NIST National Institute of Standards and Technology

BUILDING A SECURE CLOUD SOLUTION THAT SUPPORTS CONTINUOUS MONITORING AND ASSESSMENT

NIST CLOUD COMPUTING RUBIK'S CUBE (CCSRC) & OPEN SECURITY CONTROLS ASSESSMENT LANGUAGE (OSCAL)

Dr. Michaela Iorga
NIST, ITL

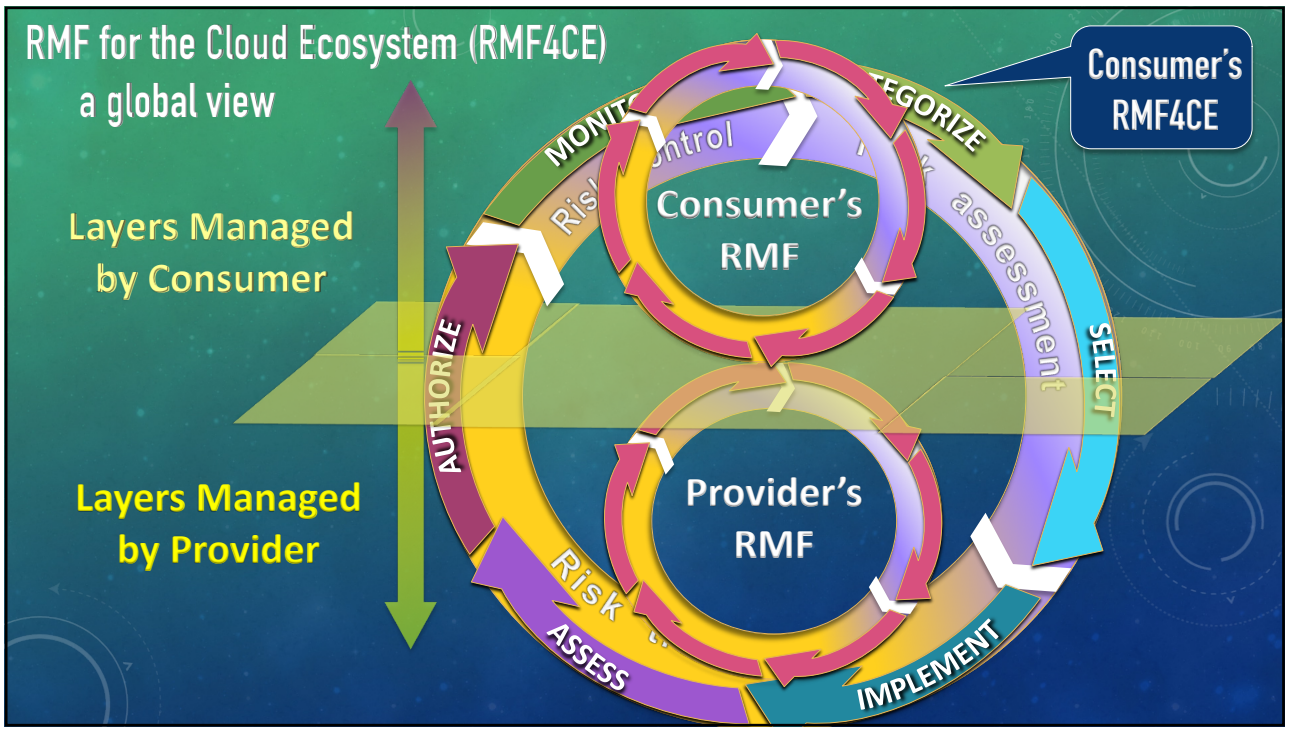
FEBRUARY 2018

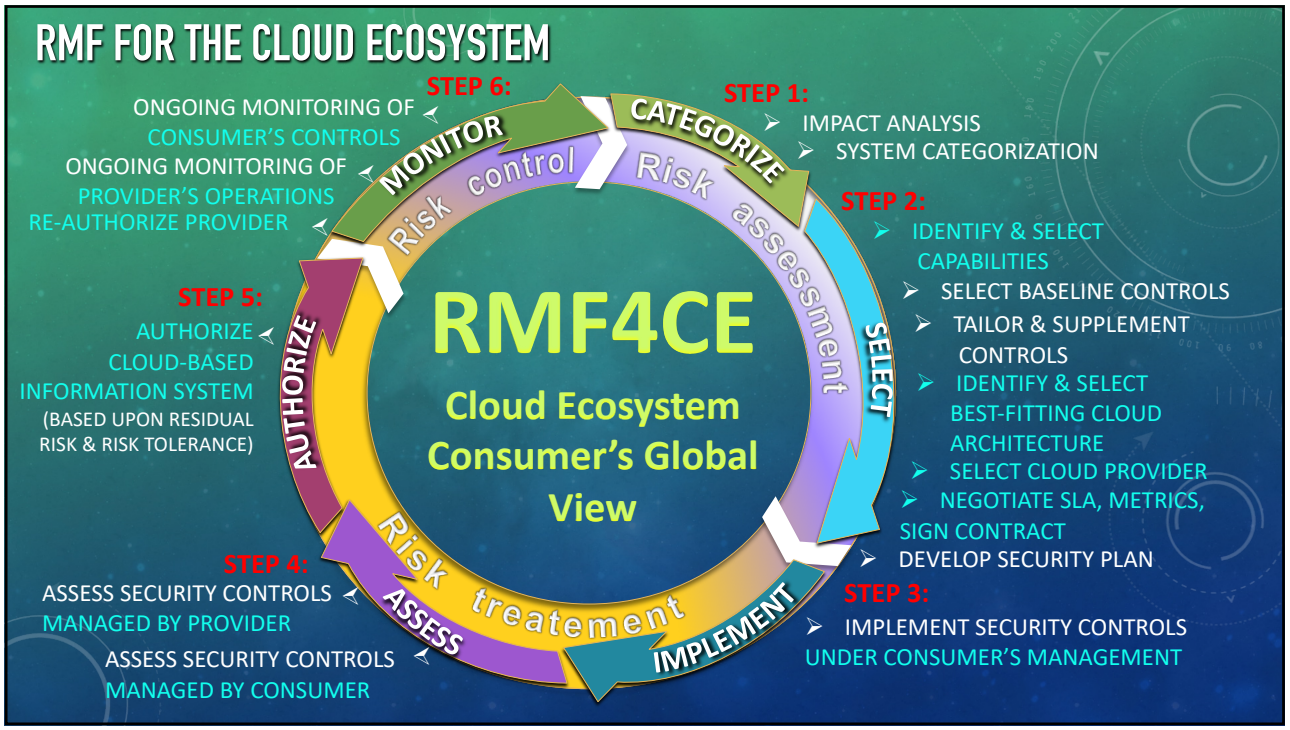
NIST National Institute of Standards and Technology

TODAY'S CHALLENGES

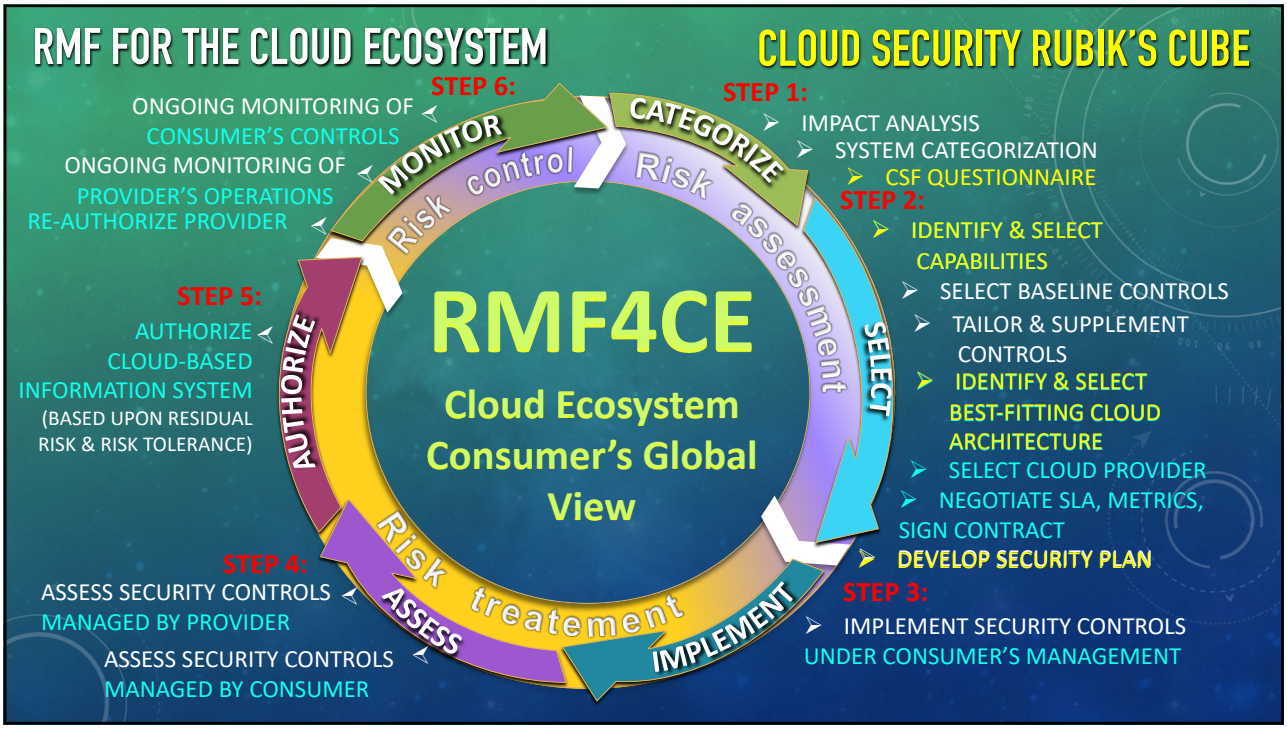
- Making the correct choice for your business (SaaS, PaaS or IaaS ?);
- Understanding the complexity of the Information Systems, especially cloud-based solutions;
- Risk Management is few orders of magnitude more complex;
  - Loss of control (trust issues not security issues, data owner & data custodian),
  - Vendor's transparency,
  - Security and Compliance,
    - Regulatory Frameworks are burdensome,
    - Security Vulnerabilities are everywhere,
  - Availability, Resilience and Reliability,
- System updates trigger documentation (SSP) to become outdated.

