Department of Justice
Office of the Chief Information Officer

Cyber Security Assessment & Management (CSAM)

Planning for Implementing SP 800-53, Revision 5

May 26, 2021

Cybersecurity Services Staff

CSAM Functionality and Benefits

Functionality	Benefits
Full end-to-end Assessment & Authorization management	Enterprise security risk visibility & awareness Automates ongoing authorization & assessment processes, supporting evolving OMB A-130 and FISMA requirements Monitors system Authorization to Operate (ATO) expirations, enhancing resource and budget allocation priorities Minimizes duplicative work by leveraging inheritance and hybrid security controls, reducing control assessment burden
Comprehensive view of FISMA System inventory and security posture with quantitative risk scoring	
Serves as organized repository for all required documentation	
Robust audit capability supporting internal and external audits	
Automation of System Security Plan (SSP) development and maintenance	
Provides for enhanced inheritance, hybrid controls, privacy controls	
Plan of Action & Milestones (POA&M) management	
Customizable dashboards, reports, & notifications	
Security control assessments with “motive” capability (e.g. A-123, core controls, privacy)	
Automated NIST 800-53 control-set migration	
Integration of NIST content supporting ATO processes	

CSAM Line of Business (LOB) Services and Benefits

Line of Business service	Benefit
DOJ hosting available	Alleviates maintenance/operation costs for LOB partner
Shared service model	Non-profit, cost recovery pricing structure
Partner community of cybersecurity subject matter experts Wide-ranging and ongoing integration capabilities	Continuous enhancements aligned with government cybersecurity requirements
Comprehensive implementation support	Tailored implementation & onboarding support for effective system utilization
Dedicated client engagement managers	Actively engages partner agency to provide guidance, gather feedback and assist in the growth of the application and customer
Helpdesk support	In-house tier 1, 2, and 3 support
Training	Regular user training and open forums, web-based and/or and on-site

CSAM and NIST SP 800-53

- The NIST SP 800-53 Security and Privacy Control catalog is a fundamental building block of the CSAM application

- Various iterations of CSAM have used the NIST publications dating back to SP 800-26 and the original SP 800-53 in the early-to-mid 2000's as the basis of their Control content

- CSAM Approach to Control Implementation and Assessment
  - Enterprise defines the importance and priority of each control
  - Systems select and describe the implementation of each control in narrative format
  - The assessment of each control drives its implementation status and residual risk analysis

- To support this approach, a control set in CSAM requires:
  - Controls from SP 800-53; and
  - Assessment Procedures from SP 800-53A
    - Also called "Determine If Statements" in CSAM

History of CSAM and NIST SP 800-53, Revision 4

April 2013

- NIST publishes SP 800-53, Revision 4 (Controls)

December 2014

- NIST publishes SP 800-53A, Revision 4 (Assessment Procedures)
- NIST publishes a machine-readable XML version

January 2015

- NIST publishes update to SP 800-53, Revision 4 (Controls)
- NIST publishes a machine-readable XML version
- CSAM team builds import logic to create the control set content for CSAM based on the 800-53 and 800-53A machine-readable XML files

March 2015

- CSAM team releases the NIST SP 800-53, Revision 4 control set with CSAM v3.4

Planning For NIST SP 800-53, Revision 5 in CSAM

September 2020

- NIST publishes SP 800-53, Revision 5 (Controls)

Spring 2021

- CSAM customers begin asking about status of the SP 800-53, Revision 5 control set
- OMB Circular A-130 requires federal agency legacy systems to be in compliance with new NIST standards and guidelines within one year of publication

Challenge

- CSAM's approach to control set content has a dependency on both the Controls (SP 800-53) and the Assessment Procedures (SP 800-53A)
  - SP 800-53, Revision 5 is final
  - SP 800-53A, Revision 5 is not final
- How do we support customers that need to use the Controls from SP 800-53, Revision 5 before SP 800-53A, Revision 5 is published?

