CHAPTER THREE

INCORPORATING SECURITY INTO THE SDLC

This section describes a number of security considerations that will help integrate information security into the SDLC. Security considerations are identified in each SDLC phase, thus advancing the business application and security requirements together to ensure a balanced approach during development. **Figure 3-1**, organized by development phase, provides an overall view of the process.

FIGURE 3-1. THE SDLC – A CONCEPTUAL VIEW

In order to provide clear, concise guidance to the reader, each life cycle phase is described in a section below that has been organized in this manner:

- Provides a brief description of the SDLC phase.
- Identifies general control gates, or established points in the life cycle, when the system will be evaluated and when management will determine whether the project should continue as is, change direction, or be discontinued. Control gates should be flexible and tailored to the specific organization. Control gates are valuable in that they provide the organization with the opportunity to verify that security considerations are being addressed, adequate security

3.1 SDLC Phase: Initiation

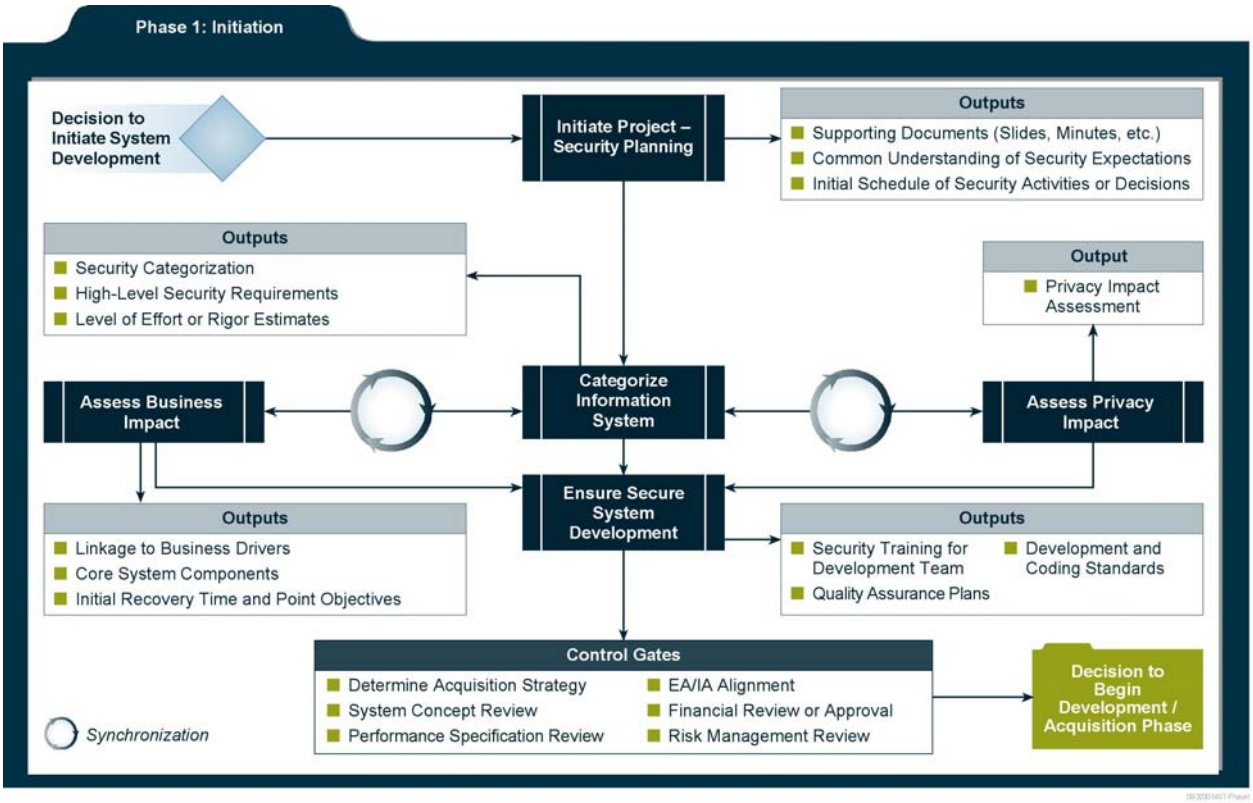

FIGURE 3-2. RELATING SECURITY CONSIDERATIONS IN INITIATION PHASE

3.1.1 Description

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 information 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 activities 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; and
- 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.

