NIST Cloud Security Architecture Tool (CSAT)
Leveraging Cyber Security Framework to Architect a FISMA-compliant Cloud Solution

Dr. Michaela Iorga
NIST
October 2018
A Triple Inflection Point Marked A New IT Era
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- System updates trigger documentation (SSP) to become outdated.
The Master Keys of the Cloud Kingdom: the 3Ts

- Transparency
- Traceability
- Trust
RMF for the Cloud Ecosystem (RMF4CE)
(a global view)
CONSUMER’S LEVEL OF CONTROL IN A CLOUD ECOSYSTEM
THE CLOUD-BASED SYSTEM’S BOUNDARIES

Authorization Boundaries
RMF4CE: Additional Tasks for a Cloud Consumer

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 PROVIDER’S OPERATIONS
- RE-AUTHORIZE PROVIDER

ONGOING MONITORING OF CONSUMER’S CONTROLS
Objectives of Cloud Security Architecture Tool (CSAT)

Innovate-Simplify-Automate

- To demonstrate how the NIST Cybersecurity Framework can be aligned with the RMF and implemented using established NIST risk management processes.

- To support the use of the NIST Special Publication 800-53 security control catalog, NIST and FedRAMP baselines.

- To provide guidance for enhancing systems’ security through organization-generated control selection approach to complement, when deemed necessary, the baseline control selection approach.

- To facilitate a more effective, efficient, and cost-effective methodology of architecting, implementing and assessing cloud-based information systems.

- To promote the development of trustworthy secure cloud-based systems that support automation and near real-time monitoring.
RMF4CE
Cloud Ecosystem
Consumer’s Global View

**Tasks Supported by Cloud Security Architecture Tool (CSAT)**

**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 Consumer
- Authorize Cloud-Based Information System (based upon residual risk & risk tolerance)

**Step 5:**
- Authorize Cloud-Based Information System

**Step 6:**
- Ongoing Monitoring of Consumer’s Controls
- Ongoing Monitoring of Provider’s Operations
- Re-Authorize Provider

Tasks supported by Cloud Security Architecture Tool (CSAT).
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
- Generate System SEC Plan (SSP)

**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 Consumer’s Controls
- Ongoing Monitoring of Provider’s Operations
- Tasks Supported by Open Security Controls Assessment Language (OSCAL)

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

Cross Cutting Concerns: Security, Privacy, etc.
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 Consumer

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

Cloud Broker
- Service Intermediation
- Service Aggregation
- Service Arbitrage

Cloud Carrier

Cross Cutting Concerns: Security, Privacy, etc
SP 800-200/500-299: NIST CLOUD SECURITY REFERENCE ARCHITECTURE
Cloud Security Alliance’s TCI Reference Architecture

## SP 800-200/500-299: NIST Cloud Security Reference Architecture

### Functional Capabilities

<table>
<thead>
<tr>
<th>BOSS Human Resource</th>
<th>Roles and Responsibilities</th>
<th>Provider</th>
<th>Broker</th>
<th>Carrier</th>
<th>Auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOSS Human Resource</td>
<td>Employee Code of Conduct</td>
<td>PS</td>
<td>B</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>BOSS Compliance</td>
<td>Information Systems Regulatory</td>
<td>RA</td>
<td>B</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>BOSS Data Governance</td>
<td>Data Ownership - Personnel</td>
<td>RA</td>
<td>B</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>BOSS Data Governance</td>
<td>Data Classification</td>
<td>RA</td>
<td>B</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>BOSS Security Monitoring</td>
<td>Managed (Outsourced) Security</td>
<td>SA</td>
<td>B</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>BOSS Legal Services</td>
<td>Contracts</td>
<td>SA</td>
<td>B</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>BOSS Security Monitoring</td>
<td>Honey Pot</td>
<td>SC</td>
<td>B</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>BOSS Security Monitoring</td>
<td>Real Time Intrusion Detection</td>
<td>SC</td>
<td>B</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>BOSS Data Governance</td>
<td>Rules for Data Retention</td>
<td>SI</td>
<td>B</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>BOSS Security Monitoring</td>
<td>SIEM Platform</td>
<td>SI</td>
<td>B</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>BOSS Security Monitoring</td>
<td>Anti-Phishing</td>
<td>SI</td>
<td>B</td>
<td>B</td>
<td>A</td>
</tr>
</tbody>
</table>