Solution – Generate Interim Content from OSCAL

- The NIST Open Security Controls Assessment Language (OSCAL) team produced a machine-readable catalog of the NIST SP 800-53, Revision 5 content
  - https://github.com/usnistgov/oscal-content/tree/master/nist.gov/SP800-53/rev5
- The OSCAL Catalog breaks the Control text down into a detailed tree structure that the CSAM team mapped into CSAM's Determine If Statement structure
  - Control parameters are broken out

```
"params": [
    {
        "id": "ac-1_prm_1",
        "label": "organization-defined personnel or roles"
    },
```

  - Each statement within a control is broken out, and contain references to control parameters where applicable

```
"id": "ac-1_smt.a",
"name": "item",
"prose": "Develop, document, and disseminate to {{ ac-1_prm_1 }}:",
"parts": [
{
    "id": "ac-1_smt.a.1",
    "name": "item",
    "prose": "{{ ac-1_prm_2 }} access control policy that:",
    "parts": [
    {
        "id": "ac-1_smt.a.1.a",
        "name": "item",
        "prose": "Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and"
    },
    {
        "id": "ac-1_smt.a.1.b",
        "name": "item",
        "prose": "Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and"
    }
    ]
```

Edited to remove some elements for brevity

Solution – Generate Interim Content from OSCAL

- The CSAM team processed the OSCAL machine-readable catalog to create the Determine If Statement content for CSAM that is comprised of two kinds of statements:
  - Statements covering the definition of each Control parameter (where applicable)
  - Statements covering the Control text in the form of complete sentences re-assembled from the tree structure defined in the OSCAL catalog

- Control Parameter Examples

  CPV-AC-1 [1]: The following control parameter is defined: (P1) assignment: organization-defined personnel or roles

  CPV-AC-1 [2]: The following control parameter is defined: (P2) selection (one or more): Organization-level; Mission/business process-level; System-level

- Control Text Examples

  AC-1 (a)(1)(a): Develop, document, and disseminate to [**(P1) Assignment: organization-defined personnel or roles] [(P2) Selection (one or more): Organization-level; Mission/business process-level; System-level]** access control policy that *addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.*

  AC-1 (a)(1)(b): Develop, document, and disseminate to [**(P1) Assignment: organization-defined personnel or roles] [(P2) Selection (one or more): Organization-level; Mission/business process-level; System-level]** access control policy that *is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.*

  - **Bold text** indicates control parameters; these are replaced when populated by customer in CSAM
  - *Italicized text* indicates where these two examples differ

Next CSAM Release will provide customers with the interim SP 800-53 Revision 5 control set

- The CSAM team will provide the interim SP 800-53, Revision 5 control set with CSAM v4.7, targeted for release this week.
- Each customer can choose to proceed with the interim control set or they can wait for NIST to publish 800-53A, Revision 5 and CSAM to be updated accordingly
- Customers ready to proceed should populate Control Parameters prior to migrating systems
- Once the customer enables the NIST 800-53 Revision 5 control set, migration can occur in a flexible manner, gradually over time
- New capabilities added to support more efficient implementation and assessments
  - Control automation – automatically update the assessment of CPV Determine If Statements when the parameters are populated
  - Easily synchronize the Determine If Statement content on a system when the master content is updated, including population of parameter values

What happens when SP 800-53A, Rev 5 is published?

- Once NIST publishes the final NIST 800-53A content for Revision 5, the CSAM team will process the updated OSCAL catalog to generate the corresponding Determine If Statement content for CSAM
- Customers that use the interim control set can migrate to the final 800-53A content in a gradual manner over the course of performing new assessments, system-by-system and control-by-control
- Customers will be able to migrate to the final NIST 800-53A content regardless of whether they make use of the interim control set

DOJ Cyber Security Points of Contact

POC	Contact Information
Nickolous Ward Chief Information Security Officer Office of the Chief Information Officer Department of Justice	Nickolous.Ward@usdoj.gov (202) 616-2478
Ramon Burks Assistant Director Engineering & ICAM Office of the Chief Information Officer Department of Justice	Ramon.Burks@usdoj.gov (202) 598-9426
Daphna Shai Shared Cybersecurity Services Program Manager Cybersecurity Services Staff Office of the Chief Information Officer Department of Justice	Daphna.shai@usdoj.gov (202) 616-0768
Ritul Walia Client Engagement Manager Office of the Chief Information Officer Department of Justice	Ritul.Walia@usdoj.gov (202) 616-1490

Demonstration