Aligning security risk management and compliance activities with the broader adoption of cloud technology and the exponential increase in the complexity of smart systems leveraging such cloud solutions, has been a challenging task to date. Additionally, the proliferation of container technology employed in cloud ecosystems for enhanced portability and security, compels organizations to leverage risk management strategies that are tightly coupled with the dynamic nature of their systems.

NIST's Open Security Controls Assessment Language (OSCAL) provides a standardized set of XML-, JSON- and YAML-based formats for use by authors and maintainers of security and privacy control catalogs, control baselines, and system security plans. These OSCAL formats provide a normalized expression of security requirements across standards, and a machine-readable representation of security information from controls to system implementation, supporting automated security assessment. This bridges the gap between antiquated approaches to IT compliance and lays a foundation for innovative technology solutions. This talk will present information on the current status of OSCAL, the benefits of using OSCAL to support controls-based risk assessment, and the next steps for the project.

About the Speaker

David A. Waltermire

Lead Standards Architect, Security Automation Program, National Institute of Standards and Technology (NIST).

David Waltermire is the Lead Standards Architect for the Security Automation Program at the National Institute of Standards and Technology. He is a significant contributor to the National Vulnerability Database (NVD) and leads the Security Content Automation Protocol (SCAP), Continuous Monitoring and many other security automation projects. He has worked as a Security Consultant advancing security automation capabilities within the government sector. His background is in systems and network operations for Internet service providers and also working as a Software Engineer designing and developing distributed systems. His research experience includes incident handling, continuous monitoring, vulnerability identification, anomaly detection, and data analysis and modeling techniques.