2


RMF for the Cloud Ecosystem (RMF4CE)
a global view
Layers Managed by Consumer
Layers Managed by Provider
Consumer's RMF4CE
Consumer's RMF
Provider's RMF
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
Risk assessment
Risk treatement


RMF FOR THE CLOUD ECOSYSTEM
RMF4CE
Cloud Ecosystem Consumer's Global View
STEP 1:
IMPACT ANALYSIS
SYSTEM CATEGORIZATION
STEP 2:
IDENTIFY & SELECT CAPABILITIES
SELECT BASELINE CONTROLS
TAILOR & SUPPLEMENT CONTROLS
IDENTIFY & SELECT BEST-FITTING CLOUD ARCHITECTURE
SELECT CLOUD PROVIDER
NEGOTIATE SLA, METRICS, SIGN CONTRACT
DEVELOP SECURITY PLAN
STEP 3:
IMPLEMENT SECURITY CONTROLS UNDER CONSUMER'S MANAGEMENT
STEP 4:
ASSESS SECURITY CONTROLS MANAGED BY PROVIDER
ASSESS SECURITY CONTROLS MANAGED BY CONSUMER
STEP 5:
AUTHORIZE CLOUD-BASED INFORMATION SYSTEM
(BASED UPON RESIDUAL RISK & RISK TOLERANCE)
STEP 6:
ONGOING MONITORING OF CONSUMER'S CONTROLS
ONGOING MONITORING OF PROVIDER'S OPERATIONS
RE-AUTHORIZE PROVIDER
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
Risk assessment
Risk treatement
Risk control

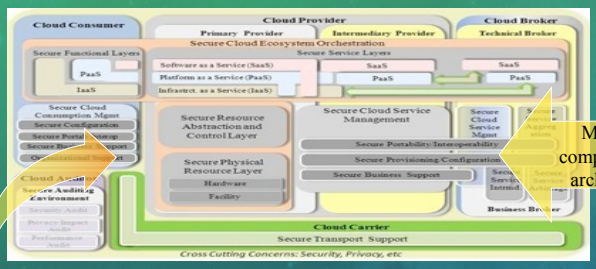
RMF FOR THE CLOUD ECOSYSTEM



CLOUD SECURITY RUBIK'S CUBE

NIST CC SECURITY REFERENCE ARCHITECTURE – THE APPROACH

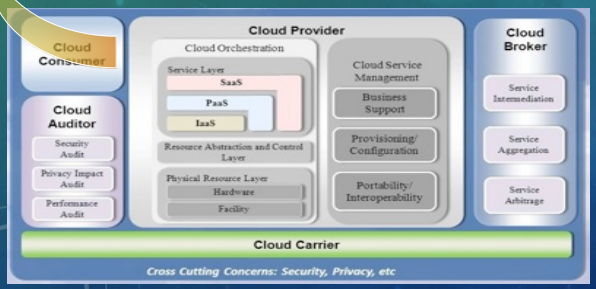
NIST Security Reference Architecture – formal model



