Non-repudiation - The origin or the receipt of a specific message must be verifiable by a third party.

Accountability - A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

Reference used for this question:

RFC 2828
SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (page 5).

QUESTION 349
During which phase of an IT system life cycle are security requirements developed?

A. Operation
B. Initiation
C. Functional design analysis and Planning
D. Implementation

Correct Answer: C
Explanation:
The software development life cycle (SDLC) (sometimes referred to as the System Development Life Cycle) is the process of creating or altering software systems, and the models and methodologies that people use to develop these systems.

The NIST SP 800-64 revision 2 has within the description section of para 3.2.1:

This section addresses security considerations unique to the second SDLC phase. 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.

Reviewing this publication you may want to pick development/acquisition. Although initiation would be a decent choice, it is correct to say during this phase you would only brainstorm the idea of security requirements. Once you start to develop and acquire hardware/software components then you would also develop the security controls for these. The Shon Harris reference below is correct as well.

Shon Harris' Book (All-in-One CISSP Certification Exam Guide) divides the SDLC differently:

Project initiation
Functional design analysis and planning
System design specifications
Software development
Installation
Maintenance support
Revision and replacement

According to the author (Shon Harris), security requirements should be developed during the

functional design analysis and planning phase.
SDLC POSITIONING FROM NIST 800-64

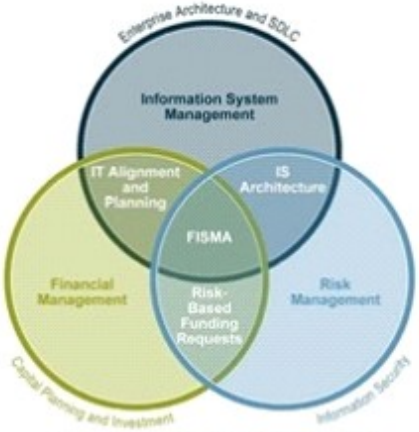
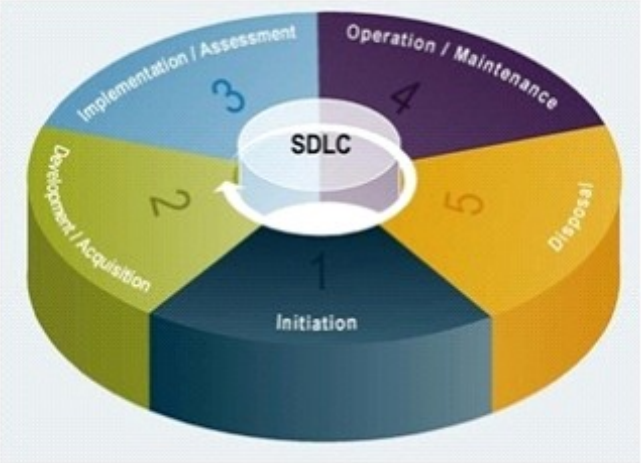


FIGURE 2-1. POSITIONING SECURITY CONSIDERATIONS

SDLC Positioning in the enterprise
Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (see Figure 2-1 above). The most effective way to implement risk management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization, revenue source, or topologies. Identification and verification of critical assets and operations and their interconnections can be achieved through the system security planning process, as well as through the compilation of information from the Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA) processes to establish insight into the agency's vital business operations, their supporting assets, and existing interdependencies and relationships.

With critical assets and operations identified, the organization can and should perform a business impact analysis (BIA). The purpose of the BIA is to relate systems and assets with the critical services they provide and assess the consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities. This positions the security office to facilitate the IT program's cost-effective performance as well as articulate its business impact and value to the agency.

SDLC OVERVIEW FROM NIST 800-64
SDLC Overview from NIST 800-64 Revision 2



NIST 800-64 Revision 2 is one publication within the NISTstandards that I would recommend you look at for more details about the SDLC. It describe in great details what activities would take place and they have a nice diagram for each of the phases of the SDLC. You will find a copy at:

http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf

DISCUSSION:
Different sources present slightly different info as far as the phases names are concerned.

