Virtual Room #1

Hosted By: Alexander Stein, NIST ITL CSD 773.03

Disclaimer: Portions of the event may be recorded and audience Q&A or comments may be captured. The recorded event may be edited and rebroadcasted or otherwise made publicly available by NIST. By attending this event, you acknowledge and consent to having your conversation recorded.
It’s challenging to manage all those controls in my security program.

Policy makers and baseline authors:

I manage information security policies for my organization. It’s challenging to maintain all the sets of the controls and disseminate them to everyone in my organization.

System engineers and security pros:

I develop and/or operate the systems in my organization. I need to stay up to date with my organization’s policies in a structured way, double-checking that my systems meet and implement those requirements.
But automation is hard!
Ok, so how I start with OSCAL?
With the official NIST RMF catalog!

ITL/CSD/OSCAL Team
3rd OSCAL Workshop
Step 1: Set up a repo, test importing the NIST catalog with one control.
Step 2: Just import everything.
Step 3: Import everything, but delete some controls.
Step 4: Import controls, but set organization’s required parameters.
Step 5: Import everything, but make some custom edits.
Step 6: NIST makes upstream updates, pull those in.
Step 7: NIST makes upstream updates, ignore some of them.
Step 8: Make it viewable, not just automatable.
And we’re done:

https://github.com/ImportantFederalAgency/catalog
OK, I’m inspired. What should my org do in the next six months?

Study and experiment with machine-readable OSCAL control catalogs.
OK, I’m inspired. What should my org do in one year?

Research the market, RFP, develop, and/or acquire OSCAL catalog management tools.
OK, I’m inspired. What do my org do in two years?

Deploy an OSCAL catalog management tool, pull catalogs from upstream, push changes inside your org.
Questions? Feedback?

https://pages.nist.gov/OSCAL/contact/