NIST Security Reference Architecture – security components

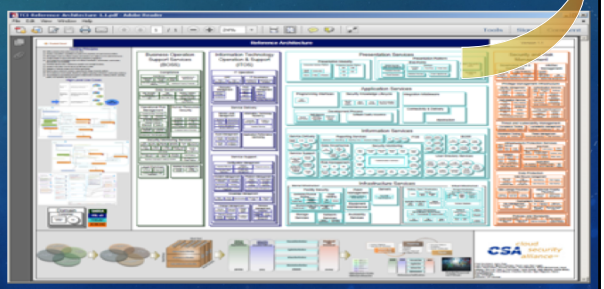
Mapping components to architecture

NIST Reference Architecture

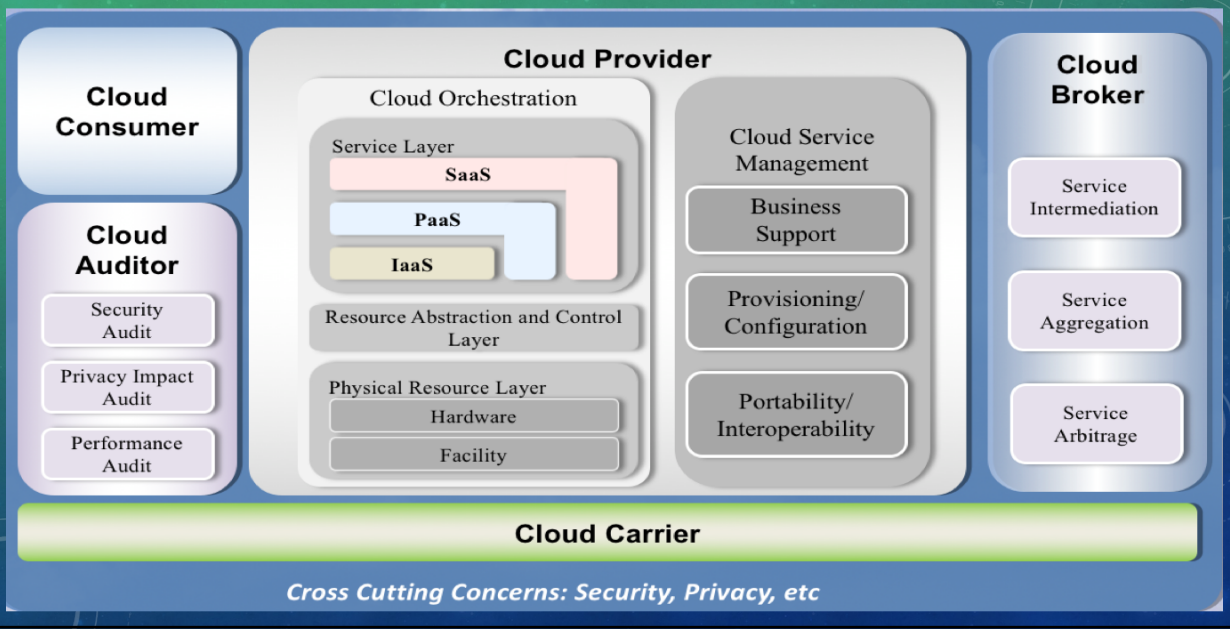


+

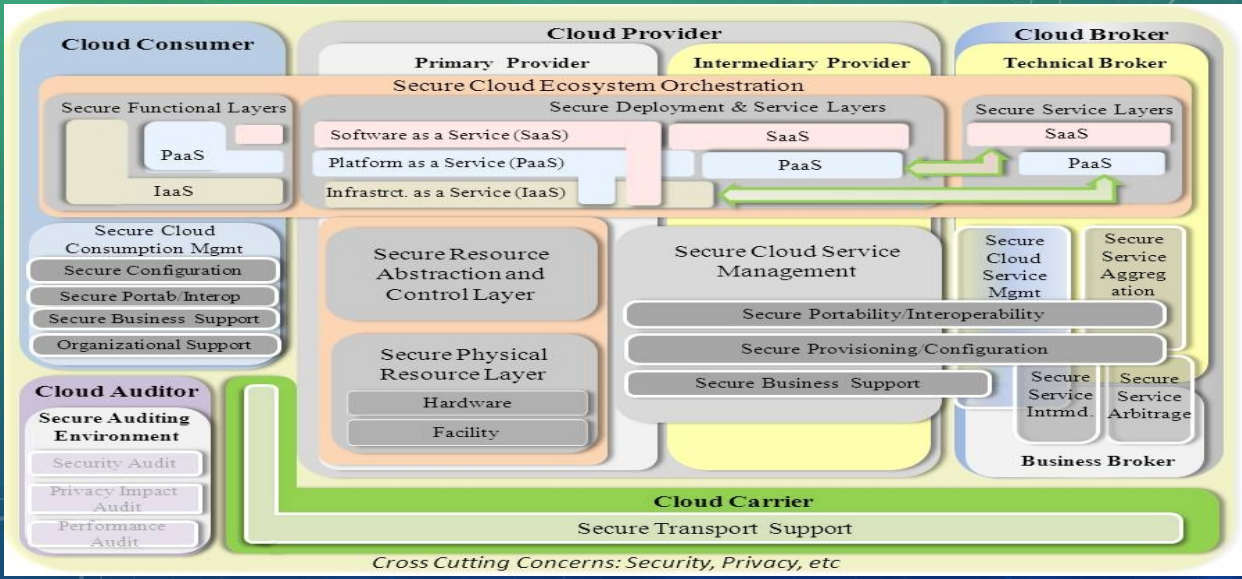
CSA's TCI Reference Architecture



SP 800-292: NIST CLOUD COMPUTING REFERENCE ARCHITECTURE

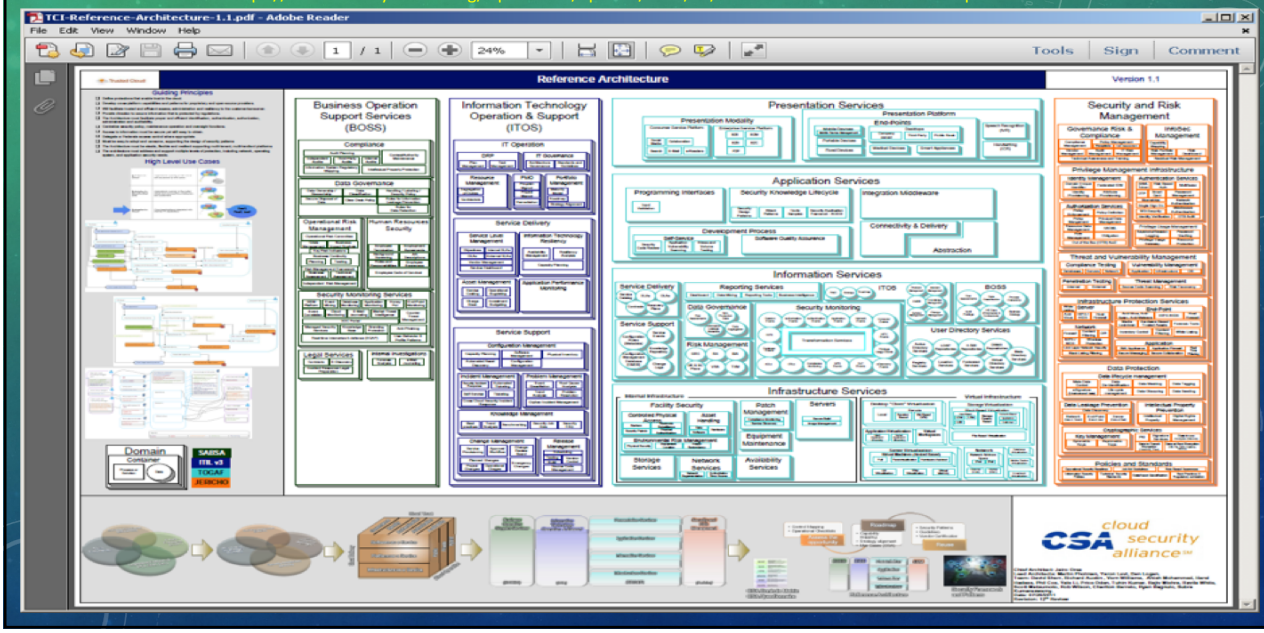


SP 800-299: NIST CLOUD SECURITY REFERENCE ARCHITECTURE



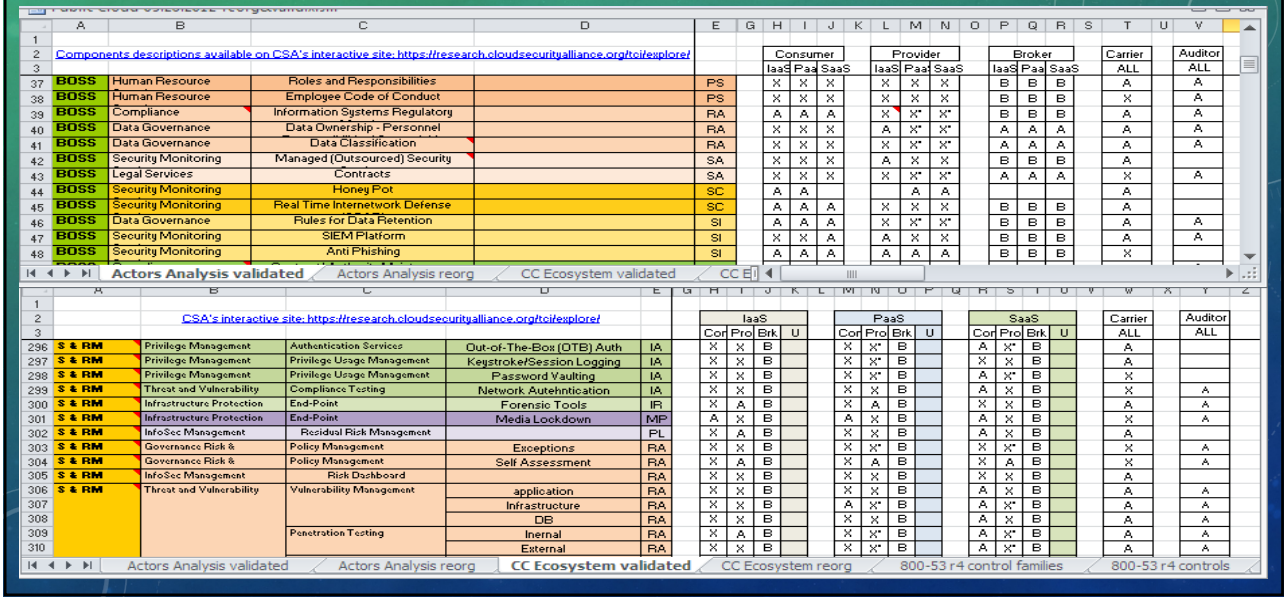
Cloud Security Alliance's TCI Reference Architecture

https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI-Reference-Architecture-v1.1.pdf



SP 800-299: NIST CLOUD SECURITY REFERENCE ARCHITECTURE

- FUNCTIONAL CAPABILITIES -



Components descriptions available on CSA's interactive site: https://research.cloudsecurityalliance.org/tci/explore/

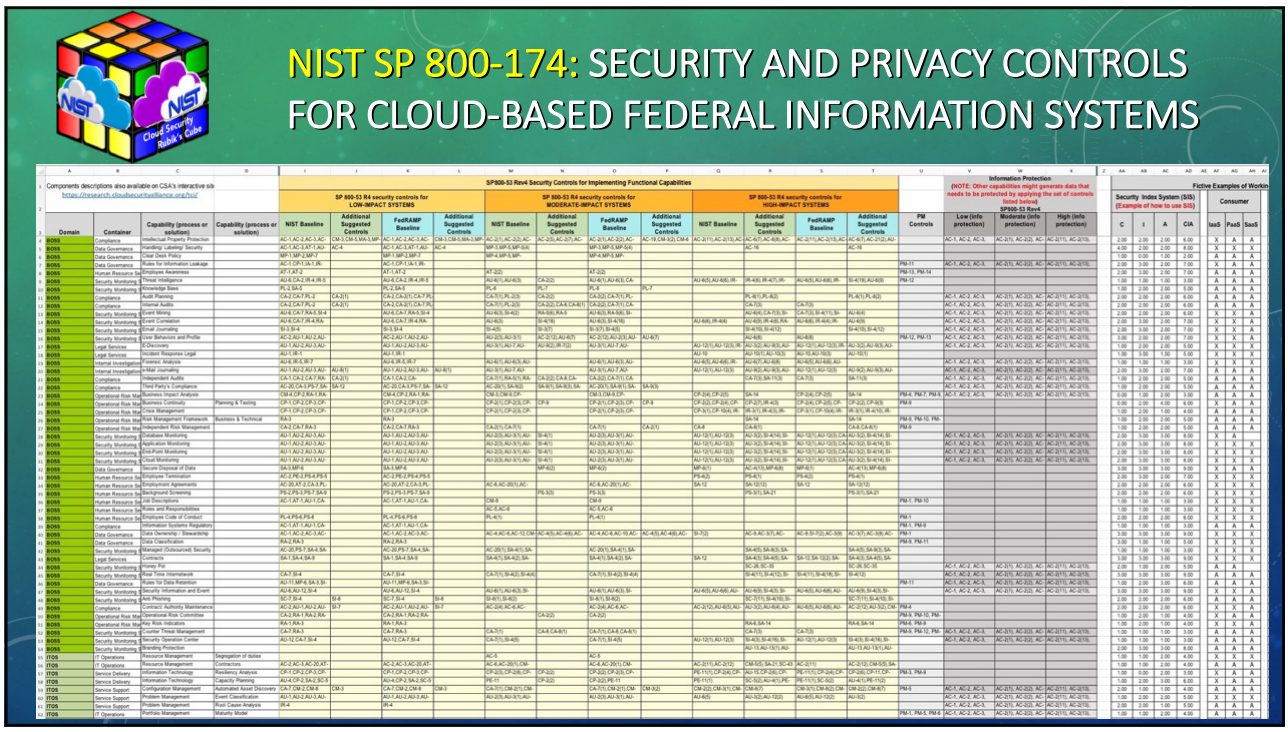
					Consumer			Provider			Broker			Carrier	Auditor
					IaaS	PaaS	SaaS	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS	ALL	ALL
37	BOSS	Human Resource	Roles and Responsibilities	PS	X	X	X	X	X	X	B	B	B	A	A
38	BOSS	Human Resource	Employee Code of Conduct	PS	X	X	X	X	X	X	B	B	B	X	A
39	BOSS	Compliance	Information Systems Regulatory	RA	A	A	A	X	X*	X*	B	B	B	A	A
40	BOSS	Data Governance	Data Ownership - Personnel	RA	X	X	X	A	X*	X*	A	A	A	A	A
41	BOSS	Data Governance	Data Classification	RA	X	X	X	X	X*	X*	A	A	A	A	A
42	BOSS	Security Monitoring	Managed (Outsourced) Security	SA	X	X	X	A	X	X	B	B	B	A	
43	BOSS	Legal Services	Contracts	SA	X	X	X	X	X*	X*	A	A	A	X	A
44	BOSS	Security Monitoring	Honey Pot	SC	A	A			A	A				A	
45	BOSS	Security Monitoring	Real Time Internetwork Defense	SC	A	A	A	X	X	X	B	B	B	A	
46	BOSS	Data Governance	Rules for Data Retention	SI	A	A	A	X	X*	X*	B	B	B	A	A
47	BOSS	Security Monitoring	SIEM Platform	SI	X	X	A	A	X	X	B	B	B	A	A
48	BOSS	Security Monitoring	Anti Phishing	SI	A	A	A	A	A	A	B	B	B	X	

