TekNirvana
Making technology bliss a reality

Case Study

Cybersecurity and FISMA Information Systems Security Officer (ISSO) support

End Client

A Civilian Federal Agency

The Challenge

The objectives and purpose of this IT project was to support the prime vendor in providing Information Systems Security Officer (ISSO) support to a civilian Federal agency on over 45 major FISMA reportable systems and over 45 minor systems. A formalized ISSO function did not previously exist at the agency and part of our task was to help establish the function and procedures for the newly created ISSO organization.

Our Services

- ✓ Strategy and IT Enablement → IT Program and Project Management
- ✓ Strategy and IT Enablement → Cybersecurity Solutions

Our Approach and the Results Achieved

TekNirvana was engaged by the prime vendor to provide overall program management support to the ISSO contract. In the program manager role, TekNirvana works with the onsite project manager and eight full time ISSO staff to provide ISSO services for over all of the FISMA reportable systems (Unclassified and Classified [TS, TS/SCI]) that are in scope. We work closely with the end client and the prime to ensure that our team helps ensure that these systems are in full compliance with the NIST Risk Management Framework (RMF) as per NIST Special Publication (SP) 800-37. Within the first three months we created a Security Control Test Strategy document based on NIST continuous monitoring guidance (NIST SP 800-137) that identifies controls that are tested on an ongoing and annual basis. For each system that we provide ISSO services for, we perform an annual contingency plan test, contingency plan updates, a Business Impact Analysis (BIA), a Privacy Threshold/Impact Analysis (PTA or PIA), and comprehensive non-privileged user account review and recertification. We perform a privileged user account review on a monthly basis and review audit logs on a weekly basis. Activities that are performed on an ongoing basis include POA&M management, System Security Plan (SSP) updates and Security Control Testing as outlined in the Security Control Testing strategy. We have created detailed desktop procedures for each activity (such as POA&M Management, Privileged User Account Review, etc.) and have trained each ISSO on these to ensure that all ISSO activities are performed consistently and in accordance with contract requirements.