Information Systems Development (ISD) and the National Institute of Standards and Technology (NIST) Risk Management Framework

TREO Talk Paper

Roberto Sandoval
The University of Texas at San Antonio
Roberto.sandoval@utsa.edu

Abstract

Information assurance (IA) has become an important aspect of information systems development (ISD) and cyber security. In large federal government organizations there are guidelines in place to ensure that information and network systems are secure. Federal government organizations include all Military Services, Intelligence communities, National Research Laboratories, Financial, Medical, and Transportation agencies. The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) Special Publication (SP) 800-53 is one of the most recent mandated guidelines for cyber security and information assurance in large U.S. federal government organizations. The implementation of the NIST’s RMF presents a unique challenge in that the focus is not only on upgrading the security posture of large organizations but also includes meeting all of the criteria specified in the RMF for security controls for sensitive information in both the physical and digital sense. This ISD effort may require a new approach for software development and integration with legacy systems that could include the use of commercial-off-the-shelf (COTS) products as well as dedicated project teams in order to ensure all of the RMF requirements are met. This study will investigate the knowledge sharing of information and group interactions that will be required of the ISD teams in order to ensure proper implementation of the NIST’s RMF SP 800-53 in large U.S. government and federal organizations.