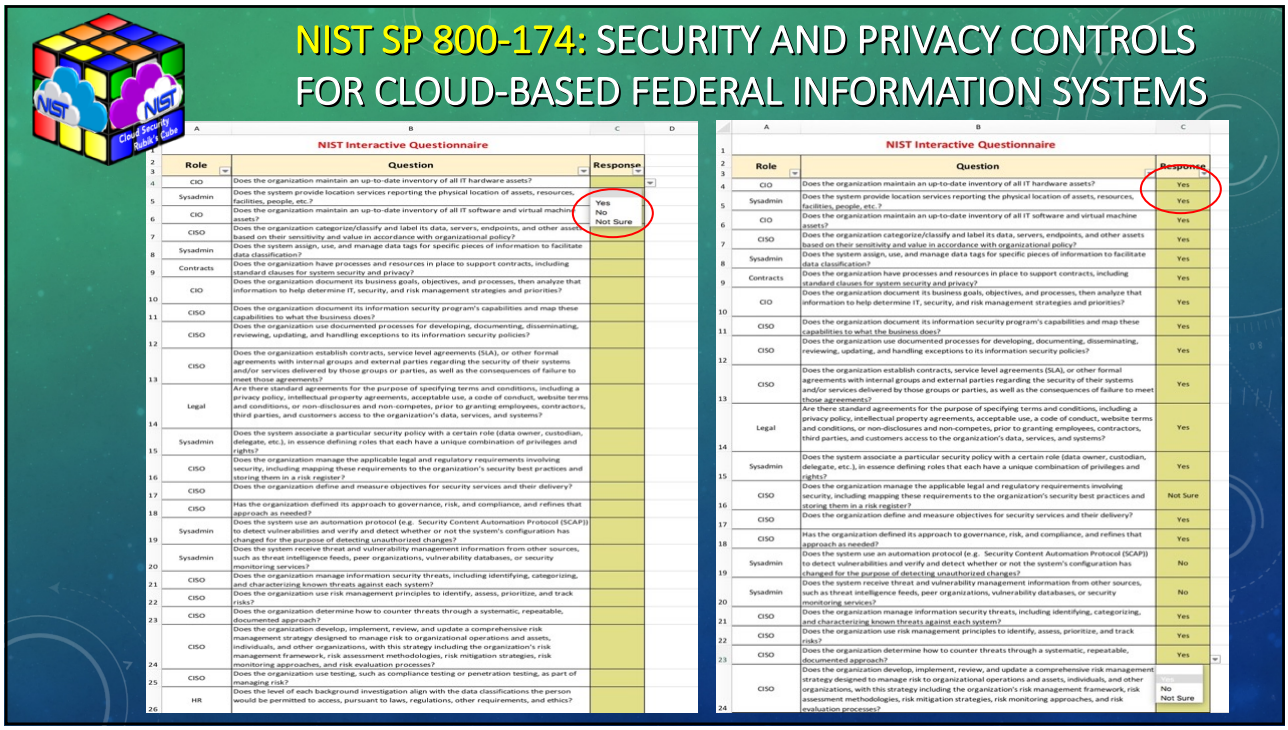
Actors Analysis validated | Actors Analysis reorg | CC Ecosystem validated | CC E

CSA's interactive site: https://research.cloudsecurityalliance.org/tci/explore/

						IaaS				PaaS				SaaS				Carrier	Auditor
						Cor	Pro	Brk	U	Cor	Pro	Brk	U	Cor	Pro	Brk	U	ALL	ALL
296	S & RM	Privilege Management	Authentication Services	Out-of-The-Box (OTB) Auth	IA	X	X	B		X	X*	B		A	X*	B		A	
297	S & RM	Privilege Management	Privilege Usage Management	Keystroke/Session Logging	IA	X	X	B		X	X*	B		A	X*	B		A	
298	S & RM	Privilege Management	Privilege Usage Management	Password Vaulting	IA	X	X	B		X	X*	B		A	X*	B		X	
299	S & RM	Threat and Vulnerability	Compliance Testing	Network Autehntication	IA	X	X	B		X	X	B		A	X	B		X	A
300	S & RM	Infrastructure Protection	End-Point	Forensic Tools	IR	X	A	B		X	A	B		X	X	B		A	A
301	S & RM	Infrastructure Protection	End-Point	Media Lockdown	MP	A	X	B		A	X	B		A	X	B		X	A
302	S & RM	InfoSec Management	Residual Risk Management		PL	X	A	B		X	X	B		A	X	B		A	
303	S & RM	Governance Risk &	Policy Management	Exceptions	RA	X	X	B		X	X*	B		X	X*	B		X	A
304	S & RM	Governance Risk &	Policy Management	Self Assessment	RA	X	A	B		X	A	B		X	A	B		X	A
305	S & RM	InfoSec Management	Risk Dashboard		RA	X	X	B		X	X	B		X	X	B		A	
306	S & RM	Threat and Vulnerability	Vulnerability Management	application	RA	X	X	B		X	X	B		A	X	B		A	A
307				Infrastructure	RA	X	X	B		A	X*	B		A	X*	B		A	A
308				DB	RA	X	X	B		X	X	B		A	X	B		A	A
309			Penetration Testing	Inernal	RA	X	A	B		X	X*	B		A	X*	B		A	A
310				External	RA	X	X	B		X	X*	B		A	X*	B		A	A

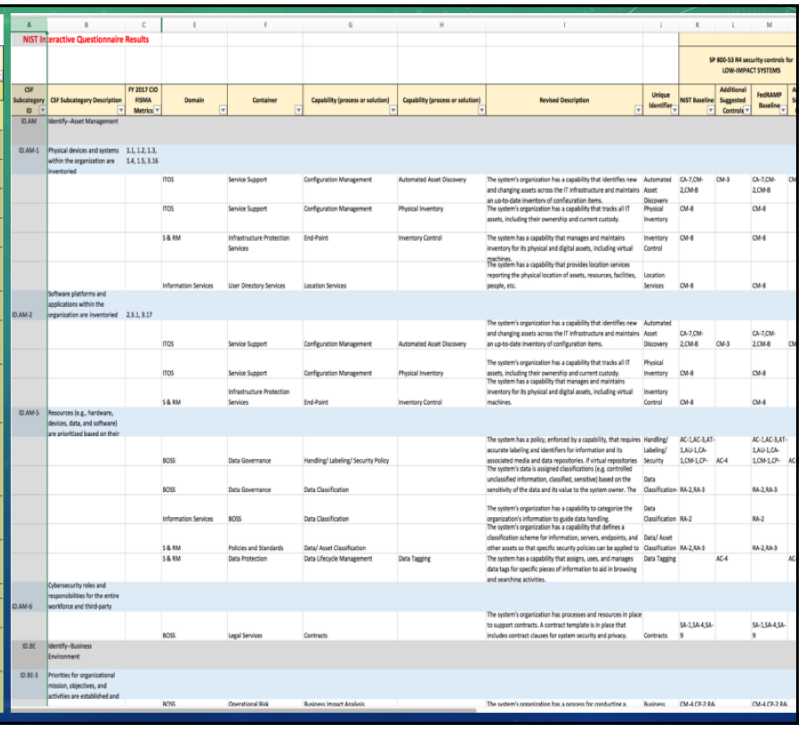
Actors Analysis validated | Actors Analysis reorg | CC Ecosystem validated | CC Ecosystem reorg | 800-53 r4 control families | 800-53 r4 controls


NIST SP 800-174: SECURITY AND PRIVACY CONTROLS
FOR CLOUD-BASED FEDERAL INFORMATION SYSTEMS


NIST SP 800-174: SECURITY AND PRIVACY CONTROLS
FOR CLOUD-BASED FEDERAL INFORMATION SYSTEMS
NIST Interactive Questionnaire
Role
Question
Response
CIO
Does the organization maintain an up-to-date inventory of all IT hardware assets?
Sysadmin
Does the system provide location services reporting the physical location of assets, resources, facilities, people, etc.?
CIO
Does the organization maintain an up-to-date inventory of all IT software and virtual machine assets?
CISO
Does the organization categorize/classify and label its data, servers, endpoints, and other assets based on their sensitivity and value in accordance with organizational policy?
Sysadmin
Does the system assign, use, and manage data tags for specific pieces of information to facilitate data classification?
Contracts
Does the organization have processes and resources in place to support contracts, including standard clauses for system security and privacy?
CIO
Does the organization document its business goals, objectives, and processes, then analyze that information to help determine IT, security, and risk management strategies and priorities?
CISO
Does the organization document its information security program's capabilities and map these capabilities to what the business does?
CISO
Does the organization use documented processes for developing, documenting, disseminating, reviewing, updating, and handling exceptions to its information security policies?
CISO
Does the organization establish contracts, service level agreements (SLA), or other formal agreements with internal groups and external parties regarding the security of their systems and/or services delivered by those groups or parties, as well as the consequences of failure to meet those agreements?
Legal
Are there standard agreements for the purpose of specifying terms and conditions, including a privacy policy, intellectual property agreements, acceptable use, a code of conduct, website terms and conditions, or non-disclosures and non-competes, prior to granting employees, contractors, third parties, and customers access to the organization's data, services, and systems?
Sysadmin
Does the system associate a particular security policy with a certain role (data owner, custodian, delegate, etc.), in essence defining roles that each have a unique combination of privileges and rights?
CISO
Does the organization manage the applicable legal and regulatory requirements involving security, including mapping these requirements to the organization's security best practices and storing them in a risk register?
CISO
Does the organization define and measure objectives for security services and their delivery?
CISO
Has the organization defined its approach to governance, risk, and compliance, and refines that approach as needed?
Sysadmin
Does the system use an automation protocol (e.g. Security Content Automation Protocol (SCAP)) to detect vulnerabilities and verify and detect whether or not the system's configuration has changed for the purpose of detecting unauthorized changes?
Sysadmin
Does the system receive threat and vulnerability management information from other sources, such as threat intelligence feeds, peer organizations, vulnerability databases, or security monitoring services?
CISO
Does the organization manage information security threats, including identifying, categorizing, and characterizing known threats against each system?
CISO
Does the organization use risk management principles to identify, assess, prioritize, and track risks?
CISO
Does the organization determine how to counter threats through a systematic, repeatable, documented approach?
CISO
Does the organization develop, implement, review, and update a comprehensive risk management strategy designed to manage risk to organizational operations and assets, individuals, and other organizations, with this strategy including the organization's risk management framework, risk assessment methodologies, risk mitigation strategies, risk monitoring approaches, and risk evaluation processes?
CISO
Does the organization use testing, such as compliance testing or penetration testing, as part of managing risk?
HR
Does the level of each background investigation align with the data classifications the person would be permitted to access, pursuant to laws, regulations, other requirements, and ethics?
Yes
No
Not Sure

