Many System Development Life Cycle (SDLC) models exist that can be used by an organization in developing an information system. A traditional SDLC is a linear sequential model. This model assumes that the system will be delivered near the end of its life cycle. More complex models have been developed to address the evolving complexity of advanced and large information system designs.

A general SDLC includes the following phases: initiation, acquisition/development, implementation/assessment, operations/maintenance, and sunset (disposition). Each of these five phases includes a minimum set of tasks to incorporate security in the system development process. Including security early in the information SDLC will usually result in less expensive and more effective security than adding it to an operational system.

The following questions should be addressed in determining the security controls that will be required for a system:

- How critical is the system in meeting the organization’s mission?
- What are the security objectives required by the system, e.g., integrity, confidentiality, and availability?
- What regulations and policies are applicable in determining what is to be protected?
- What are the threats that are applicable in the environment where the system will be operational?

For more information:
http://csrc.nist.gov/SDLCinfosec
SDLCinfosec@nist.gov

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Computer Security Division
Information Technology Laboratory

Common Criteria for Information Technology Security Evaluation, Version 2.2
All References Available at http://csrc.nist.gov