A RISK-BASED APPROACH TO CLOUD COMPUTING INFORMATION SYSTEMS

Dr. Michaela Iorga
Cloud Computing Security Technical Lead
NIST, ITL

MARCH 2018
THE KEYS TO THE CLOUD KINGDOM:
The 3Ts

- Transparency
- Traceability
- Trustworthiness
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- System updates trigger documentation (SSP) to become outdated.
"INDUSTRY SHOULD STEAL FEDRAMP CLOUD SECURITY BASELINES"

"You need good security requirements around procuring cloud? Look what FedRAMP's done. Not some industry-driven consortium."

*John Pescatore, Director SANS @ CyberCon*
UNDERSTANDING THE CLOUD-BASED SYSTEM’S BOUNDARIES
RMF FOR A CLOUD ECOSYSTEM (RMF4CE) (a global view)

Layers Managed by Consumer

Layers Managed by Provider

FedRAMP applies RMF when P-A&A Cloud Providers

Consumer’s RMF

Provider’s RMF

FedRAMP applies RMF when P-A&A Cloud Providers
RMF FOR THE CLOUD ECOSYSTEM

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

RMF4CE
RMF FOR THE CLOUD ECOSYSTEM

RMF4CE

Cloud Ecosystem Consumer’s Global View

STEP 1:
- IMPACT ANALYSIS
- SYSTEM CATEGORIZATION
- CSF QUESTIONNAIRE

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 PROVIDER’S OPERATIONS
- RE-AUTHORIZE PROVIDER

ONGOING MONITORING OF CONSUMER’S CONTROLS

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 500-292: NIST CLOUD COMPUTING REFERENCE ARCHITECTURE

Cloud Provider
- Cloud Orchestration
  - Service Layer
    - SaaS
    - PaaS
    - IaaS
  - Resource Abstraction and Control Layer
  - Physical Resource Layer
    - Hardware
    - Facility
- Cloud Service Management
  - Business Support
  - Provisioning/Configuration
  - Portability/Interoperability

Cloud Carrier

Cloud Consumer

Cloud Auditor
- Security Audit
- Privacy Impact Audit
- Performance Audit

Cloud Broker
- Service Intermediation
- Service Aggregation
- Service Arbitrage

Cross Cutting Concerns: Security, Privacy, etc
SP 500-299: NIST CLOUD SECURITY REFERENCE ARCHITECTURE
Cloud Security Alliance’s TCI Reference Architecture

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Consumer</th>
<th>Provider</th>
<th>Brokerson</th>
<th>Carrier</th>
<th>Auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOSS Human Resource</td>
<td>Roles and Responsibilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOSS Human Resource</td>
<td>Employee Code of Conduct</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOSS Compliance</td>
<td>Information Systems Regulatory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOSS Data Governance</td>
<td>Data Ownership - Personnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOSS Data Governance</td>
<td>Data Classification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOSS Security Monitoring</td>
<td>Managed (Outsourced) Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOSS Security Monitoring</td>
<td>Honey Pot</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOSS Security Monitoring</td>
<td>Real Time Internetwork Defense</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOSS Data Governance</td>
<td>Rules For Data Retention</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOSS Security Monitoring</td>
<td>SI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOSS Security Monitoring</td>
<td>Anti Phishing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SP 500-299: NIST CLOUD SECURITY REFERENCE ARCHITECTURE
- FUNCTIONAL CAPABILITIES -
## NIST SP 800-174: Security and Privacy Controls for Cloud-Based Federal Information Systems