NIST Interactive Questionnaire

Role	Question	Response
CIO	Does the organization maintain an up-to-date inventory of all IT hardware assets?	Yes
Sysadmin	Does the system provide location services reporting the physical location of assets, resources, facilities, people, etc.?	Yes
CIO	Does the organization maintain an up-to-date inventory of all IT software and virtual machine assets?	Yes
CISO	Does the organization categorize/classify and label its data, servers, endpoints, and other assets based on their sensitivity and value in accordance with organizational policy?	Yes
Sysadmin	Does the system assign, use, and manage data tags for specific pieces of information to facilitate data classification?	Yes
Contracts	Does the organization have processes and resources in place to support contracts, including standard clauses for system security and privacy?	Yes
CIO	Does the organization document its business goals, objectives, and processes, then analyze that information to help determine IT, security, and risk management strategies and priorities?	Yes
CISO	Does the organization document its information security program's capabilities and map these capabilities to what the business does?	Yes
CISO	Does the organization use documented processes for developing, documenting, disseminating, reviewing, updating, and handling exceptions to its information security policies?	Yes
CISO	Does the organization establish contracts, service level agreements (SLA), or other formal agreements with internal groups and external parties regarding the security of their systems and/or services delivered by those groups or parties, as well as the consequences of failure to meet those agreements?	Yes
Legal	Are there standard agreements for the purpose of specifying terms and conditions, including a privacy policy, intellectual property agreements, acceptable use, a code of conduct, website terms and conditions, or non-disclosures and non-competes, prior to granting employees, contractors, third parties, and customers access to the organization's data, services, and systems?	Yes
Sysadmin	Does the system associate a particular security policy with a certain role (data owner, custodian, delegate, etc.), in essence defining roles that each have a unique combination of privileges and rights?	Yes
CISO	Does the organization manage the applicable legal and regulatory requirements involving security, including mapping these requirements to the organization's security best practices and storing them in a risk register?	Yes
CISO	Does the organization define and measure objectives for security services and their delivery?	Yes
CISO	Has the organization defined its approach to governance, risk, and compliance, and refines that approach as needed?	Yes
Sysadmin	Does the system use an automation protocol (e.g. Security Content Automation Protocol (SCAP)) to detect vulnerabilities and verify and detect whether or not the system's configuration has changed for the purpose of detecting unauthorized changes?	Yes
Sysadmin	Does the system receive threat and vulnerability management information from other sources, such as threat intelligence feeds, peer organizations, vulnerability databases, or security monitoring services?	Yes

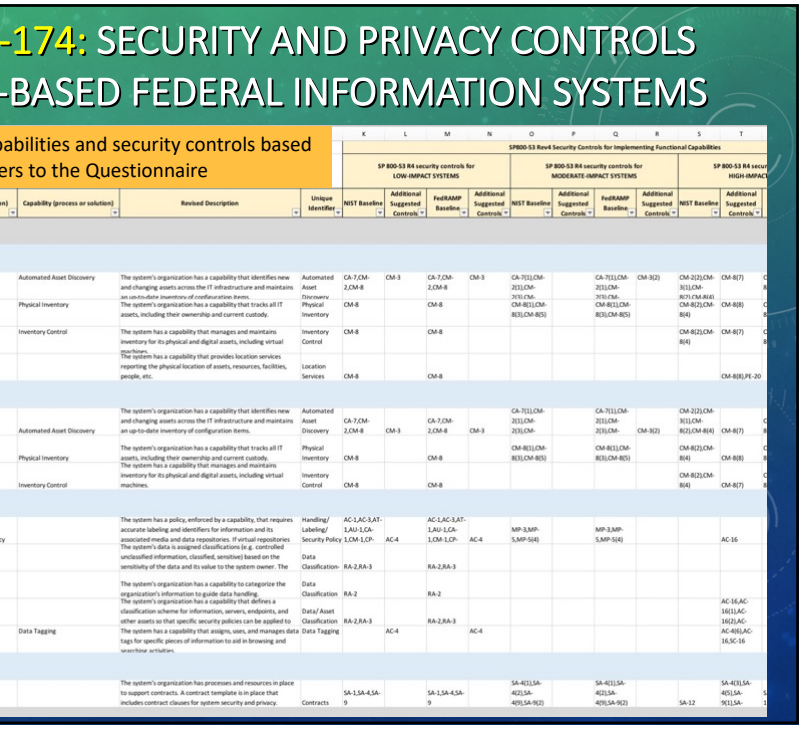


NIST Interactive Questionnaire Results

CSF Subcategory ID	CSF Subcategory Description	FY 2017 CIO FISMA Metrics	Domain	Container	Capability (process or solution)	Capability (process or solution)	Revised Description	Unique Identifier	NIST Baseline	Additional Suggested Controls	FedRAMP Baseline	Additional Suggested Controls
ID.AM	Identify--Asset Management											
ID.AM-1	Physical devices and systems within the organization are inventoried	1.1, 1.2, 1.3, 1.4, 1.5, 3.16										
			ITOS	Service Support	Configuration Management	Automated Asset Discovery	The system's organization has a capability that identifies new and changing assets across the IT infrastructure and maintains an up-to-date inventory of configuration items.	Automated Asset Discovery	CA-7,CM-2,CM-8	CM-3	CA-7,CM-2,CM-8	CM-3
			ITOS	Service Support	Configuration Management	Physical Inventory	The system's organization has a capability that tracks all IT assets, including their ownership and current custody.	Physical Inventory	CM-8		CM-8	
			S & RM	Infrastructure Protection Services	End-Point	Inventory Control	The system has a capability that manages and maintains inventory for its physical and digital assets, including virtual machines.	Inventory Control	CM-8		CM-8	
			Information Services	User Directory Services	Location Services		The system has a capability that provides location services reporting the physical location of assets, resources, facilities, people, etc.	Location Services	CM-8		CM-8	
ID.AM-2	Software platforms and applications within the organization are inventoried	2.3.1, 3.17										
			ITOS	Service Support	Configuration Management	Automated Asset Discovery	The system's organization has a capability that identifies new and changing assets across the IT infrastructure and maintains an up-to-date inventory of configuration items.	Automated Asset Discovery	CA-7,CM-2,CM-8	CM-3	CA-7,CM-2,CM-8	CM-3
			ITOS	Service Support	Configuration Management	Physical Inventory	The system's organization has a capability that tracks all IT assets, including their ownership and current custody.	Physical Inventory	CM-8		CM-8	
			S & RM	Infrastructure Protection Services	End-Point	Inventory Control	The system has a capability that manages and maintains inventory for its physical and digital assets, including virtual machines.	Inventory Control	CM-8		CM-8	
ID.AM-5	Resources (e.g., hardware, devices, data, and software) are prioritized based on their											
			BOSS	Data Governance	Handling/ Labeling/ Security Policy		The system has a policy, enforced by a capability, that requires accurate labeling and identifiers for information and its associated media and data repositories. If virtual repositories	Handling/ Labeling/ Security	AC-1,AC-3,AT-1,AU-1,CA-1,CM-1,CP-	AC-4		AC-1,AC-3,AT-1,AU-1,CA-1,CM-1,CP-
			BOSS	Data Governance	Data Classification		The system's data is assigned classifications (e.g. controlled unclassified information, classified, sensitive) based on the sensitivity of the data and its value to the system owner. The	Data Classification	RA-2,RA-3		RA-2,RA-3	
			Information Services	BOSS	Data Classification		The system's organization has a capability to categorize the organization's information to guide data handling.	Data Classification	RA-2		RA-2	
			S & RM	Policies and Standards	Data/ Asset Classification		The system's organization has a capability that defines a classification scheme for information, servers, endpoints, and other assets so that specific security policies can be applied to	Data/ Asset Classification	RA-2,RA-3		RA-2,RA-3	
			S & RM	Data Protection	Data Lifecycle Management	Data Tagging	The system has a capability that assigns, uses, and manages data tags for specific pieces of information to aid in browsing and searching activities.	Data Tagging		AC-4		AC
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party											
			BOSS	Legal Services	Contracts		The system's organization has processes and resources in place to support contracts. A contract template is in place that includes contract clauses for system security and privacy.	Contracts	SA-1,SA-4,SA-9		SA-1,SA-4,SA-9	
ID.BE	Identify--Business Environment											
ID.BE-3	Priorities for organizational mission, objectives, and activities are established and											
			BOSS	Operational Risk	Business Impact Analysis		The system's organization has a process for conducting a	Business	CM-4,CP-2,RA-		CM-4,CP-2,RA-	