3.2 SDLC Phase: Development/Acquisition

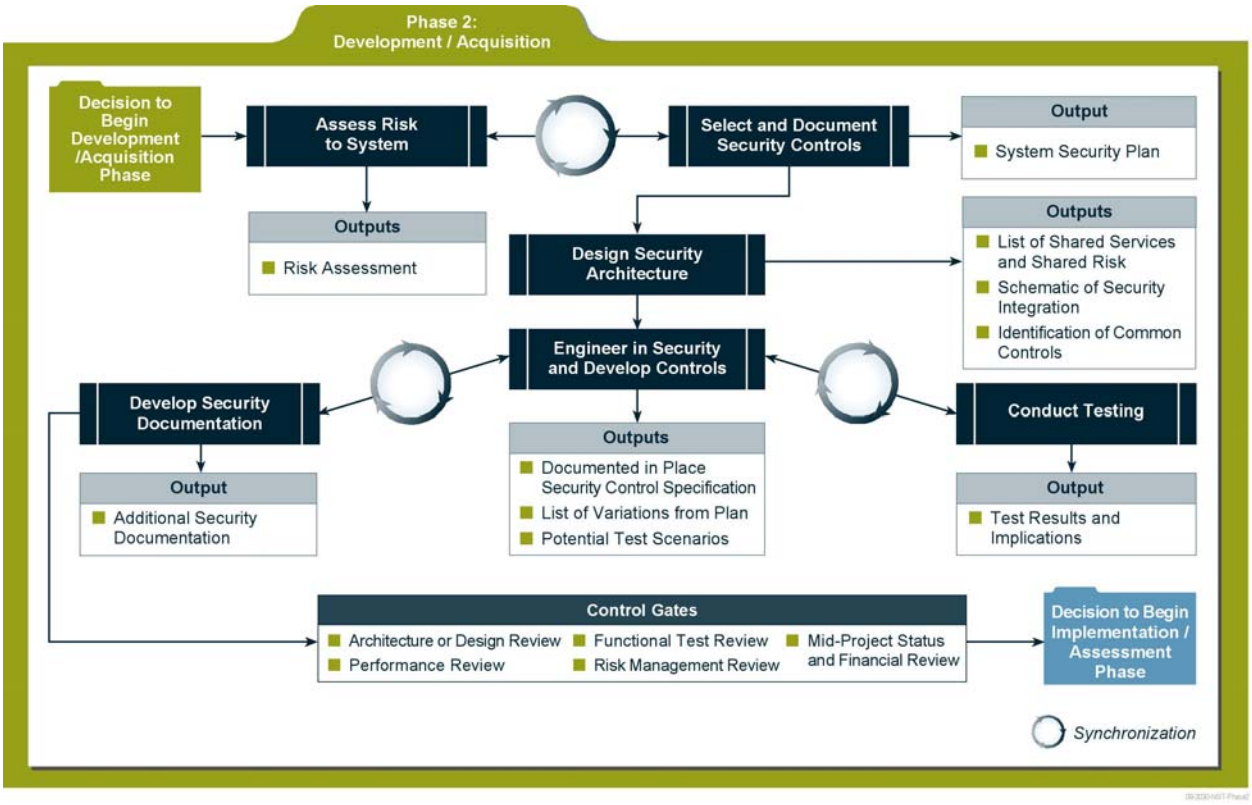

FIGURE 3-3. RELATING SECURITY CONSIDERATIONS IN THE DEVELOPMENT/ACQUISITION PHASE

3.2.1 Description

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.

Although this section presents the information security components in a sequential top-down manner, the order of completion is not necessarily fixed. Security analysis of complex systems will need to be iterated until consistency and completeness is achieved.

3.2.2 Control Gates

General types of control gates for this phase may include:

3.3 SDLC Phase: Implementation / Assessment

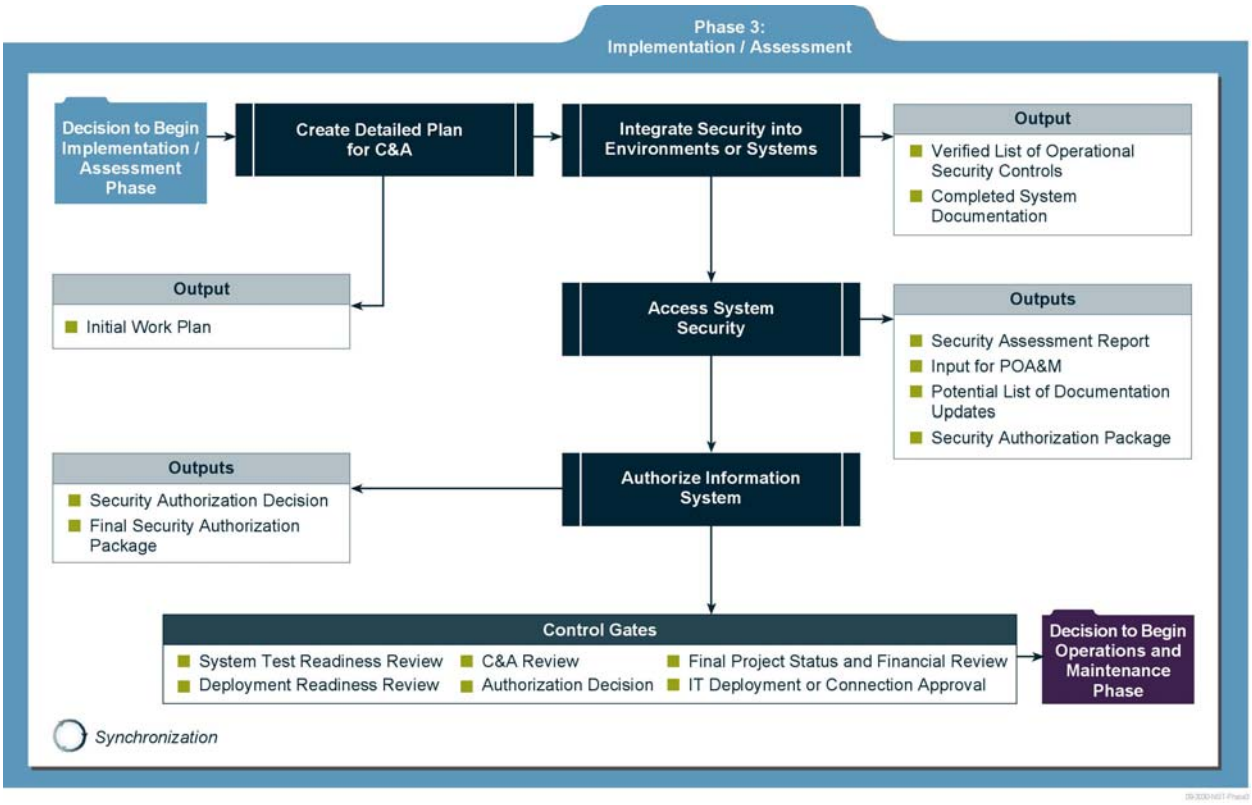

FIGURE 3-4. RELATING SECURITY CONSIDERATIONS IN THE IMPLEMENTATION/ASSESSMENT PHASE

3.3.1 Description

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.

3.3.2 Control Gates

General types of control gates for this phase may include:

- System Test Readiness Review
- C&A Review

3.4 SDLC Phase: Operations and Maintenance

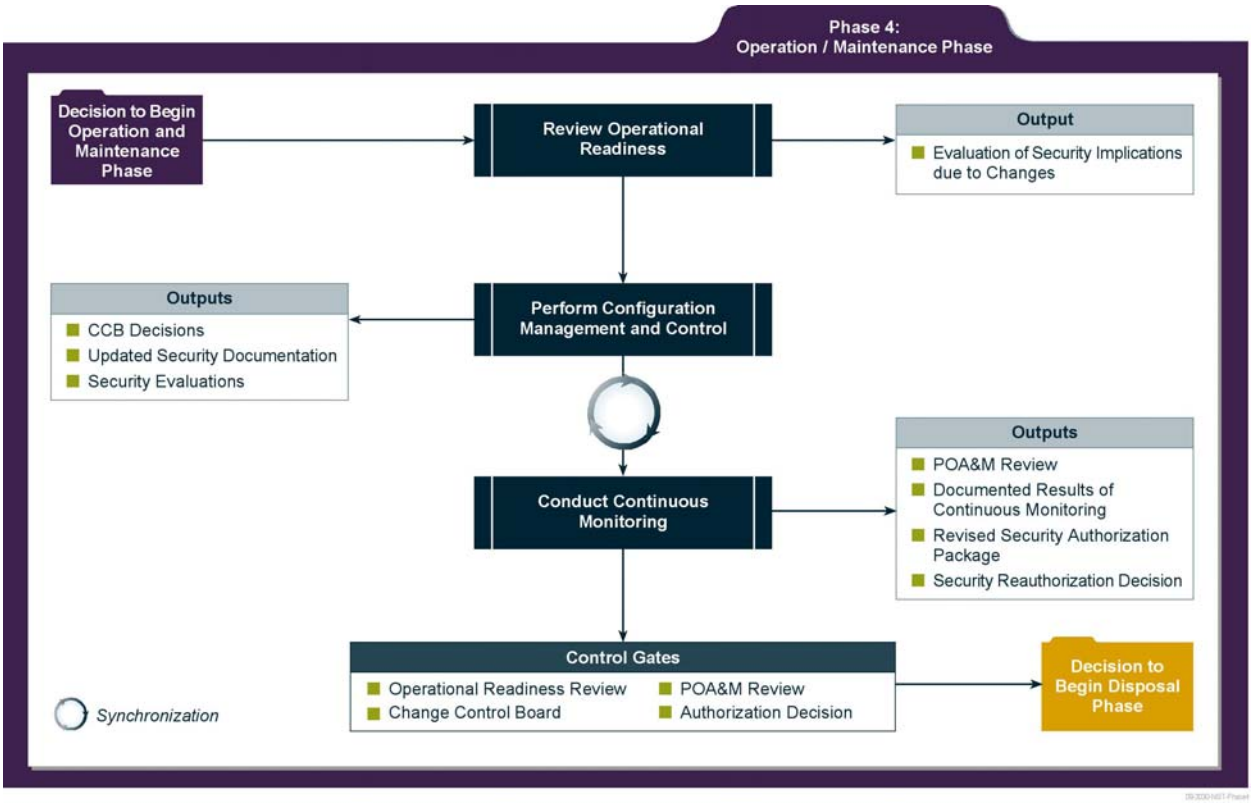

FIGURE 3-5. RELATING SECURITY CONSIDERATIONS IN THE OPERATIONS/MAINTENANCE PHASE

3.4.1 Description

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.

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.

3.5 SDLC Phase: Disposal

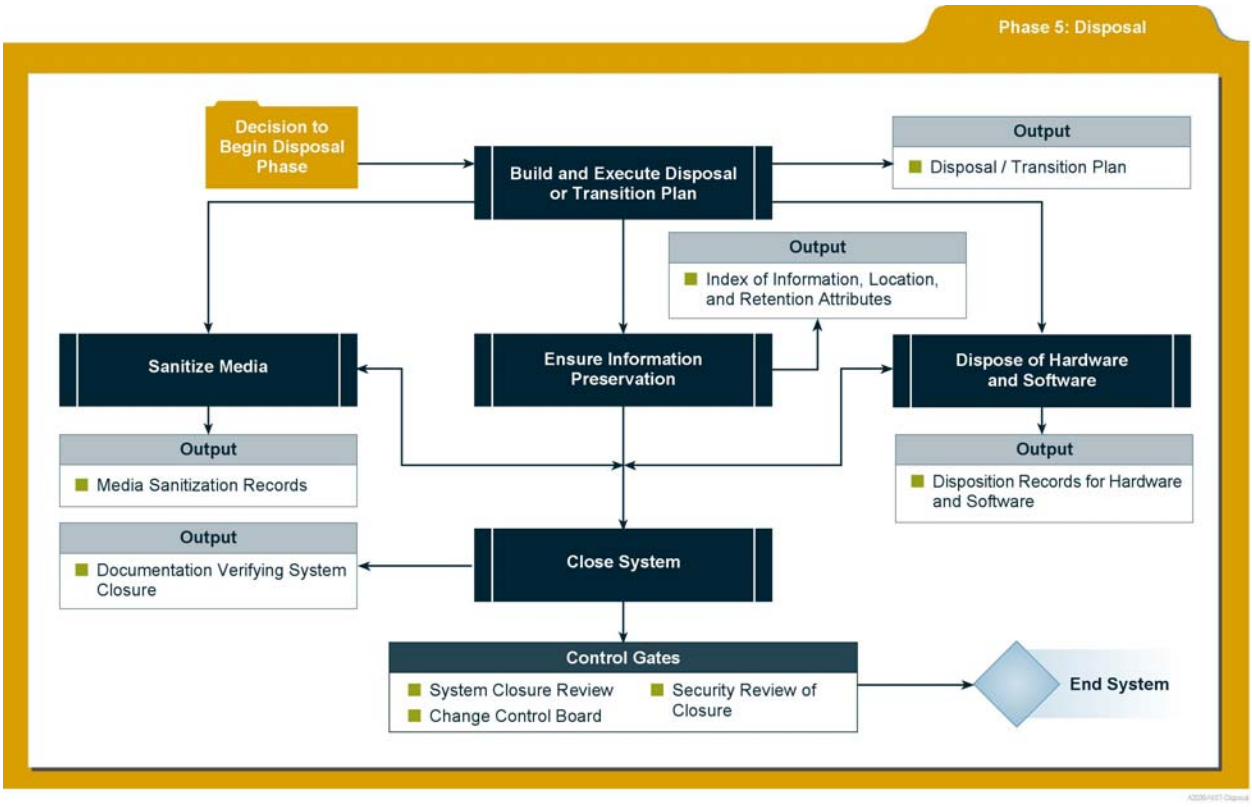

FIGURE 3-6. RELATING SECURITY CONSIDERATIONS IN THE DISPOSAL PHASE

3.5.1 Description

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.

