GovReady®

Greg Elin

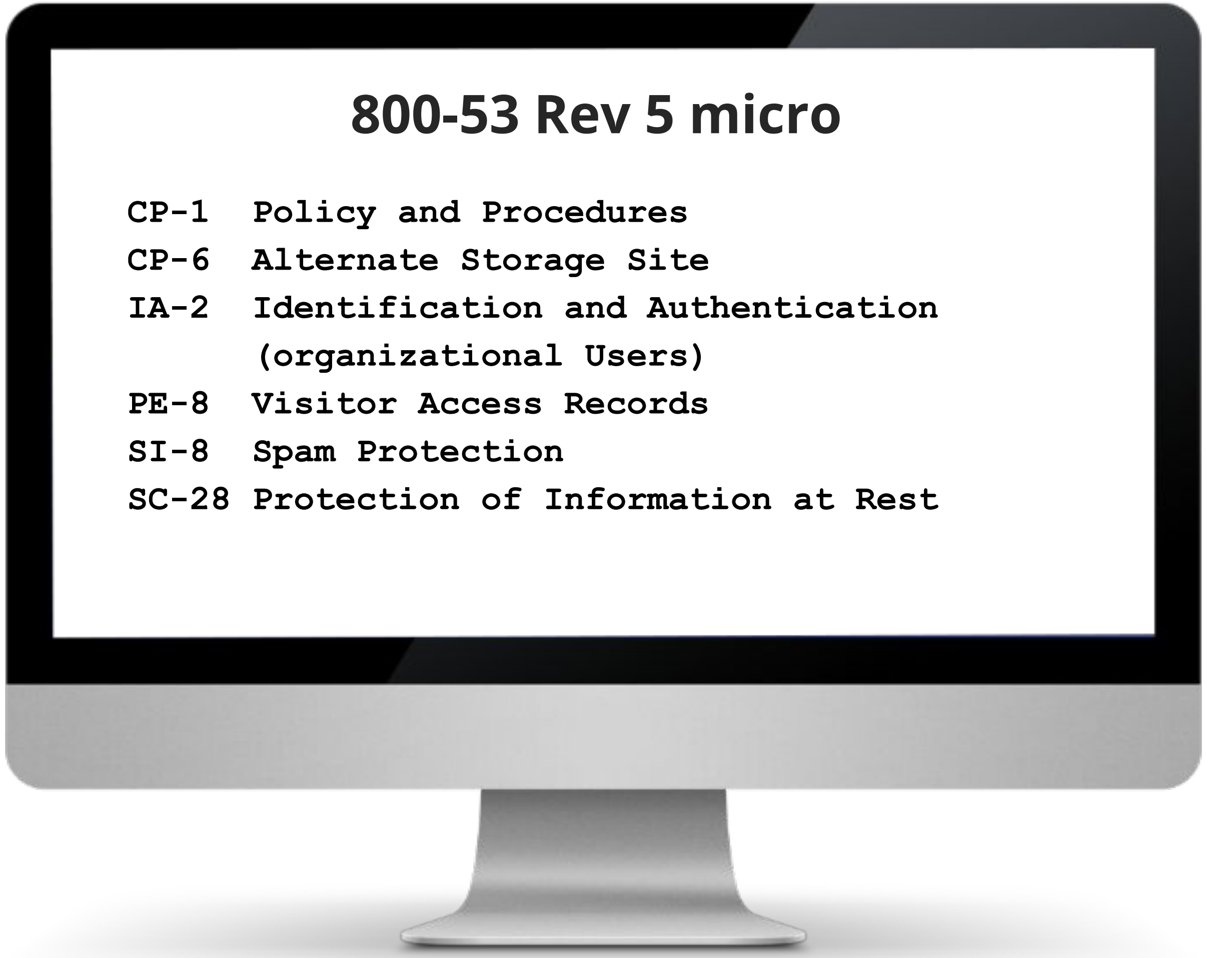
OSCAL Example Control Set
July 22, 2022

Proposal: OSCAL Example Control Set

Let’s pick a small set of controls to consistently use in examples.

Why

- Examples are very helpful
- Nice if everyone is using same examples
- Common public reference
- Good learning tool
- Only a few controls to make prototyping easier
- Product evaluations
- Support R&D