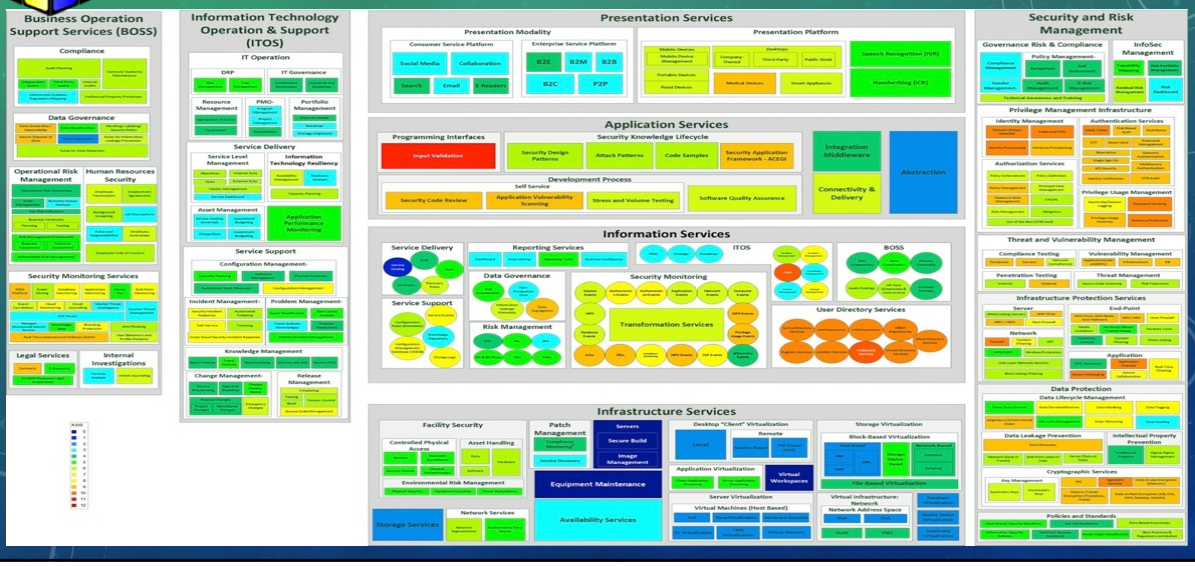
NIST SP 800-174: SECURITY AND PRIVACY CONTROLS FOR CLOUD-BASED FEDERAL INFORMATION SYSTEMS

Suggested functional capabilities and security controls based on the answers to the Questionnaire

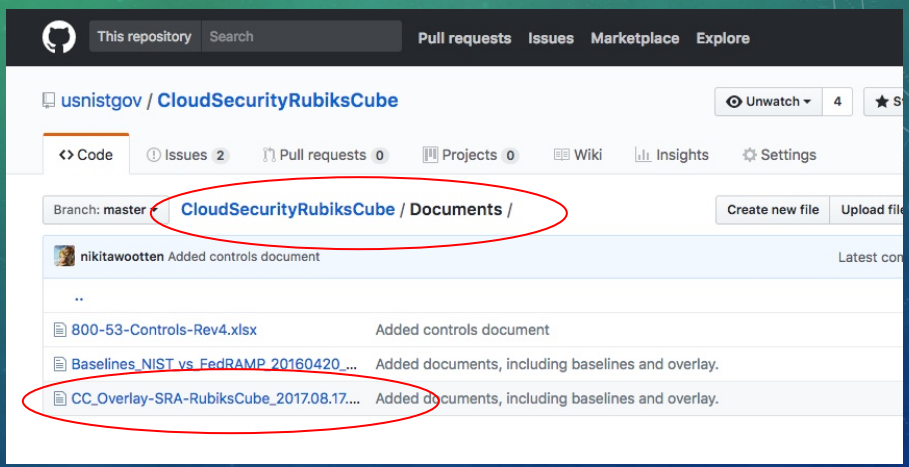


CSF Subcategory ID	CSF Subcategory Description	FY 2017 CIO FISMA Metrics	Domain	Container	Capability (process or solution)	Capability (process or solution)	Revised Description	Unique Identifier	SP800-53 Rev4 Security Controls for Implementing Functional Capabilities: SP 800-53 R4 security controls for LOW-IMPACT SYSTEMS: NIST Baseline	Additional Suggested Controls	FedRAMP Baseline	Additional Suggested Controls	SP 800-53 R4 security controls for MODERATE-IMPACT SYSTEMS: NIST Baseline	Additional Suggested Controls	FedRAMP Baseline	Additional Suggested Controls	SP 800-53 R4 security controls for HIGH-IMPACT: NIST Baseline	Additional Suggested Controls
ID.AM	Identify--Asset Management																	
ID.AM-1	Physical devices and systems within the organization are inventoried	1.1, 1.2, 1.3, 1.4, 1.5, 3.16																
			ITOS	Service Support	Configuration Management	Automated Asset Discovery	The system's organization has a capability that identifies new and changing assets across the IT infrastructure and maintains an up-to-date inventory of configuration items.	Automated Asset Discovery	CA-7,CM-2,CM-8	CM-3	CA-7,CM-2,CM-8	CM-3	CA-7(1),CM-2(1),CM-8(3),CM-8(5)		CA-7(1),CM-2(1),CM-8(3),CM-8(5)	CM-3(2)	CM-2(2),CM-3(1),CM-8(2),CM-8(4)	CM-8(7)
			ITOS	Service Support	Configuration Management	Physical Inventory	The system's organization has a capability that tracks all IT assets, including their ownership and current custody.	Physical Inventory	CM-8		CM-8		CM-8(1),CM-8(3),CM-8(5)		CM-8(1),CM-8(3),CM-8(5)		CM-8(2),CM-8(4)	CM-8(8)
			S & RM	Infrastructure Protection Services	End-Point	Inventory Control	The system has a capability that manages and maintains inventory for its physical and digital assets, including virtual machines.	Inventory Control	CM-8		CM-8						CM-8(2),CM-8(4)	CM-8(7)
			Information Services	User Directory Services	Location Services		The system has a capability that provides location services reporting the physical location of assets, resources, facilities, people, etc.	Location Services	CM-8		CM-8							CM-8(8),PE-20
ID.AM-2	Software platforms and applications within the organization are inventoried	2.3.1, 3.17																
			ITOS	Service Support	Configuration Management	Automated Asset Discovery	The system's organization has a capability that identifies new and changing assets across the IT infrastructure and maintains an up-to-date inventory of configuration items.	Automated Asset Discovery	CA-7,CM-2,CM-8	CM-3	CA-7,CM-2,CM-8	CM-3	CA-7(1),CM-2(1),CM-8(3),CM-		CA-7(1),CM-2(1),CM-8(3),CM-	CM-3(2)	CM-2(2),CM-3(1),CM-8(2),CM-8(4)	CM-8(7)
			ITOS	Service Support	Configuration Management	Physical Inventory	The system's organization has a capability that tracks all IT assets, including their ownership and current custody.	Physical Inventory	CM-8		CM-8		CM-8(1),CM-8(3),CM-8(5)		CM-8(1),CM-8(3),CM-8(5)		CM-8(2),CM-8(4)	CM-8(8)
			S & RM	Infrastructure Protection Services	End-Point	Inventory Control	The system has a capability that manages and maintains inventory for its physical and digital assets, including virtual machines.	Inventory Control	CM-8		CM-8						CM-8(2),CM-8(4)	CM-8(7)
ID.AM-5	Resources (e.g., hardware, devices, data, and software) are prioritized based on their																	
			BOSS	Data Governance	Handling/ Labeling/ Security Policy		The system has a policy, enforced by a capability, that requires accurate labeling and identifiers for information and its associated media and data repositories. If virtual repositories	Handling/ Labeling/ Security Policy	AC-1,AC-3,AT-1,AU-1,CA-1,CM-1,CP-	AC-4	AC-1,AC-3,AT-1,AU-1,CA-1,CM-1,CP-	AC-4	MP-3,MP-5,MP-5(4)		MP-3,MP-5,MP-5(4)			AC-16
			BOSS	Data Governance	Data Classification		The system's data is assigned classifications (e.g. controlled unclassified information, classified, sensitive) based on the sensitivity of the data and its value to the system owner. The	Data Classification	RA-2,RA-3		RA-2,RA-3							
			Information Services	BOSS	Data Classification		The system's organization has a capability to categorize the organization's information to guide data handling.	Data Classification	RA-2		RA-2							
			S & RM	Policies and Standards	Data/ Asset Classification		The system's organization has a capability that defines a classification scheme for information, servers, endpoints, and other assets so that specific security policies can be applied to	Data/ Asset Classification	RA-2,RA-3		RA-2,RA-3							AC-16,AC-16(1),AC-16(2),AC-
			S & RM	Data Protection	Data Lifecycle Management	Data Tagging	The system has a capability that assigns, uses, and manages data tags for specific pieces of information to aid in browsing and searching activities.	Data Tagging		AC-4		AC-4						AC-4(6),AC-16,SC-16
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party																	
			BOSS	Legal Services	Contracts		The system's organization has processes and resources in place to support contracts. A contract template is in place that includes contract clauses for system security and privacy.	Contracts	SA-1,SA-4,SA-9		SA-1,SA-4,SA-9		SA-4(1),SA-4(2),SA-4(9),SA-9(2)		SA-4(1),SA-4(2),SA-4(9),SA-9(2)		SA-12	SA-4(1),SA-4(5),SA-9(1),SA-
ID.BE	Identify--Business Environment																	

