

Risk Assessment Analyses

Task Overview

As part of FSA's response to last year's GISRA findings, each IT system classified as either a Major Application or General Support System was required to conduct an independent risk assessment. These assessments resulted in a risk assessment report, which included a general description of the system's characteristics, its interactions with other systems, and a prioritized list of the inherent risks within the system. While several systems already had current risk assessments, about half of FSA's systems used the Department's contractor as the assessor. In order to ensure the validity and completeness of the assessments, the Security and Privacy team asked KPMG Consulting to review the Departmentally-contracted assessor risk assessment reports and critique them for inaccuracies, clarifications, or corrections. Additionally, the PEPS SSO requested some final assistance to complete the PEPS risk assessment.

Task Description

As stated in our June 15 deliverable, several of FSA's General Support Systems and Major Applications had recently completed a risk assessment and were waived by the Department from requiring another assessment. Three systems, Direct Loan Origination System (DLOS), Direct Loan Servicing System (DLSS), and Postsecondary Education Participants System (PEPS), made arrangements with other contractors to complete their assessments. DLOS and DLSS finished their assessments with the suggestions we provided, while PEPS had some additional concerns. We responded quickly to these concerns, and the PEPS risk assessment was completed soon thereafter.

Of the remaining systems, nine decided to use the Departmentally contracted assessor as their independent provider. Upon receipt of the risk assessments, FSA requested that we review these assessments applying the same criteria used for DLOS, DLSS, and PEPS so as to have a baseline comparison of the different assessments. Unfortunately, we would not be able to provide suggestions for improvement or clarification for these assessments, as the Department had decreed that no dialogue was allowed after the assessments' completion.

The analysis of the Departmentally contracted risk assessments found them woefully inadequate. Given the amount of time and resources allocated to their completion, the assessments found comparatively fewer findings than the independent risk assessments, contained numerous mistakes or confusing remarks, and provided little value to each system's owner, system's manager, and system's security officer.

Task Status

After reviewing the assessments, we quickly moved on to assisting the SSO's interpret the results and suggest ways to implement corrections. Results of this assistance can be found in the corrective action plan assistance provided in the GISRA assistance, a separate section of this deliverable. Currently, FSA is investigating the quality of the Departmentally contracted assessments.