800-53 Rev 5 micro

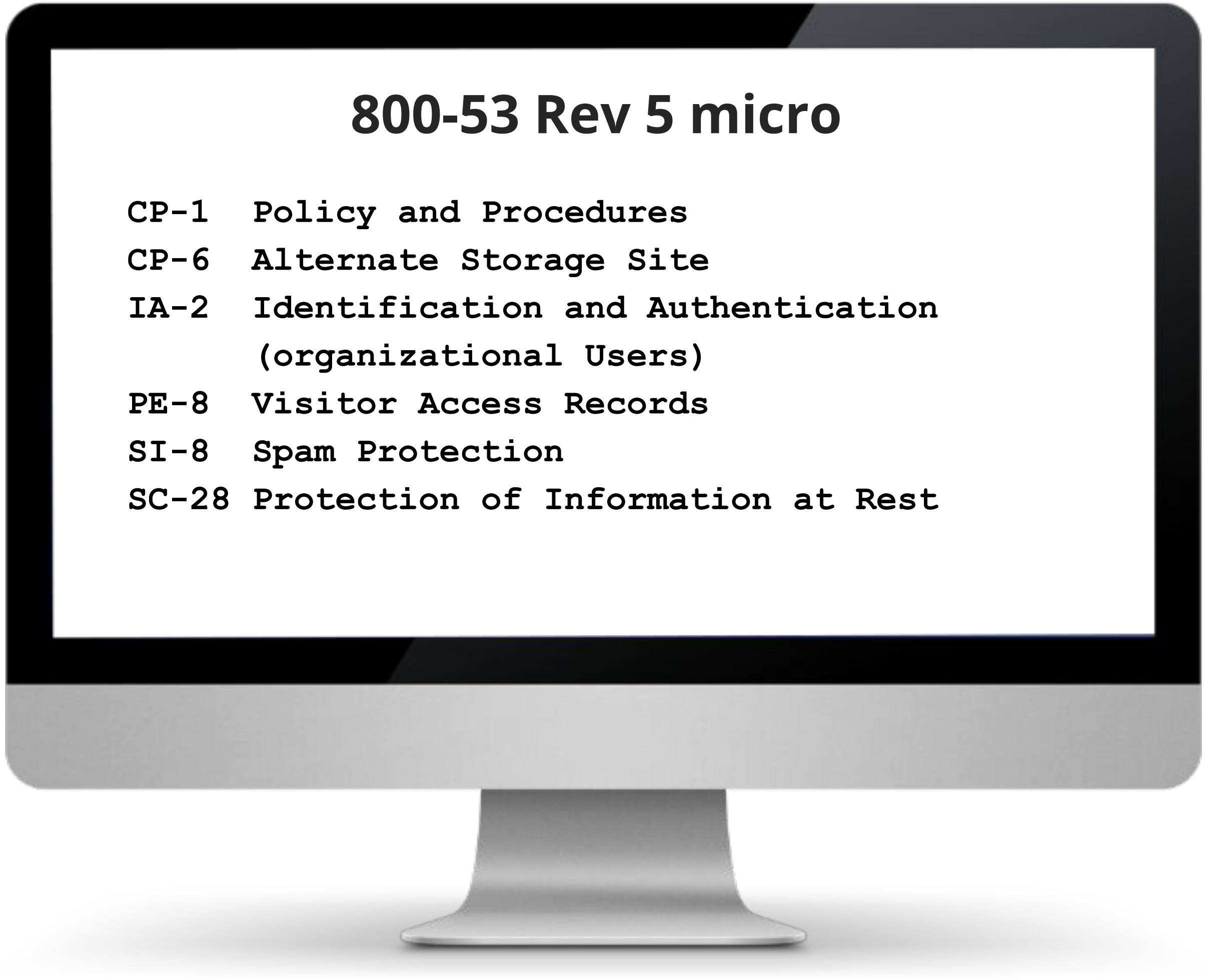
CP-1	Policy and Procedures
CP-6	Alternate Storage Site
IA-2	Identification and Authentication (organizational Users)
PE-8	Visitor Access Records
SI-8	Spam Protection
SC-28	Protection of Information at Rest

https://github.com/usnistgov/OSCAL/issues/1383

Introduction: OSCAL Example Control Set

Criteria

- Demonstrates common types of controls
- Demonstrates common characteristics
- More than one family
- ODP with frequency (natural language v computable)
- Good for demonstrating rules
- (maybe) FedRAMP “useful”
- (maybe) Control with change to 800-53 Rev 5
- (maybe) Controls that exists at different baselines
- (maybe) Requires artifact



800-53 Rev 5 micro

CP-1	Policy and Procedures
CP-6	Alternate Storage Site
IA-2	Identification and Authentication (organizational Users)
PE-8	Visitor Access Records
SI-8	Spam Protection
SC-28	Protection of Information at Rest

Types/Characteristics of Controls

- Organizational
- Technical
- Policy (-1’s)
- Process-Oriented

- Parts & Sub Parts
- Organizational Defined Params
- References policy
- Interconnection

- [Usually] Inherited
- Hybrid
- Customer Responsibilities
- Roles

Types/Characteristics of Controls

Organizational

CP-1, CP-6, PE-8, SI-8

Technical

IA-2, SC-28

Policy (-1’s)

CP-1

Process-Oriented

IA-2

Parts & Sub Parts

CP-1, CP-6, PE-8, SI-8, SC-28

Organizational Defined Params

CP-1, PE-8, SC-28*

References policy or?

CP-6, IA-2

Interconnection

?

[Usually] Inherited

CP-1, CP-6, PE-8, SI-8

Hybrid

CP-1, IA-2, PE-8, SC-28

Customer Responsibilities

?