| Domain | Container | Capability (process or system) | NIST Baseline | Additional Baseline Controls | FunSAMP Baseline | Additional Controls
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Authentication</td>
<td>AC-11, AC-12, AC-13</td>
<td>AC-11, AC-12, AC-13</td>
<td>AC-11, AC-12, AC-13</td>
<td>AC-11, AC-12, AC-13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Assurances</td>
<td>AC-14, AC-15</td>
<td>AC-14, AC-15</td>
<td>AC-14, AC-15</td>
<td>AC-14, AC-15</td>
</tr>
<tr>
<td>Data Security</td>
<td>Data Sharing</td>
<td>Access Control</td>
<td>AC-1, AC-2, AC-3</td>
<td>AC-1, AC-2, AC-3</td>
<td>AC-1, AC-2, AC-3</td>
<td>AC-1, AC-2, AC-3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Authentication</td>
<td>AC-11, AC-12, AC-13</td>
<td>AC-11, AC-12, AC-13</td>
<td>AC-11, AC-12, AC-13</td>
<td>AC-11, AC-12, AC-13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Assurances</td>
<td>AC-14, AC-15</td>
<td>AC-14, AC-15</td>
<td>AC-14, AC-15</td>
<td>AC-14, AC-15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Encryption</td>
<td>AC-16</td>
<td>AC-16</td>
<td>AC-16</td>
<td>AC-16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Protection</td>
<td>AC-17, AC-18</td>
<td>AC-17, AC-18</td>
<td>AC-17, AC-18</td>
<td>AC-17, AC-18</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Export</td>
<td>AC-30</td>
<td>AC-30</td>
<td>AC-30</td>
<td>AC-30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Export Controls</td>
<td>AC-33</td>
<td>AC-33</td>
<td>AC-33</td>
<td>AC-33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Assurances</td>
<td>AC-34, AC-35</td>
<td>AC-34, AC-35</td>
<td>AC-34, AC-35</td>
<td>AC-34, AC-35</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Loss Prevention</td>
<td>AC-36</td>
<td>AC-36</td>
<td>AC-36</td>
<td>AC-36</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Assurances</td>
<td>AC-37, AC-38</td>
<td>AC-37, AC-38</td>
<td>AC-37, AC-38</td>
<td>AC-37, AC-38</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Retention</td>
<td>AC-42</td>
<td>AC-42</td>
<td>AC-42</td>
<td>AC-42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Storage</td>
<td>AC-45</td>
<td>AC-45</td>
<td>AC-45</td>
<td>AC-45</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Transfer</td>
<td>AC-48</td>
<td>AC-48</td>
<td>AC-48</td>
<td>AC-48</td>
</tr>
</tbody>
</table>

**NIST Baseline**
- AC-1: Access Control
- AC-2: Authentication
- AC-3: Security Assurances
- AC-11, AC-12, AC-13: Authorization Controls
- AC-14, AC-15: Accountability
- AC-16: Confidentiality
- AC-17: Integrity
- AC-18: Availability
- AC-19: Risk Assessment
- AC-20: Risk Management
- AC-21, AC-22, AC-23: Key Management
- AC-24, AC-25: Cryptography
- AC-26, AC-27: Data Lifecycle Management
- AC-28, AC-29: Incident Response
- AC-30: Data Export
- AC-31, AC-32: Data Export Controls
- AC-33: Data Recovery
- AC-34, AC-35: Data Retention
- AC-36: Data Storage
- AC-37, AC-38: Data Transfer
- AC-39, AC-40, AC-41: Security Assurances
- AC-42: Data Loss Prevention
- AC-43, AC-44: Data Recovery
- AC-45: Data Storage
- AC-46, AC-47: Data Transfer
- AC-48: Data Storage
- AC-49, AC-50: Security Assurances

**Additional Baseline Controls**
- AC-1: Access Control
- AC-2: Authentication
- AC-3: Security Assurances
- AC-11, AC-12, AC-13: Authorization Controls
- AC-14, AC-15: Accountability
- AC-16: Confidentiality
- AC-17: Integrity
- AC-18: Availability
- AC-19: Risk Assessment
- AC-20: Risk Management
- AC-21, AC-22, AC-23: Key Management
- AC-24, AC-25: Cryptography
- AC-26, AC-27: Data Lifecycle Management
- AC-28, AC-29: Incident Response
- AC-30: Data Export
- AC-31, AC-32: Data Export Controls
- AC-33: Data Recovery
- AC-34, AC-35: Data Retention
- AC-36: Data Storage
- AC-37, AC-38: Data Transfer
- AC-39, AC-40, AC-41: Security Assurances
- AC-42: Data Loss Prevention
- AC-43, AC-44: Data Recovery
- AC-45: Data Storage
- AC-46, AC-47: Data Transfer
- AC-48: Data Storage
- AC-49, AC-50: Security Assurances

