Rules, What Are They Good For? Absolutely Something!

National Institute of Standards and Technology
U.S. Department of Commerce

ITL/CSD/OSCAL Team

Model Meeting 20220121

What is a rule?

From the textbook:

An element that holds **check references** and may also hold **remediation information**.

- **NIST CSRC Glossary**

For OSCAL, a rule is:

a **condition to check** [1]

possible **evaluation methods** [0 to ∞]

links to what it supports [0 to ∞]

But where is the remediation info?

What about rule results?

Stay tuned for OSCAL#1059.

But wait, that's just [RMF] Assessment stuff!?

National Institute of Standards and Technology
U.S. Department of Commerce

ITL/CSD/OSCAL Team

Model Meeting 20220121

Why rules?

Wait, don’t we already have that!?

Playbooks, runbooks, team checklists

SCAP, STIGs, CIS Benchmarks, config baselines

“Limit the number of concurrent sessions for each organization-defined account three (3) sessions for privileged access and two (2) sessions for non-privileged access.” (AC-10)

→ Server instances

→ Managed services

→ Network control plane

→ Cloud infrastructure at the “account level”

The answers to these questions are not given in isolation but rather in the context of a risk management process for the organization that identifies, assesses, responds to, and monitors security and privacy risks arising from its information and systems on an ongoing basis.[8] The security and privacy controls in this publication are recommended for use by organizations to satisfy their information security and privacy requirements. The control catalog can be viewed as a toolbox containing a collection of safeguards, countermeasures, techniques, and processes to respond to security and privacy risks. The controls are employed as part of a well-defined risk management process that supports organizational information security and privacy programs. In turn, those information security and privacy programs lay the foundation for the success of the mission and business functions of the organization.

It is important that responsible officials understand the security and privacy risks that could adversely affect organizational operations and assets, individuals, other organizations, and the Nation.[9] These officials must also understand the current status of their security and privacy programs and the controls planned or in place to protect information, information systems, and organizations in order to make informed judgments and investments that respond to identified risks in an acceptable manner. The objective is to manage these risks through the selection and implementation of security and privacy controls.

1.1 PURPOSE AND APPLICABILITY

This publication establishes controls for systems and organizations. The controls can be implemented within any organization or system that processes, stores, or transmits information. The use of these controls is mandatory for federal information systems[10] in accordance with Office of Management and Budget (OMB) Circular A-130 [OMB A-130] and the provisions of the Federal Information Security Modernization Act[11] [FISMA], which requires the implementation of minimum controls to protect federal information and information systems.[12] This publication, along with other supporting NIST publications, is designed to help organizations identify the security and privacy controls needed to manage risk and to satisfy the security and privacy requirements in FISMA, the Privacy Act of 1974 [PRIVACT], OMB policies (e.g., [OMB A-130]), and designated Federal Information Processing Standards (FIPS), among others. It accomplishes

```
        insecure-bind-address is found and set to 'localhost' in th
        this is a finding.</check-content>
    </check>
  </Rule>
</Group>
<Group id="V-242389">
  <title>SRG-APP-000033-CTR-000100</title>
  <description>&lt;GroupDescription&gt;&lt;/GroupDescription&gt;</d
  <Rule id="SV-242389r712523_rule" weight="10.0" severity="medium">
    <version>CNTR-K8-000350</version>
    <title>The Kubernetes API server must have the secure port set.
    <description>&lt;VulnDiscussion&gt;By default, the API server w
      rightfully called the secure port, port 6443. Any requests to
      authentication and authorization checks. If this port is disal
      to the host on which the master is running has full control o
      encrypted traffic. Open the secure port by setting the API se
      value other than
      "0".&lt;/VulnDiscussion&gt;&lt;FalsePositives&gt;&lt;/FalsePo
    <reference><dc:title>DPMS Target
        Kubernetes</dc:title><dc:publisher>DISA</dc:publisher><dc:t
        Target</dc:type><dc:subject>Kubernetes</dc:subject><dc:iden
    <ident system="http://cyber.mil/cci">CCI-000213</ident>
    <fixtext fixref="F-45622r712522_fix">Edit the Kubernetes API Se
      /etc/kubernetes/manifests directory on the Kubernetes Master
      --secure-port to a value greater than "0".</fixtext>
    <fix id="F-45622r712522_fix"/>
    <check system="C-45664r712521_chk">
      <check-content-ref href="Kubernetes_STIG.xml" name="M"/>
      <check-content>Change to the /etc/kubernetes/manifests direct
        Node. Run the command: grep -i secure-port * If the setting
        is not configured in the Kubernetes API manifest file, this
    </check>
  </Rule>
</Group>
```

National Institute of Standards and Technology
U.S. Department of Commerce

ITL/CSD/OSCAL Team

Model Meeting 20220121

How to make and use rules?

Goals

Summarize conditions in structured data

with flexible methods (automated manual)

without vendor lock-in

Adding rules where we need

component-definition system-security-plan

Adding rules where want

assessment-plan assessment-results plan-of-actions-and-milestones profile catalog

Model

```
rule [0 to ∞]
    uuid [1]
    name [0 to 1]
    title [1]
      description [1]
         condition [0 to 1]
        condition-evaluator [0 to ∞]
           uuid [1]
           name [0 to 1]
           type [0 to 1]
              prop [0 to ∞]
              link [0 to ∞]
                 href
                 rel: dependency
        prop [0 to ∞]
           name: supports
```

Examples and Samples

Fully automated

CSP offers a secure PaaS for agency systems and want to provide rules for service hardening and self-assessment.

ocpv4-example-component-definition.xml

Semi-automated

Lead DevSecOps Engineer of an agency engineering org defines guidelines on how to review audit logs in their centralized logging SIEM.

semi-automated-log-review.xml

Manual

The Office of the CISO establishes rules for engineering teams to follow account management and audit logging policy.

agency-ciso-overlay-component.xml

Open Questions

Overlap & relevance to SAP&SAR models

National Institute of Standards and Technology
U.S. Department of Commerce

ITL/CSD/OSCAL Team

Model Meeting 20220121

How will we do grouping for rules?

National Institute of Standards and Technology
U.S. Department of Commerce

ITL/CSD/OSCAL Team

Model Meeting 20220121

Data architecture for linking

National Institute of Standards and Technology
U.S. Department of Commerce

ITL/CSD/OSCAL Team

Model Meeting 20220121

Rules are good for component definitions and SSPs, but are they good for everything?

National Institute of Standards and Technology
U.S. Department of Commerce

ITL/CSD/OSCAL Team

Model Meeting 20220121

How can you help?

We want feedback re

current use cases (or recommend others)

the model structure

example data for automated rules

feedback on open questions

GitHub:
github.com/usnistgov/OSCAL/issues/1058

Gitter:
gitter.im/usnistgov-OSCAL/Lobby

Email:
oscal-dev@list.nist.gov