acquisition Phase (continued)

Developmental Security Test and Evaluation (Continued)

Test ID	M-14		
Control Type	Management Controls – System and Services Acquisition		
Objective	Determine if the organization manages the information system using a system development life cycle methodology that includes information security considerations.		
NIST SP 800-53 Cross-Ref.	SA-3		
Method of Execution	Examine	Interview	Test
Test Execution			
Expected Results			
Actual Results	Pass	Fail	Re-test
Discrepancies/ Vulnerabilities			
Test Date(s)			
Tester(s)			
Point(s) of Contact			
Documents Reviewed/Received			
Comments			



Development/Acquisition Phase (continued)

Other Planning Components (NIST SP 800-64)

- Type of contract
- Review by other functional groups
- Review by certifier and accreditor
- Cyclical nature of the process
- Evaluation and acceptance
- Request for proposal development
- Security specification and statement of work development
- Information security specification sources
 - General specifications
 - Federally mandated specifications
- Proposal evaluation
- Developing an evaluation plan, etc.



Implementation Phase (Security: Certification & Accreditation)



Implementation Phase

Overview

During this phase the system is tested, certified, accredited, and installed in the operational environment.

- Inspection and Acceptance
- System Integration
- Security Certification
- Security Accreditation



Implementation Phase (Continued)

Inspection and Acceptance

- Involves the government's decision to inspect, accept and pay for a deliverable.
- While related to the Certification and Accreditation (C&A) process, this is a different process; this inspection involves the system meeting functional specification.
- May include security specification that will be validated through the C&A process.



Implementation Phase (Continued)

System Integration

- Occurs at the operational site where the information system is to be deployed.
- Security control settings and switches are enabled in accordance with manufacturer instructions and available security implementation guidance.



Implementation Phase (Continued)

Security Certification

- Must occur prior to the system's final deployment.
- Should be accomplished by an independent third party.
- Verifies which security controls are in place and if they are operating as intended.
- Tests are based on the System Test & Evaluation plan developed previously in the Development Acquisition Phase.
- The depth of testing, "examine, interview, or test," is based on the tailored security control baseline and NIST SP 800-53A, Technical and Procedures for Verifying the Effectiveness of Security controls in Federal Information Systems.



Implementation Phase (Continued)

Security Certification, NIST SP 800-53A (Continued)

STEP NO	SPECIALIZED ASSESSMENT PROCEDURE
SA-3	<p>LIFE CYCLE SUPPORT</p> <p><u>Control</u>: The organization manages the information system using a system development life cycle methodology that includes information security considerations.</p> <p><u>Supplemental Guidance</u>: NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.</p> <p>(L) Indicates that this section of the assessment procedure is optional for low-impact information systems. (M) Indicates that this section of the assessment procedure is optional for moderate-impact information systems.</p>
SA-3.1	<p>ASSESSMENT OBJECTIVE:</p> <p><i>Determine if:</i></p> <ul style="list-style-type: none"> <i>(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations; and</i> <i>(ii) the organization uses a system development life cycle that is consistent with NIST Special Publication 800-64.</i> <p>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</p> <p>Examine: [<i>SELECT FROM</i>: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST Special Publication 800-64; information system development life cycle documentation; other relevant documents or records]. (L) (M) (H)</p> <p>Interview: [<i>SELECT FROM</i>: Organizational personnel with information security and system life cycle development responsibilities]. (H)</p>



Implementation Phase (Continued)

Security Accreditation

- OMB Circular A-130 requires the security authorization of an information system to process, store, or transmit information.
- In order to make a sound risk-based accreditation decision the senior agency official relies on the recommendation of the Certifying Authority, the ST&E results, the completed system security plan, the plan of action and milestones, and the risk assessment.
- The Accreditation letter must be signed, indicating the acceptance of residual risk, before the system is placed into production.



Operational/Maintenance Phase (Security: Continuous Monitoring)



Operational/Maintenance Phase

Overview

The purpose of this phase is to allow the system to operate performing its intended mission. While the system operates, it is essential to continuously assess and maintain the proper level of security.

- Configuration management and control
- Continuous monitoring



Operational/Maintenance Phase (Continued)

Configuration Management and Control

“The only thing consistent in IT is change”

- Implement a configuration management and change control process.
- Ensure that there are baseline configurations for all system components including hardware, software, procedures, etc.
- Ensure the change control process is in-place and functioning.
- Evaluate the security risk of proposed changes before approval.
- Evaluate the significance of system changes to determine if a new system C&A is required in accordance with NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal information Systems*.
- Involve your ISSO in the change control process.



Operational/Maintenance Phase (Continued)

Continuous Monitoring

- FISMA requires periodic and continuous testing and evaluation of the security controls in an information system to ensure that the controls are effective in applications.
- May include:
 - Security reviews
 - Self-assessments
 - Security Test and Evaluations
 - Audits
- NIST SP 800-53A should be consulted to determine the appropriate level of testing rigor for the system under test.

Testing must be accomplished at least annually and each control must be tested by an independent party at least once over a three year period.



Disposition Phase ***(Security: Continuous Monitoring)***



Disposition Phase

Overview

Disposition is the final phase of the SDLC. It ensures orderly termination of the system; safeguarding vital system information; and migrating data processed by the system to a new system, or preserving it in accordance with applicable records management regulations and policies.

The steps involved in this phase of the SDLC follow:

- Information preservation
- Media sanitization
- Hardware and software disposal



Disposition Phase (Continued)

Information Preservation

- Determine records retention requirements prior to moving, archiving, or destroying any data.
- Consider the technology required to retrieve or read the data. Will it be available if the data is to be retrieved? Should it be retained as well?
- Ensure long-term storage is in place for cryptographic keys (for encrypted data).
- Consider legal requirements for retaining or disposition of data, suspense, purge requirements, etc.



Disposition Phase (Continued)

Media Sanitization (NIST SP 800-88)

- Media Sanitization is the act of clearing or purging information from storage media.
- The method used depends on the sensitivity of the information to be removed.
 - Clearing is the removal of information to the level where it cannot be restored using normal system resources.
 - Purging is the removal of data in such a way that there is an assurance that the data may not be reconstructed unless very sophisticated and expensive means are employed to recover it.
- Some methods for purging data from media are degaussing, overwriting, and media destruction.



Disposition Phase (Continued)

Hardware and Software Disposal

- Rarely a need to destroy hardware unless it contains sensitive information that cannot be purged.
- Hardware and software may be sold, given away, reused, or simply discarded according to agency policy.
- Care must be taken to ensure the disposition of software complies with license agreements.
- If in doubt contact your ISSO for guidance.



Summary

- What is the SDLC?
- Why integrate security in the SDLC?
- Roles and responsibilities?
- Security in the SDLC?



Questions?