CDC Unified Process

Project Management

Newsletter

Supporting A Common Project Delivery Framework

Volume 2 | Issue 6 | June 2008

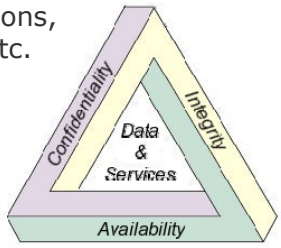
Security Issues that Project Managers at CDC Need to Address

Almost all projects use, or produce, some form of information technology and/or information. More often than not, this information needs to be protected through some form of security. Security planning is an integral part of the overall project life cycle and incorporates many different aspects to be considered when planning a project. However, ultimately what is being protected is the data produced by the system, the information that data is used to create, and in some instances, the decisions made based upon that information.

A security threat is something that jeopardizes the confidentiality, integrity, and/or availability of a system's data. Security risks result from such threats. Planning to address such items begins in the very early stages of a project's life with the identification of these security related threats and risks. Subsequent efforts work towards continually identifying new threats and minimizing identified security risks through the diligent planning and execution of risk mitigation strategies specifically developed to address each unique threat.

Security of information and associated information technology systems must to be considered when planning projects, developing applications, implementing systems, etc. To be effective, security must be planned for and designed into a system from the very beginning, reviewed periodically during the life of the project, and be maintained throughout the life of the system. As a result, planning early and incorporating security into all phases of a project's life cycle is often considerably easier and much less expensive than waiting until later project phases to consider it.

When considering the security of information systems, it can be decomposed in three main components that require consideration; hardware, software, and communications. Planning for how each of these areas is protected involves not only consideration of people, policy, practice, etc. but also budgetary considerations to provide for the review of they system, resource requirements, implementation of security solutions, ongoing security maintenance, etc.



The image to the right illustrates the ultimate goal of such efforts which is to support the confidentiality, integrity, and availability of system data. In the center of the image are the data and/or services that the security planning effort is attempting to protect. An information system has:

- *Confidentiality* - disclosure or exposure to unauthorized individuals or systems is prevented
- *Integrity* - data cannot be created, changed, or deleted without proper authorization
- *Availability* - information and the security controls used to protect it are functioning correctly when the information is needed

Items to avoid that will strengthen the security of a system and/or the information it produces include:

- Avoid designing and writing poor applications
- Perform regular system security assessments
- Use server side certificates (SSL)
- Hash passwords and encrypt sensitive data
- Utilize access control management, role based authentication, that grants only the minimum privileges required for what users need to do
- Do not mix sensitive and non-sensitive data
- Change default admin passwords
- Ensure the system is backed-up and encrypted
- Separate development, staging, and testing environments from production environments
- Do not use production data in a development environment
- Train users, developers, DBA's, etc. on security policies, procedures, etc.

To ensure proper security all CDC information systems are certified and accredited (C&A) based on the standards defined in NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. The CDC C&A process ensures that information systems are:

- Operating with appropriate management review
- Performing ongoing security control monitoring
- Submitted for reaccreditations before the end of the accreditation period (at least every 3 years) or when significant change to an information system or its environment has occurred

CDC's C&A process also involves making recommendations to enhance existing system security controls, and to implement additional security controls to mitigate system vulnerabilities discovered while conducting a risk assessment. Additional information on this and other security related items can be found on the Office of the Chief Information Security Officer (OCISO) website located on the CDC intranet.

For more information regarding the Project Management Community of Practice (PMCoP) or the CDC Unified Process (UP) please visit the CDC UP website located at http://www.cdc.gov/cdcup/.

Portions of the content of this newsletter were paraphrased from a presentation conducted by Kevin Lyday, CISSP, PMP during the May 2008 meeting of the CDC PMCoP.▮

Upcoming Project Management Community of Practice Meetings and Topics

- **Friday, June 27**
  PGO Processes
- **Thursday, July 24**
  Scrum in the Research Environment
- **Friday, August 22**
  General Management vs. Project Management
- **Friday, September 26**
  Records Management, PIA, and Classified Information
- **Friday, October 24**
  Facilitation – A Key to Project Success
- **Friday, December 5**
  Influence – A Critical Skill for Successful Project Managers

CDC Unified Process Working on HHS EPLC

The Department of Health and Human Services (HHS) Enterprise Performance Life Cycle (EPLC) Framework will provide HHS with a solid project management methodology that incorporates best government, and commercial, practices through a consistent and repeatable process, and provides a standard structure for planning, managing, and overseeing projects over their entire life cycle.

To successfully deliver the EPLC Framework, and its supporting project management artifacts, HHS is utilizing a collaborative development approach that allows all HHS operating divisions (OPDIV) to contribute to the development of EPLC artifacts. HHS has challenged the CDC, and other HHS OPDIV, by proposing an aggressive deadline for delivery of such artifacts. Scheduled are over one hundred artifacts to be created, critiqued, and finalized over the next few months. To successfully deliver on this challenge, HHS has requested that the CDC Unified Process (UP) Team take a lead role in the planning, facilitation, development, and delivery of this effort.

The CDC UP Team, in collaboration with HHS, and other HHS OPDIVs, have been aggressively working on the EPLC for several weeks and will be doing so for several more. The CDC UP Design Group has been an integral part of this effort. Made up of representatives from across the CDC the Design Group acts as CDC's voice in the EPLC development effort. Working collaboratively and utilizing technology to assist the process, the CDC UP Design Group has been meeting weekly to review new draft EPLC artifacts, share ideas, discuss points of interest, and make suggestions to HHS regarding final development of HHS EPLC artifacts.▮

Contact the CDC Unified Process Team

The *CDC Unified Process Project Management Newsletter* is authored by Daniel Vitek MBA, PMP and published by the National Center for Public Health Informatics.

For questions about the CDC UP, comments regarding this newsletter, suggestions for future newsletter topics, or to subscribe to the CDC UP Project Management Newsletter please contact the CDC UP Team at cdcup@cdc.gov

http://www.cdc.gov/cdcup/