

SFA Risk Assessment Support

Task Overview

The enforced requirement for all SFA systems to complete Risk Assessments came as a result of last year's GISRA review. KPMG Consulting responded to this requirement by assisting the SFA security office organize and respond to ED CIO's mandated response to GISRA. The effort included numerous interactions with ED CIO, attending ED CIO risk assessment training, creating SFA's risk assessment methodology, briefing SFA contractors and staff on this methodology, and supporting the business channels complete their assessments by the April 2002 deadline. Our support has been successful to date, positioning SFA in a favorable position for all systems to complete the risk assessments by the SFA CIO's April 8 deadline.

Task Details

KPMG Consulting's risk assessment support to the SFA Security and Privacy team and the business channels has taken many shapes. From creating templates to training contractors about SFA's risk assessment methodology, our support has been broad and thorough. We began our response to the risk assessment requirement by reviewing and deciphering the Department's IT Security Risk Assessment Guide. The guide, while appropriate for a Department level document, did not contain sufficient detail for SFA's purposes. The SFA system's environment possesses several inherent challenges that we needed to ensure the risk assessment methodology would take into account. To accomplish this task we broke down the Department's guidance, analyzed its requirements, created language and matrices that would clarify certain requirements, and finally briefed our interpretation to ED OCIO and their contract support. KPMG Consulting's methodology was approved, giving our team one week to finalize our guidance, create training material, and develop a training program.

On February 7, we presented SFA's risk assessment methodology to numerous SFA personnel, contract support staff, and their subcontractors. The training session included a PowerPoint briefing, a risk assessment matrix, and a risk assessment template/guide book. The session lasted roughly 90 minutes, leaving the majority of the teams more clear as to their six-week mission. We responded to questions and concerns during and after the session, provided more detail where necessary, and gave examples where some were still unsure. Overall, the training session was well received and recommendations were made for similar sessions on other security topics, such as security plans and the certification and accreditations process.

Additional support requirements have and will continue to surface until the project is completed. For example, each system will need independent contract support to perform the risk assessment. KPMG Consulting was asked to provide an analysis of the factors influencing the costs to perform the risk assessment. Our analysis described, in general, the cost factors that may influence a risk assessment and then provided three scenarios to further explain these cost factors. The analysis has been used to provide the initial framework for assessing the eventual costs of performing these risk assessments to SFA.

Task Status

KPMG Consulting will continue to support the risk assessment task until its completion in April. At such time, we will shift the majority of our support to the June deadline for updating every SFA System Security Plan.