Changing How We Address Cybersecurity and Compliance

Are We Ready?

Organizational security and policy compliance is by no means fun, often requiring teams to produce 100's of pages of artifacts for each system, then repeating that process every 2-3 years. There have been several efforts over the years to shrink the time to compliance and authorization with process models, tools, and techniques, but they have not significantly reduced the cost and time to achieve compliance.   As the nation continues to face existential Cybersecurity threats, the need for organizations to secure sensitive information is a strategic priority. In June of 2021, the National Institute of Standards and Technology (NIST), released the Open Security Controls Assessment Language (OSCAL). OSCAL is a standardized, data-centric framework for the documentation and coordination of information required to meet many current compliance frameworks.

What Should I Know About OSCAL?

With organizations moving more business operations and data to cloud services providers, meeting regulatory compliance is becoming increasingly complex and expensive. For public sector organizations, managing compliance across 100's of information systems requires skilled labor and deep expertise in cybersecurity and privacy to support ongoing assessments within a constantly changing threat landscape.
OSCAL introduces a standardized approach for management of compliance activities with a new, machine-readable language for communicating security and privacy controls. By doing this, security authorization and assessment activity has been organized into structured data that describes the behavior of a system. Through the adoption of OSCAL, organizations can begin to:

- Decentralize the creation of security controls and documentation to the developers and engineers at the time of system architecture and engineering, promoting a secure by design culture
- Assess compliance control implementations across multiple information systems and components
- Support multiple regulatory frameworks, simultaneously
- Automate the generation of compliance documentation
- Automate processes and human driven activities such as validation of a system security plan
- Support continuous authorizations by decreasing assessment-related labor and automation of continuous monitoring capabilities
- Bridge legacy and emerging processes by converting from OSCAL to familiar formats such as Word or Excel

How Can I Take Advantage of OSCAL Today?

Organizations looking to accelerate compliance can take advantage of OSCAL today by shifting-left compliance activities earlier in their Software Development Lifecycle (SDLC) process and by supporting the creation of OSCAL artifacts. To facilitate that journey, Easy Dynamics has developed an OSCAL Adoption Framework and recommends a comprehensive 6-step process, from identifying a candidate compliance system to educational and change management efforts, resulting in the digital transformation of an organization's ability to develop and maintain highly reusable compliance artifacts. Our framework also leverages our open-source projects that accelerate adoption of OSCAL and facilitates simplified engagement of non-technical team members into the shift-left compliance workflow.

What Can OSCAL Deliver?

The organizations that will benefit most from the OSCAL framework are those that are already thinking about security as their systems are being built. The framework itself is designed to adapt compliance management into smaller reusable components familiar to modern software design methodologies. By creating a secure-by-design approach to compliance, architects and engineers are encouraged to consider how security and privacy controls are embedded into each component, how they should be assessed and therefore how to ensure active compliance, or continuous authorizations, is more readily achieved. By making this a machine-readable framework, the system is able to embed this thinking info these reusable components to increase speed to value and reduce cost from refactoring for security after the initial design is complete.

This approach is designed by NIST to provide continuous assessment of security compliance at the component level which reduces the amount of custom work, the time to create unique compliance documentation, and the time to detect and respond to changes in operations that could result in a security weakness. The result is a system which is more secure, resilient and cost effective.

How Can Easy Dynamics Help Me?

At our core, Easy Dynamics has been helping clients adapt to change, and OSCAL is no exception. We have been a partner with NIST and the Federal Government in helping to develop this technology. By making our tools open source, we are demonstrating our commitment to both the technology and the success of the government to reduce cost and increase security using OSCAL. Our team of subject matter experts can help you chart your path as well. This technology, like others that we have helped bring to market, will be an important achievement in creating a more secure, resilient, and cost-effective infrastructure for the Federal Government and we can help you bring that to your organization.

For more information, please contact Ray Gauss and Adam Mouw.

Contact us today

Ray Gauss
Director of Innovation
rgauss@easydynamics.com
(301) 717 - 4205

Adam Mouw
VP of Business Development
amouw@easydynamics.com
(703) 217 - 9329

Who We Are

Easy Dynamics has been at the forefront in developing identity solutions for the federal government since our inception in 2007. Whether it's focusing on emerging technologies like NIST's OSCAL or helping clients move their workloads to a cloud centric model – Easy Dynamics brings a culturally unique blend of talent and strategic leadership to help government realize its objective of secure, efficient, and effective delivery of service to its constituents.