Key security activities for this phase include:

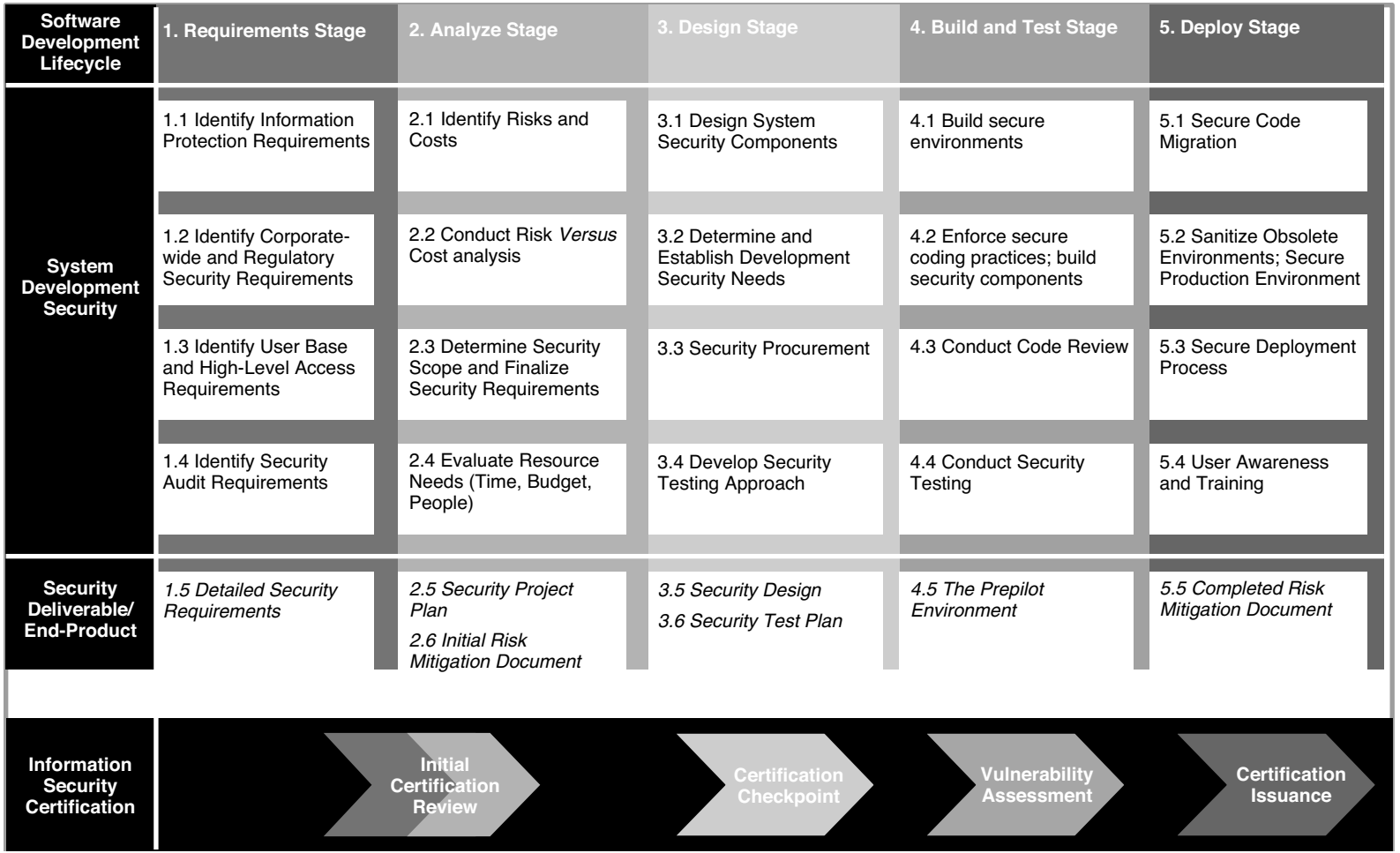

FIGURE 25.1 System development security framework.