VOLANT ASSOCIATES

Case Study D

AUTOMATING ACCREDITATION AND AUTHORIZATION

Since January 2019, Volant has been working with the government to streamline a government customer's security accreditation process. Like in most government organizations every application and system must be formally accredited based on the selection and specification of security controls as defined by the NIST Risk Management Framework (RMF) described in NIST Special Publication (SP) 800-37 Revision 2. While the NIST SP 800-37 documentation defines the overarching risk management approach, government agencies are afforded the opportunity to implement security controls in a manner consistent with their unique mission needs. Based on Volant's consistent track record of delivering successful technical solutions for this customer, the Volant team was selected to provide an innovative approach to address, contribute, and solve key elements of their accreditation process.

> **Volant's technical approach in leveraging Opencontrol (open source security standard) is a paradigm shift and completely changes how a developer implements a system and how an organization verifies those security controls.**

The Challenge

Currently, security accreditation for a typical application or system at this customer's agency can take a year to 18 months to complete. Volant is leveraging years of experience in automating software development tools and processes and directly applying this experience to help streamline and automate the accreditation process.

Like many organizations, this customer uses the Risk Management Framework (RMF) to manage and monitor the security related elements of a system or capability. There are six key steps for the RMF process, as listed below.

Risk Management Framework (RMF):

01 **Categorize System**

02 **Select Controls**

03 **Build System**

04 **Test System**

05 **Accredit System**

06 **Continuous Monitoring of System**

For this initial work, Volant addressed and focused on Steps 1 through 4 in the RMF process. Per customer's guidance, key emphasis was on the transition from RMF Step 3 to 4, namely verifying that security controls were properly implemented. However, Volant also delivered and provided a foundation for Steps 1 through 3, namely, to help the developer categorize, select controls, and to build the system. Currently, verifying security controls is labor intensive and in most cases is a manual process. The work from this project is laying the foundation that will reduce the time to verify security controls and thereby shorten the overall time to complete the security accreditation process.

Our Approach

After careful review of the government's requirements, Volant saw an opportunity to provide efficiencies to the customer by leveraging an innovative approach to accreditation based on an open source standard called "Opencontrol." Opencontrol was developed by a group of technology and security experts with a specific focus to streamline the accreditation process by creating an open standard to support compliance. The standard supports compliance for any industry, whether government or commercial.

The standard supports compliance for any industry, whether government or commercial. The Opencontrol approach can be used for the entire RMF process.

The Opencontrol approach is a paradigm shift and completely changes how a developer implements a system and how an organization verifies those security controls. For example, let's compare what is done today and how Opencontrol is used to address and implement security compliance:

Current Model for Implementing and Verifying Security Controls:

- Worst, but Typical Scenario
  - In many instances, a developer would build a system without any initial idea of security controls needed. Or, the developer would guess what security controls they should implement.
  - After building the system, the developer would then engage with security representatives from the hosting organization.
  - After hosting organization reviewed the system being built, the developer would than make corrections or changes to the system to ensure compliance.
  - After developer revised the system, the hosting organization would again test and verify to ensure the capability was in compliance.
- Best Current Scenario
  - Developer determines a category or certification level of the system being built. Based on the category of the system, a number of security controls are identified to be addressed and possibly implemented.
  - Once an initial set of controls are identified, the developer works with security representatives to refine and determine the final security controls that are required to be implemented.
  - After the developer has a final set of security controls, the system is built.
  - After the system is developed, the hosting organization must verify the developer has implemented the required security controls.

Opencontrol Approach to Implementing and Verifying Security Controls:

- An initial setup by the hosting organization is created and a Framework/Library is established before any actions from a developer are taken:
  - The hosting organization develops predetermined templates, or in Opencontrol language, "components." These components predefine re-usable parts that can be used by a developer.
  - Opencontrol components include elements like organizational policies, other predefined systems, typical software, and other software elements.
  - Each component has a set of pre-determined set of security controls that apply to that component. This dramatically streamlines the overall accreditation process.
  - The Opencontrol framework also provides the means for verifying and testing security controls that have been implemented. Developers can rely on pre-determined security control guidance provided by NRO. In addition, the hosting organization can rapidly validate since these controls will likely have defined testing and verification tools set up in advance.

- Developer determines a category or certification level of the system being built.
- The developer, as much as possible, selects pre-determined Opencontrol components that the hosting organization has provided. The more existing components that are used, the less the developer has to do. In many cases, a hosting organization will determine certain security elements do not have to be addressed by the developer since prior arrangements for addressing the controls has already been determined and implemented.
- After the developer builds the system, the same Opencontrol elements can be used to verify and test. In many cases, the Opencontrol components can be tested and verified automatically.

In summary, Volant's technical approach provides the government with the means to significantly reduce the time to complete the accreditation compliance process. Volant provides innovation, while simultaneously adhering to well established RMF processes and controls by demonstrating the value of leveraging an open source standard called Opencontrol.

As our customer creates and establishes more security library components, the accreditation process will continue to become shorter. Not only does the Opencontrol approach being implemented by Volant help a developer effectively and efficiently build a system, it is also the open source standard that enables a framework for rapid and automated security testing and verification by the hosting organization.

For more information contact us at **(571) 210-0030** or **info@volantco.com**