**FunSAMP Baseline**
- AC-1: Access Control
- AC-2: Authentication
- AC-3: Security Assurances
- AC-11, AC-12, AC-13: Authorization Controls
- AC-14, AC-15: Accountability
- AC-16: Confidentiality
- AC-17: Integrity
- AC-18: Availability
- AC-19: Risk Assessment
- AC-20: Risk Management
- AC-21, AC-22, AC-23: Key Management
- AC-24, AC-25: Cryptography
- AC-26, AC-27: Data Lifecycle Management
- AC-28, AC-29: Incident Response
- AC-30: Data Export
- AC-31, AC-32: Data Export Controls
- AC-33: Data Recovery
- AC-34, AC-35: Data Retention
- AC-36: Data Storage
- AC-37, AC-38: Data Transfer
- AC-39, AC-40, AC-41: Security Assurances
- AC-42: Data Loss Prevention
- AC-43, AC-44: Data Recovery
- AC-45: Data Storage
- AC-46, AC-47: Data Transfer
- AC-48: Data Storage
- AC-49, AC-50: Security Assurances

**Additional Controls**
- AC-1: Access Control
- AC-2: Authentication
- AC-3: Security Assurances
- AC-11, AC-12, AC-13: Authorization Controls
- AC-14, AC-15: Accountability
- AC-16: Confidentiality
- AC-17: Integrity
- AC-18: Availability
- AC-19: Risk Assessment
- AC-20: Risk Management
- AC-21, AC-22, AC-23: Key Management
- AC-24, AC-25: Cryptography
- AC-26, AC-27: Data Lifecycle Management
- AC-28, AC-29: Incident Response
- AC-30: Data Export
- AC-31, AC-32: Data Export Controls
- AC-33: Data Recovery
- AC-34, AC-35: Data Retention
- AC-36: Data Storage
- AC-37, AC-38: Data Transfer
- AC-39, AC-40, AC-41: Security Assurances
- AC-42: Data Loss Prevention
- AC-43, AC-44: Data Recovery
- AC-45: Data Storage
- AC-46, AC-47: Data Transfer
- AC-48: Data Storage
- AC-49, AC-50: Security Assurances
<table>
<thead>
<tr>
<th>Role</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>EKI</td>
<td>Does the organization maintain an up-to-date inventory of all IT hardware assets?</td>
<td>Yes</td>
</tr>
<tr>
<td>Sys Admin</td>
<td>Does the organization maintain an up-to-date inventory of all IT software and virtual machine assets?</td>
<td>Yes</td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization maintain an up-to-date inventory of all IT software and virtual machine assets?</td>
<td>Not Sure</td>
</tr>
<tr>
<td>Contracts</td>
<td>Does the organization document its information security policy and map the capabilities to what the business does?</td>
<td>Yes</td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization document its information security program's capabilities and map to what the business does?</td>
<td>Yes</td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization use documented processes for developing, documenting, disseminating, reviewing, updating, and handling exceptions to its information security policies?</td>
<td>Yes</td>
</tr>
<tr>
<td>Legal</td>
<td>Are there standard agreements for the purpose of specifying terms and conditions, including a privacy policy, intellectual property agreements, acceptable use, code of conduct, website terms and conditions, or non-disclosure and non-compete, prior to granting employees, contractors, third parties, and customers access to the organization's data, services, and systems?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**NIST Interactive Questionnaire**
<table>
<thead>
<tr>
<th>Role</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIO</td>
<td>Does the organization maintain an up-to-date inventory of all IT hardware assets?</td>
<td>Yes</td>
</tr>
<tr>
<td>CIO</td>
<td>Does the organization maintain an up-to-date inventory of all IT software and virtual machine assets?</td>
<td>Yes</td>
</tr>
<tr>
<td>CSO</td>
<td>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?</td>
<td>Yes</td>
</tr>
<tr>
<td>Sysadmin</td>
<td>Does the system assign, use, and manage data tags for specific pieces of information to facilitate data classification?</td>
<td>Yes</td>
</tr>
<tr>
<td>Contracts</td>
<td>Does the organization have processes and resources in place to support contracts, including standard clauses for system security and privacy?</td>
<td>Yes</td>
</tr>
<tr>
<td>CIO</td>
<td>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?</td>
<td>Yes</td>
</tr>
<tr>
<td>CSO</td>
<td>Does the organization use documented processes for developing, documenting, disseminating, reviewing, updating, and handling exceptions to its information security policies?</td>
<td>Yes</td>
</tr>
<tr>
<td>CSO</td>
<td>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?</td>
<td>Yes</td>
</tr>
<tr>
<td>Legal</td>
<td>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?</td>
<td>Yes</td>
</tr>
<tr>
<td>Sysadmin</td>
<td>Does the organization 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?</td>
<td>Yes</td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization manage the applicable legal and regulatory requirements involving security, including mapping those requirements to the organization’s security best practices and storing them in a risk register?</td>
<td>Yes</td>
</tr>
<tr>
<td>CISO</td>
<td>Has the organization defined its approach to governance, risk, and compliance, and refined that approach as needed?</td>
<td>Yes</td>
</tr>
<tr>
<td>CSO</td>
<td>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?</td>
<td>Yes</td>
</tr>
<tr>
<td>Sysadmin</td>
<td>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?</td>
<td>Yes</td>
</tr>
</tbody>
</table>
# 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