People sometimes gets confused with some of the NIST standards. For example NIST 800-64 Security Considerations in the Information System Development Life Cycle has slightly different names, the activities mostly remains the same.

NIST clearly specifies that Security requirements would be considered throughout ALL of the phases. The keyword here is considered, if a question is about which phase they would be developed than Functional Design Analysis would be the correct choice.

Within the NIST standard they use different phase, howeverr under the second phase you will see that they talk specifically about Security Functional requirements analysis which confirms it is not at the initiation stage so it become easier to come out with the answer to this question. Here is what is stated:

The security functional requirements analysis considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance.

At the initiation step you would NOT have enough detailed yet to produce the Security Requirements. You are mostly brainstorming on all of the issues listed but you do not develop them all at that stage.

By considering security early in the information system development life cycle (SDLC), you may be able to avoid higher costs later on and develop a more secure system from the start.

NIST says:
NIST`s Information Technology Laboratory recently issued Special Publication (SP) 800- 64, Security Considerations in the Information System Development Life Cycle, by Tim Grance, Joan

Hash, and Marc Stevens, to help organizations include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls.

I must admit this is all very tricky but reading skills and paying attention to KEY WORDS is a must for this exam.

References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Page 956
NIST S-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
http://www.mks.com/resources/resource-pages/software-development-life-cycle-sdlc-system-development

QUESTION 350
Which of the following is an unintended communication path that is NOT protected by the system's normal security mechanisms?

A. A trusted path
B. A protection domain
C. A covert channel
D. A maintenance hook

Correct Answer: C
Explanation:
A covert channel is an unintended communication path within a system, therefore it is not protected by the system's normal security mechanisms. Covert channels are a secret way to convey information.

Covert channels are addressed from TCSEC level B2.

The following are incorrect answers:

A trusted path is the protected channel that allows a user to access the Trusted Computing Base (TCB) without being compromised by other processes or users.

A protection domain consists of the execution and memory space assigned to each process.

A maintenance hook is a hardware or software mechanism that was installed to permit system maintenance and to bypass the system's security protections.

Reference used for this question:
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 6: Operations Security (page 219).

QUESTION 351
Which of the following phases of a system development life-cycle is most concerned with maintaining proper authentication of users and processes to ensure appropriate access control decisions?

A. Development/acquisition
B. Implementation

C. Operation/Maintenance
D. Initiation

Correct Answer: C
Explanation:
The operation phase of an IT system is concerned with user authentication.

Authentication is the process where a system establishes the validity of a transmission, message, or a means of verifying the eligibility of an individual, process, or machine to carry out a desired action, thereby ensuring that security is not compromised by an untrusted source.

It is essential that adequate authentication be achieved in order to implement security policies and achieve security goals. Additionally, level of trust is always an issue when dealing with cross-domain interactions. The solution is to establish an authentication policy and apply it to cross-domain interactions as required.

Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 15).

QUESTION 352
Which of the following is NOT a common integrity goal?

A. Prevent unauthorized users from making modifications.
B. Maintain internal and external consistency.
C. Prevent authorized users from making improper modifications.
D. Prevent paths that could lead to inappropriate disclosure.

Correct Answer: D
Explanation:
Inappropriate disclosure is a confidentiality, not an integrity goal. All of the other choices above are integrity goals addressed by the Clark-Wilson integrity model.

The Clark-Wilson model is an integrity model that addresses all three integrity goals:

1. prevent unauthorized users from making modifications,
2. prevent authorized users from making improper modifications, and
3. maintain internal and external consistency through auditing.

NOTE: Biba address only the first goal of integrity above

Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1384). McGraw- Hill. Kindle Edition.

QUESTION 353
What is the most secure way to dispose of information on a CD-ROM?

A. Sanitizing
B. Physical damage
C. Degaussing
D. Physical destruction