Roles

PE-8

Types of Controls

CP-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and c. Review and update the current contingency planning: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CP-6	Alternate Storage Site	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Types of Controls

IA-2	Identification and Authentication (organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Types of Controls

PE-8	Visitor Access Records	a. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period]; b. Review visitor access records [Assignment: organization-defined frequency]; and c. Report anomalies in visitor access records to [Assignment: organization-defined personnel].

Types of Controls

SC-28	Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

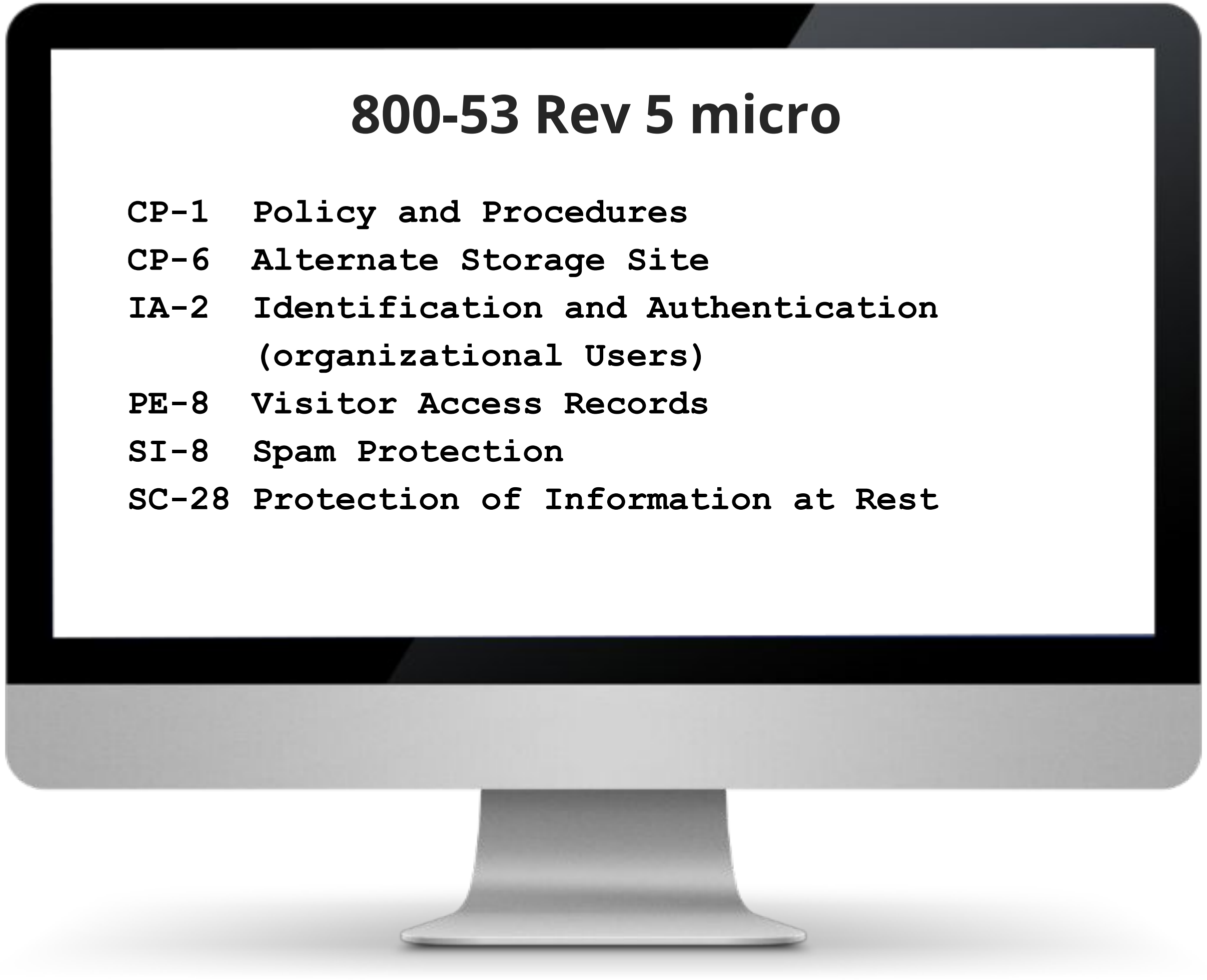
Types of Controls

SI-8	Spam Protection	a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

For Consideration: Other Issues to Consider

Discuss

- Control Enhancement?
- Control Overlay Example?
- Controls from second framework?



800-53 Rev 5 micro

CP-1	Policy and Procedures
CP-6	Alternate Storage Site
IA-2	Identification and Authentication (organizational Users)
PE-8	Visitor Access Records
SI-8	Spam Protection
SC-28	Protection of Information at Rest

Greg Elin, GovReady PBC

☎ 917-304-3488

✉ gregelin@govready.com

🌐 www.govready.com

THANK YOU

www.govready.com