

National Institutes of Health, Office of Research Services (NIH/ORS) Case Study: Certification and Accreditation Tool (CAT) Document Repository

Challenge

How to produce, store and actively manage required documentation that ensures compliance with Federal, Departmental and NIST Standards, while at the same time providing an automated mechanism that allows the data managers to capture and be updated on rapidly changing IT environments.

Background

The National Institutes of Health, Office of Research Services (ORS) provides a comprehensive portfolio of services to support the biomedical research mission of the NIH. Examples of these services include: laboratory safety, police and fire departments, veterinary resources, the NIH Library, events management, travel and transportation, services for foreign scientists, and programs to enrich and enhance the NIH worksite.

Solution

Develop a tool that captures all relevant data needed to produce documentation required for the environment, store it securely, and populate pre-approved templates with the captured system-unique information.

OnPoint was contracted to assist the NIH/ORS Information Systems Security Officer (ISSO), Vicky Ames, in the production of 20 Certification and Accreditation (C&A) packages for their most critical systems. Recognizing the sensitivity and quantity of data contained in a typical C&A package, OnPoint and NIH researched several commercial off the shelf (COTS) solutions. Requirements that were evaluated included the ability to produce C&A packages, and the flexibility to easily add additional documentation as needed. After reviewing the market, Ms. Ames noted, "The COTS solutions, while certainly capable of producing the C&A packages, were very expensive and somewhat restrictive in nature for our unique needs at the NIH. We had specific Departmental and Agency requirements to meet, and we needed a solution that could easily be modified to fit our environment."

To meet and exceed the NIH requirements, OnPoint architected and designed the Certification and Accreditation Tool, referred to as "CAT", and provided NIH with a customized version for their unique environment. The customization included the development of several document templates, all of which were then vetted by the NIH Center for Information Technology (CIT) and the Office of the Chief Information Officer (OCIO), to ensure a compliant C&A package.

The following document templates were created by the OnPoint team, in conjunction with the ISSO:

- System Security Plan
- Configuration Management Plan
- Contingency Plan / Continuity of Operations Plan (COOP)
- Disaster Recovery Plan
- Interconnection Service Agreements
- Certifying Authority (CA) Recommendation Statements
- Full and Interim Accreditation Memos

- Plan of Action and Milestone (POAM)
- Privacy Impact Assessment
- Rules of Behavior
- Security Self Assessment
- Security Testing and Evaluation Plan

CAT is a web-based tool, developed in ASP .NET, using Microsoft SQL in the backend database to store the data. The tool was developed to produce NIST compliant C&A packages, aiding NIH with FISMA Compliance. Utilizing the tool, OnPoint was able to meet very strict deadlines imposed by NIH and Health and Human Services (HHS).

“We estimate that the CAT Tool cut the time to prepare these documents almost in half, allowing us to meet our aggressive deadlines and realize significant cost savings. Having the templates pre-approved as compliant provided us with a comfort level in the quality of our C&A packages. Additionally, we now have the data saved in a secure central location, allowing our system owners and managers an easy way to keep the security documentation up to date in our ever-changing IT environment. I believe that having this data archived, if properly updated, will yield significant time and costs savings during the continuous monitoring phase as well as during future C&A efforts at NIH/ORS,” stated Ms.Ames.

Secondary Benefit – Global document repository

While successful in producing compliant C&A packages, a secondary - but equally important - use was found for the CAT tool. CAT provides a globally accessible document repository for all mission-critical documentation at ORS, providing system owners, security administrators and policy managers with the ability to keep the documents up to date with the most current data.

Many departments, agencies and offices create documents like System Security Plans, Disaster Recovery Plans and Continuity of Operation Plans to be used within the IT environment. The challenge managing these documents is that they only represent a “snapshot in time”, showing the environment as it existed when the documents were created. IT environments are constantly changing, often on a daily or weekly basis. As they do, the changes render these documents as obsolete unless they are updated.

It is costly and time-consuming to re-create documents so that they reflect the current IT environment. As change inevitably occurs, quite often several of documents require updating with the same information. Most of the documents today are generated in Microsoft Word, so managers are forced to manually perform global “find and replace” efforts on each document every time a significant change occurs.

CAT provides the managers with an easy mechanism to make global changes across all relevant system documents by simply capturing the change in one field. The change is then applied to each of the documents stored in CAT as appropriate.

For example, if a system name or IP address changes, the manager would simply find the appropriate field in CAT and make the change one time. Subsequently, as new documents are produced, the change would be applied to each document in the appropriate area.

“Having the ability to keep our COOP, Disaster Recovery Plans and System Security Plans current is of tremendous value to NIH and any large agency. We find ourselves proactively managing our risk, rather than scrambling to meet the deadlines. In the dynamic world of an ISSO, or any IT Manager, any tool that can assist us in maintaining a proactive security posture is worth its weight in gold,” stated Ms.Ames.