<table>
<thead>
<tr>
<th>Category</th>
<th>Domain</th>
<th>Capability (process or solution)</th>
<th>Revised Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify-Asset Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT IS 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical devices and systems within the system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT IS 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure Protection Services</td>
<td>End Point</td>
<td>Inventory Control</td>
<td></td>
</tr>
<tr>
<td>Information Services</td>
<td>User Directory Services</td>
<td>Location Services</td>
<td></td>
</tr>
<tr>
<td>Software platforms and applications within the system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT IS 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Support Configuration Management</td>
<td>Automated Asset Discovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT IS 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure Protection Services</td>
<td>End Point</td>
<td>Inventory Control</td>
<td></td>
</tr>
<tr>
<td>Information Services</td>
<td>User Directory Services</td>
<td>Location Services</td>
<td></td>
</tr>
</tbody>
</table>

## SP 800-150 Baseline Security Controls for Implementing Functional Capabilities

<table>
<thead>
<tr>
<th>Domain</th>
<th>K</th>
<th>L</th>
<th>M</th>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
<th>R</th>
<th>S</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP 800-150 Baseline security controls for LOW IMPACT SYSTEMS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP 800-150 Baseline security controls for MEDIUM IMPACT SYSTEMS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP 800-150 Baseline security controls for HIGH IMPACT SYSTEMS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Cybersecurity roles and responsibilities for the entire workforce and third party

- **R005** Data Governance Handling/Labeling/Security Policy
- **R006** Data Governance Data Classification
- **Information Services** (R001) Data Classification
- **R007** Policies and Standards Data Access Classification
- **S & R** Data Protection Data Lifecycle Management

## Identify-Contract Environment

- **R008** Legal Services Contracts
RMF FOR THE CLOUD ECOSYSTEM

CLOUD SECURITY RUBIK’S CUBE

OSCAL

RMF4CE
Cloud Ecosystem
Consumer’s Global View

**STEP 1:**
- IMPACT ANALYSIS
- SYSTEM CATEGORIZATION
- CSF QUESTIONNAIRE

**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)
- RE-AUTHORIZE PROVIDER

**STEP 6:**
- ONGOING MONITORING OF PROVIDER’S OPERATIONS
- ONGOING MONITORING OF CONSUMER’S CONTROLS

CLOUD SECURITY RUBIK’S CUBE

- AUTHORIZATION
- CATEGORIZATION
- MONITORING
- RISK CONTROL
- RISK ASSESSMENT
- IMPLEMENTATION
WHAT IS OSCAL?