NIST SP 500-299/SP 800-200: NIST CLOUD COMPUTING SECURITY REFERENCE ARCHITECTURE



NIST SP 800-174: SECURITY AND PRIVACY CONTROLS FOR CLOUD-BASED FEDERAL INFORMATION SYSTEMS



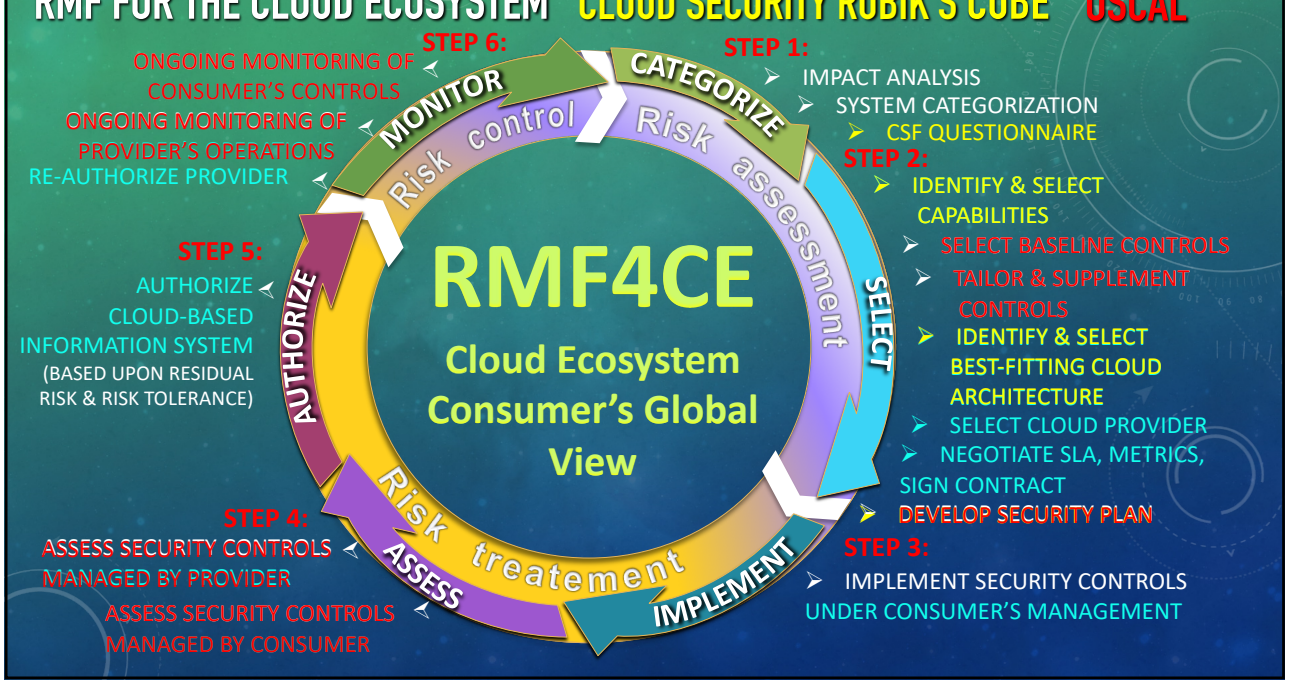
https://github.com/usnistgov/CloudSecurityRubiksCube/tree/master/Documents

GENERATING A SYSTEM SECURITY PLAN (SSP) THAT SUPPORTS ASSESSEMENT AUTOMATION AND NEAR-REAL-TIME MONITORING

BY LEVERAGING

OPEN SECURITY CONTROLS ASSESSMENT LANGUAGE (OSCAL)

SAL GAME CHANGER



NIST National Institute of Standards and Technology

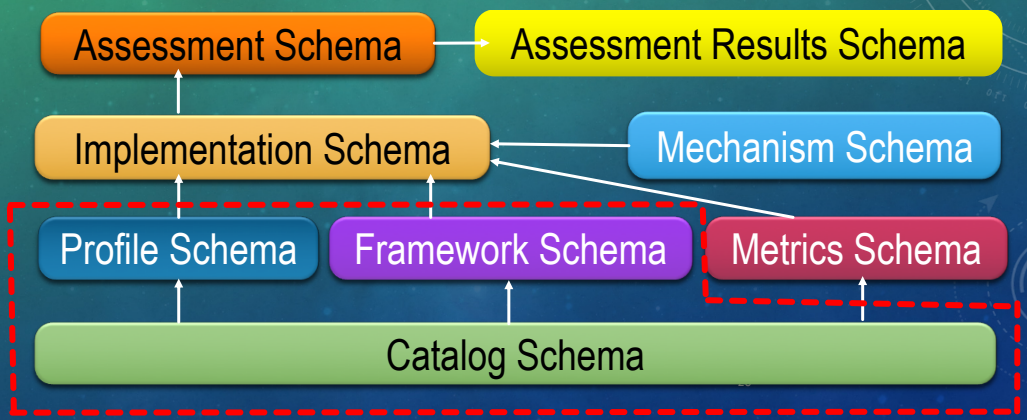
WHAT IS OSCAL?

- New "Standard of Standard" normalizing how system security controls and corresponding assessment information are represented;
  - **Standardized:** Provide security control, control implementation, and assessment information in an open, standardized way that can be used by both humans and machines
  - **Interoperable:** Ensure OSCAL is well-defined so tools using OSCAL information are interoperable and use information consistently
  - **Easy to use:** Promote developer adoption of OSCAL so tools are available for organizations to build, customize, and use OSCAL information
- Improves the efficiency, accuracy, and consistency of system security assessments.

19

NIST National Institute of Standards and Technology

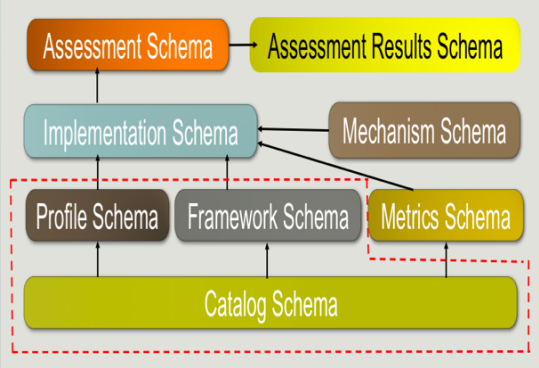
CURRENT FOCUS OF OSCAL DEVELOPMENT



NIST National Institute of Standards and Technology

DESCRIPTIONS OF CURRENT COMPONENTS

- **Catalog:** Defines a set of security controls (e.g., NIST SP 800-53 Appendix F); may also define objectives and methods for assessing the controls (e.g., NIST SP 800-53A)
- **Profile:** Defines a set of security requirements, where meeting each requirement necessitates implementing one or more security controls
- **Framework**: Defines a set of security requirements expressed at a higher level (e.g. Cybersecurity Framework)



21

PROSE VS. OSCAL CATALOG

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

1. Access control policy [*Assignment: organization-defined frequency*]; and
2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW AC-1	MOD AC-1	HIGH AC-1

```
<catalog xmlns="http://scap.nist.gov/schema/oscal">
  <title>NIST SP800-53</title>
  <declarations href="800-53-declarations.xml"/>
  <group class="family">
    <title>ACCESS CONTROL</title>
    <control class="SP800-53">
      <title>ACCESS CONTROL POLICY AND PROCEDURES</title>
      <prop class="number">AC-1</prop>
      <prop class="priority">P1</prop>
      <feat class="statement">
        <prop class="description">The organization:</prop>
        <feat class="statement">
          <prop class="number">AC-1a.</prop>
          <prop class="description">Develops, documents, and disseminates to <assign id="ac1a">
              organization-defined personnel or roles</assign></prop>
          <feat class="statement-item">
            <prop class="number">AC-1a.1.</prop>
            <prop class="description">An access control policy that addresses purpose, scope, roles, responsibilities,
management commitment, coordination among organizational ...[snip]...</prop>
          </feat>
        </feat>
      </feat>
      ...[snip]...
      <references>
        <ref>
          <citation href="http://csrc.nist.gov/publications/PubsSPs.html#800-12">NIST Special Publication 800-
12</citation>
        </ref>
        ...[snip]...
      </references>
    </control>
  </group>
</catalog>
```

PROSE VS. OSCAL CATALOG

Control Title

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

1. Access control policy [*Assignment: organization-defined frequency*]; and

2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW AC-1	MOD AC-1	HIGH AC-1

```
<catalog xmlns="http://scap.nist.gov/schema/oscal">
  <title>NIST SP800-53</title>
  <declarations href="800-53-declarations.xml"/>
  <group class="family">
    <title>ACCESS CONTROL</title>
    <control class="SP800-53">
      <title>ACCESS CONTROL POLICY AND PROCEDURES</title>
      <prop class="number">AC-1</prop>
      <prop class="priority">P1</prop>
      <feat class="statement">
        <prop class="description">The organization:</prop>
        <feat class="statement">
          <prop class="number">AC-1a.</prop>
          <prop class="description">Develops, documents, and disseminates to <assign id="ac1a">
            organization-defined personnel or roles</assign></prop>
          <feat class="statement-item">
            <prop class="number">AC-1a.1.</prop>
            <prop class="description">An access control policy that addresses purpose, scope, roles,
responsibilities, management commitment, coordination among organizational ...[snip]...</prop>
          </feat>
        </feat>
      </feat>
      ...[snip]...
      <references>
        <ref>
          <citation href="http://csrc.nist.gov/publications/PubsSPs.html#800-12">NIST Special Publication
800-12</citation>
        </ref>
        ...[snip]...
      </references>
    </control>
  </group>
</catalog>
```

