Responsible Individual

- The policy champion and manager is called the policy administrator.
- Policy administrator is a mid-level staff member and is responsible for the creation, revision, distribution, and storage of the policy.
- It is good practice to actively solicit input both from the technically adept information security experts and from the business-focused managers in each community of interest when making revisions to security policies.
- This individual should also notify all affected members of the organization when the policy is modified.
- The policy administrator must be clearly identified on the policy document as the primary point of contact for additional information or for revision suggestions to the policy.

Schedule of Reviews

- Policies are effective only if they are periodically reviewed for currency and accuracy and modified to reflect these changes.
- Policies that are not kept current can become liabilities for the organization, as outdated rules are enforced or not, and new requirements are ignored.
- Organization must demonstrate with due diligence, that it is actively trying to meet the requirements of the market in which it operates.
- A properly organized schedule of reviews should be defined (at least annually) and published as part of the document.

Review Procedures and Practices

- To facilitate policy reviews, the policy manager should implement a mechanism by which individuals can comfortably make recommendations for revisions.
- Recommendation methods can involve e-mail, office mail, and an anonymous drop box.
- Once the policy Hs come up for review, all comments should be examined and management –approved improvements should be implemented.
- Most policies are drafted by a single, responsible individual and are then reviewed by a higher-level manager.
- But even this method should not preclude the collection and review of employee input.

Policy and Revision Date

- When policies are drafted and published without a date, confusion can arise when users of the policy's age or status.
- If policies are not reviewed and kept current, or if members of the organization are following undated versions, disastrous results and legal headaches can ensue.
- It is therefore, important that the policy contain the date of origin, along with the date(s) of any revisions.
- Some policies may also need a SUNSET clause indicating their expiration date.
- Automation can streamline the repetitive steps of writing policy, tracking the workflow of policy approvals, publishing policy once it is written and approved, and tracking when individuals have read the policy.
- Using techniques from computer based training and testing, organizations can train staff members and also improve the organization's awareness program.
- NetIQ corporation quotes that:
  - SOFTWARE THAT PUTS YOU IN CONTROL OF SECURITY POLICY CREATION, DISTRIBUTION, EDUCATION, AND TRACKING FOR COMPLIANCE
  - VigilEnt Policy Center makes it possible to manage security policy dynamically so that you can create, distribute, educate, and track understanding of information security policies for all employees in the organization.
  - It enables to keep policies up-to-date, change them quickly as needed, and ensure that they are being understood properly, all through a new automated, interactive, web-based software application.

Information Classification

- The classification of information is an important aspect of policy.
- The same protection scheme created to prevent production data from accidental release to the wrong party should be applied to policies in order to keep them freely available, but only within the organization.
- In today's open office environments, it may be beneficial to implement a clean desk policy

- A clean desk policy stipulates that at the end of the business day, all classified information must be properly stored and secured.

Systems Design

- At this point in the Security SDLC, the analysis phase is complete and the design phase begins – many work products have been created
- Designing a plan for security begins by creating or validating a security blueprint
- Then use the blueprint to plan the tasks to be accomplished and the order in which to proceed
- Setting priorities can follow the recommendations of published sources, or from published standards provided by government agencies, or private consultants

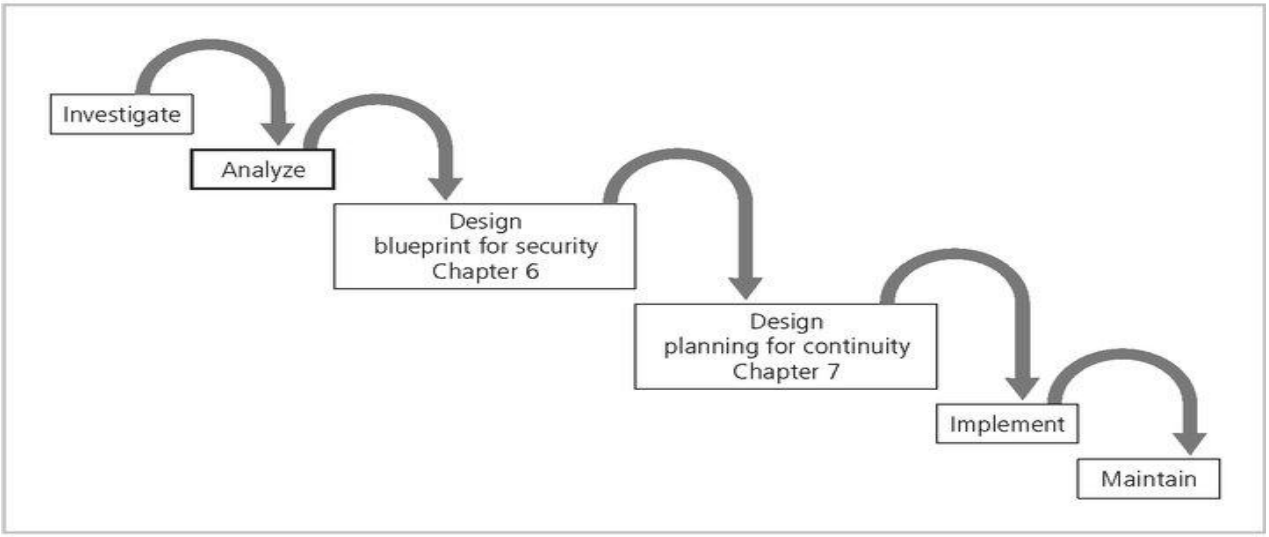

FIGURE 6-8 SecSDLC Methodology

1.3 Information Security Blueprints

- One approach is to adapt or adopt a published model or framework for information security
- A framework is the basic skeletal structure within which additional detailed planning of

the blueprint can be placed as it is developed of refined

- Experience teaches us that what works well for one organization may not precisely fit another
- This **security blueprint** is the basis for the design, selection, and implementation of all security policies, education and training programs, and technological controls.
- The security blueprint is a more detailed version of the **security framework**, which is an outline of the overall information security strategy for the organization and the roadmap for planned changes to the information security environment of the organization.
- The blueprint should specify the tasks to be accomplished and the order in which they are to be realized and serve as a scalable, upgradeable, and comprehensive plan for the information security needs for coming years.
- One approach to selecting a methodology by which to develop an information security blueprint is to adapt or adopt a published model or framework for information security.
- This framework can be an outline of steps involved in designing and later implementing information security in the organization.
- There is a number of published information security frameworks, including those from government sources presented later in this chapter.
- Because each information security environment is unique, the security team may need to modify or adapt pieces from several frameworks.
- Experience teaches you that what works well for one organization may not precisely fit another.
- Therefore, each implementation may need modification or even redesign before it suits the needs of a particular asset-threat problem.

ISO 17799/BS 7799

- One of the most widely referenced and often discussed security models is the Information Technology – Code of Practice for Information Security Management, which was originally published as British Standard BS 7799
- This Code of Practice was adopted as an international standard by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) as ISO/IEC 17799 in 2000 as a framework for information security.