• New “Standard of Standards” normalizing how system security controls and corresponding assessment information are represented;

• OSCAL Project Goals:
  • **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.
RMF FOR THE CLOUD ECOSYSTEM

RMF4CE
Cloud Ecosystem Consumer’s Global View

ON-GOING MONITORING OF CONSUMER’S CONTROLS
ON-GOING MONITORING OF PROVIDER’S OPERATIONS
RE-AUTHORIZE PROVIDER

STEP 1:
IMPACT ANALYSIS
- SYSTEM CATEGORIZATION
- CSF QUESTIONNAIRE

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:
PERFORM DEEPER SECURITY AUDITS
MACHINE LEARNING
ON-GOING MONITORING OF CONSUMER’S CONTROLS
ON-GOING MONITORING OF PROVIDER’S OPERATIONS
RE-AUTHORIZE PROVIDER

CLOUD SECURITY RUBIK’S CUBE

SCHEMAS

CATALOG / FRAMEWORK

PROFILE

IMPLEMENTATION (SSP)

ASSESSMENT

ASSESSMENT RESULTS
CURRENT FOCUS OF OSCAL DEVELOPMENT

- Assessment Schema
- Implementation Schema
- Profile Schema
- Catalog / Framework Schema
- Assessment Results Schema
- Mechanism Schema
- Metrics Schema
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)
**Access Control Policy and Procedures**

The organization:

- 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
- 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:**

<table>
<thead>
<tr>
<th>Priority</th>
<th>Baseline</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOW</td>
<td>AC-1</td>
</tr>
<tr>
<td>MOD</td>
<td>AC-1</td>
</tr>
<tr>
<td>HIGH</td>
<td>AC-1</td>
</tr>
</tbody>
</table>
### SP 800-53 Baseline vs OSCAL Profile

#### Table 1: Initial Control Baselines

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

```xml
<profile xmlns="http://csrc.nist.gov/ns/oscal/1.0">
  <title>SP 800-53 Low Baseline</title>
  <invoke href="..snip..">
    <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>
```
## OSCAL DELIVERABLES

<table>
<thead>
<tr>
<th>Deliverables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML and JSON Schemas</td>
<td>Validate catalogs and profiles against constraints</td>
</tr>
<tr>
<td>XSL Templates</td>
<td>Produce human-readable versions (PDFs)</td>
</tr>
<tr>
<td>CSS</td>
<td>Edit OSCAL catalogs and profiles using XML tools</td>
</tr>
<tr>
<td>Documentation</td>
<td>Define the OSCAL specification</td>
</tr>
<tr>
<td></td>
<td>Explain how organizations can convert existing catalogs and profiles into OSCAL formats</td>
</tr>
</tbody>
</table>

Posted to a NIST GitHub repo: [https://github.com/usnistgov/OSCAL](https://github.com/usnistgov/OSCAL)
Email oscal@nist.gov for access
OSCAL REPOSITORY ON GITHUB
QUESTIONS?

FOR MORE GENERAL INFORMATION: MICHAELA.IORGA@NIST.GOV.

CLOUD SECURITY RUBLIK’S CUBE IS ON GITHUB (WORK IN PROGRESS):
HTTPS://GITHUB.COM/USNISTGOV/CLOUDSECURITYRUBLIKSCUBE

FOR MORE INFORMATION REGARDING OSCAL: OSCAL@NIST.GOV.

OSCAL ON GITHUB (WORK IN PROGRESS): (EMAIL FIRST TO US FOR ACCESS TO THE PRIVATE REPOSITORY): HTTPS://GITHUB.COM/USNISTGOV/OSCAL

THANK YOU!

OSCAL TEAM WOULD LIKE TO INVITE YOUR TO COLLABORATE WITH US.