PROSE VS. OSCAL CATALOG

Control Text

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

1. Access control policy [*Assignment: organization-defined frequency*]; and

2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW AC-1	MOD AC-1	HIGH AC-1

```
<catalog xmlns="http://scap.nist.gov/schema/oscal">
  <title>NIST SP800-53</title>
  <declarations href="800-53-declarations.xml"/>
  <group class="family">
    <title>ACCESS CONTROL</title>
    <control class="SP800-53">
      <title>ACCESS CONTROL POLICY AND PROCEDURES</title>
      <prop class="number">AC-1</prop>
      <prop class="priority">P1</prop>
      <feat class="statement">
        <prop class="description">The organization:</prop>
        <feat class="statement">
          <prop class="number">AC-1a.</prop>
          <prop class="description">Develops, documents, and disseminates to <assign id="ac1a">
            organization-defined personnel or roles</assign></prop>
          <feat class="statement-item">
            <prop class="number">AC-1a.1.</prop>
            <prop class="description">An access control policy that addresses purpose, scope, roles,
responsibilities, management commitment, coordination among organizational ...[snip]...</prop>
          </feat>
        </feat>
      </feat>
      ...[snip]...
      <references>
        <ref>
          <citation href="http://csrc.nist.gov/publications/PubsSPs.html#800-12">NIST Special Publication 800-
12</citation>
        </ref>
        ...[snip]...
      </references>
    </control>
  </group>
</catalog>
```

24

PROSE VS. OSCAL CATALOG

Parameter Assignment

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

1. Access control policy [*Assignment: organization-defined frequency*]; and
2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW AC-1	MOD AC-1	HIGH AC-1

```
<catalog xmlns="http://csrc.nist.gov/ns/oscal/1.0">
   <title>NIST SP800-53 rev 4</title>
   <declarations href="SP800-53-oscal-declarations.xml"/>
   <group class="family">
      <title>ACCESS CONTROL</title>
      <control class="SP800-53" id="ac.1">
         <title>ACCESS CONTROL POLICY AND PROCEDURES</title>
         <param id="ac-1_a">
            <desc>organization-defined personnel or roles</desc>
            <value>organization-defined personnel or roles</value>
         </param>
         <prop class="name">AC-1</prop>
         <prop class="priority">P1</prop>
         <part class="statement">
            <p class="description">The organization:</p>
            <part class="item" id="sms_ac-1a.">
               <prop class="name">AC-1a.</prop>
               <p class="description">Develops, documents, and disseminates to <insert param-id="ac-1_a"/>:</p>
               <part class="item" id="sms_ac-1a.1.">
                  <prop class="name">AC-1a.1.</prop>
                  <p class="description">An access control policy that addresses purpose, scope, roles, responsibilities, management
commitment, coordination among organizational entities, and compliance; and</p>
               </part>
               <part class="item" id="sms_ac-1a.2.">
                  <prop class="name">AC-1a.2.</prop>
                  <p class="description">Procedures to facilitate the implementation of the access control policy and associated access
controls; and</p>
               </part>
            </part>
            [... snip ...]
         </part>
         [... snip ...]
         <references>
            <ref>
               <citation href="http://csrc.nist.gov/publications/PubsSPs.html#800-12">NIST Special Publication 800-12</citation>
            </ref>
            [... snip ...]
         </references>
      </control>
   </group>
</catalog>
```

PROSE VS. OSCAL CATALOG

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

1. Access control policy [*Assignment: organization-defined frequency*]; and
2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW AC-1	MOD AC-1	HIGH AC-1

Document Reference

```
<catalog xmlns="http://scap.nist.gov/schema/oscal">
  <title>NIST SP800-53</title>
  <declarations href="800-53-declarations.xml"/>
  <group class="family">
    <title>ACCESS CONTROL</title>
    <control class="SP800-53">
      <title>ACCESS CONTROL POLICY AND PROCEDURES</title>
      <prop class="number">AC-1</prop>
      <prop class="priority">P1</prop>
      <feat class="statement">
        <prop class="description">The organization:</prop>
        <feat class="statement">
          <prop class="number">AC-1a.</prop>
          <prop class="description">Develops, documents, and disseminates to <assign id="ac1a">
            organization-defined personnel or roles</assign></prop>
          <feat class="statement-item">
            <prop class="number">AC-1a.1.</prop>
            <prop class="description">An access control policy that addresses purpose, scope, roles, responsibilities,
management commitment, coordination among organizational ...[snip]...</prop>
        </feat>
      </feat>
    </feat>
    ...[snip]...
    <references>
      <ref>
        <citation href="http://csrc.nist.gov/publications/PubsSPs.html#800-12">NIST Special Publication 800-
12</citation>
      </ref>
      ...[snip]...
    </references>
  </control>
  </group>
</catalog>
```

NIST National Institute of Standards and Technology

THE OSCAL FORMAT – OTHER FEATURES

A number of other features are also supported:

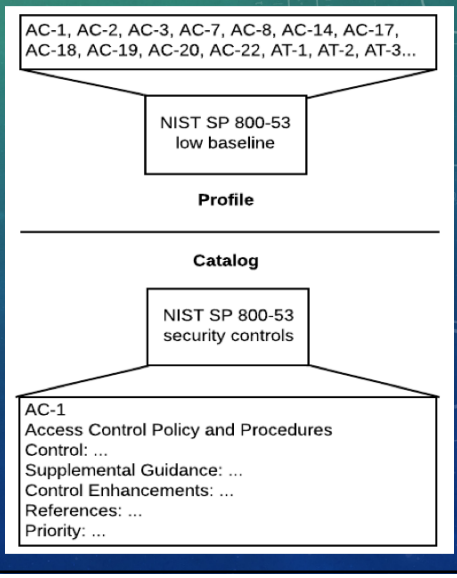
- Inclusion of additional guidance text
- References to related controls
- Definition of control enhancements
- Inclusion of assessment objectives and assessment methods (e.g., SP 800-53a)

27

PROFILE AND CATALOG MAPPING: A TRIVIAL EXAMPLE

Representing an NIST SP 800-53 low baseline:

- NIST SP 800-53 catalog defines possible security controls within its scope
- NIST SP 800-53 profile indicates which security controls from the catalog are required to be compliant
- Clear mapping between the controls specified in the profile and the controls defined in the catalog
- OSCAL provides a standardized, machine-readable profile with clear semantics
- Other catalogs and profiles can use the same interoperable format (e.g., ISO/IEC 27001/2)



NIST National Institute of Standards and Technology

SP 800-53 BASELINE VS OSCAL PROFILE

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	—	—	—	—
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	—	—	—	—
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

```
<profile xmlns="http://csrc.nist.gov/ns/oscal/1.0">
  <title>SP 800-53 Low Baseline</title>
  <invoke href="..snip..l">
    <call control-id="ac.1"/>

    <call control-id="ac.2"/>

    <call control-id="ac.3"/>

    <call control-id="ac.7"/>

    <call control-id="ac.8"/>

    <call control-id="ac.14"/>

    <call control-id="ac.17"/>

    <call control-id="ac.18"/>

    <call control-id="ac.19"/>

    <call control-id="ac.20"/>

    ...snip...
  </invoke>
</profile>
```

NIST National Institute of Standards and Technology

OSCAL DELIVERABLES

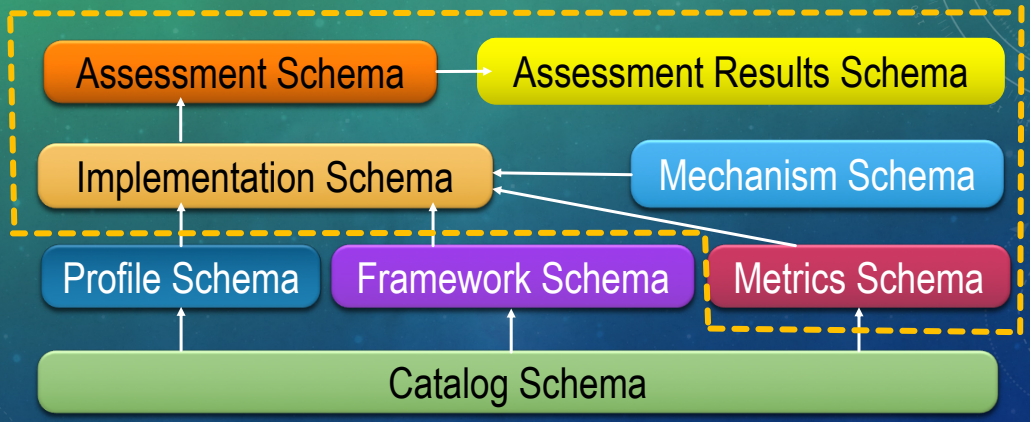
XML and JSON Schemas	Validate catalogs and profiles against constraints
XSL Templates	Produce human-readable versions (PDFs)
CSS	Edit OSCAL catalogs and profiles using XML tools
Documentation	Define the OSCAL specification Explain how organizations can convert existing catalogs and profiles into OSCAL formats

Posted to a NIST GitHub repo: https://github.com/usnistgov/OSCAL
Email oscal@nist.gov for access

30

NIST National Institute of Standards and Technology

FUTURE FOCUS

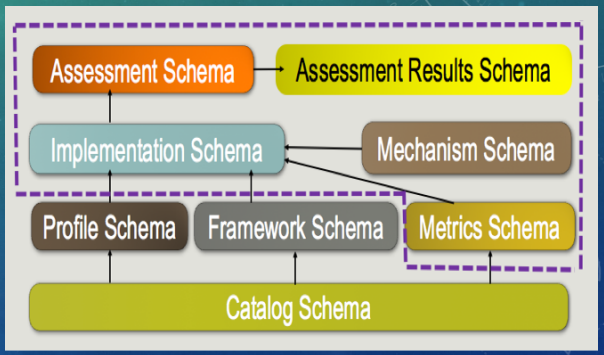


31

NIST National Institute of Standards and Technology

DESCRIPTIONS OF FUTURE COMPONENTS

- **Implementation:** Defines how each profile item is implemented (System Security Plan)
- **Assessment:** Describes how the system assessment is to be performed
- **Assessment Results:** Records the findings of the assessment
- **Metrics:** Defines metrics and measurements for understanding the effectiveness of the system's security
- **Mechanism:** Describes methods used to monitor the system's current security state (e.g., Security Content Automation Protocol (SCAP))



32