### S & RM Privilege Management

<table>
<thead>
<tr>
<th>S &amp; RM Privilege Management</th>
<th>Authentication Services</th>
<th>Out-Of-The-Box (OTB) Auth</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
<th>Carrier</th>
<th>Auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege Management</td>
<td>Authentication Services</td>
<td>Out-Of-The-Box (OTB) Auth</td>
<td>IA</td>
<td>IA</td>
<td>IA</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Privilege Management</td>
<td>Privilege Usage Management</td>
<td>Keystroke/Session Logging</td>
<td>IA</td>
<td>IA</td>
<td>IA</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Privilege Management</td>
<td>Privilege Usage Management</td>
<td>Password Vaulting</td>
<td>IA</td>
<td>IA</td>
<td>IA</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Threat and Vulnerability</td>
<td>Compliance Testing</td>
<td>Network Authentication</td>
<td>IA</td>
<td>IA</td>
<td>IA</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Infrastructure Protection</td>
<td>End-Points</td>
<td>Media Lockdown</td>
<td>MP</td>
<td>MP</td>
<td>MP</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Infrastructure Protection</td>
<td>End-Points</td>
<td>Media Lockdown</td>
<td>PL</td>
<td>PL</td>
<td>PL</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>InfoSec Management</td>
<td>Residual Risk Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance Risk A</td>
<td>Policy Management</td>
<td>Exceptions</td>
<td>RA</td>
<td>RA</td>
<td>RA</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Governance Risk B</td>
<td>Policy Management</td>
<td>Exceptions</td>
<td>RA</td>
<td>RA</td>
<td>RA</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Governance Risk B</td>
<td>Policy Management</td>
<td>Self Assessment</td>
<td>RA</td>
<td>RA</td>
<td>RA</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Threat and Vulnerability</td>
<td>Vulnerability Management</td>
<td>Application</td>
<td>RA</td>
<td>RA</td>
<td>RA</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Threat and Vulnerability</td>
<td>Vulnerability Management</td>
<td>Application</td>
<td>RA</td>
<td>RA</td>
<td>RA</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Threat and Vulnerability</td>
<td>Vulnerability Management</td>
<td>Infrastructure</td>
<td>RA</td>
<td>RA</td>
<td>RA</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Threat and Vulnerability</td>
<td>Vulnerability Management</td>
<td>DB</td>
<td>RA</td>
<td>RA</td>
<td>RA</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Threat and Vulnerability</td>
<td>Vulnerability Management</td>
<td>Penetration Testing</td>
<td>RA</td>
<td>RA</td>
<td>RA</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Threat and Vulnerability</td>
<td>Vulnerability Management</td>
<td>External</td>
<td>RA</td>
<td>RA</td>
<td>RA</td>
<td>A</td>
<td>A</td>
</tr>
</tbody>
</table>
# NIST SP 800-174: SECURITY AND PRIVACY CONTROLS FOR CLOUD-BASED FEDERAL INFORMATION SYSTEMS

<table>
<thead>
<tr>
<th>Domain</th>
<th>Container</th>
<th>Capability (process or solution)</th>
<th>Capability (process or solution)</th>
<th>NIST Baseline</th>
<th>Additional Segmentation Controls</th>
<th>FedRAMP Controls</th>
<th>FedRAMP Additional Segmentation Controls</th>
<th>NIST Baseline</th>
<th>Additional Segmentation Controls</th>
<th>FedRAMP Controls</th>
<th>FedRAMP Additional Segmentation Controls</th>
<th>PM Controls</th>
<th>Low Info Security</th>
<th>Middle Info Security</th>
<th>High Info Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Governance</td>
<td>Identity and Access Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Monitoring</td>
<td>Network Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Monitoring</td>
<td>Information System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Overview of the NIST Cybersecurity Framework

Functions
- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

Categories

Subcategories

Informative Reference
CAN BE MAPPED TO DIFFERENT STANDARDS

Identify
- Asset management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect
- Access Control
- Awareness and training
- Data Security
- Information protection and procedures
- Maintenance
- Protective Technology

Detect
- Anomalies and events
- Security continuous monitoring
- Detection process

Respond
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover
- Recovery Planning
- Improvements
- Communications
CSF FUNCTIONS & CATEGORIES

IDENTIFY
- Asset management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT
- Access Control
- Awareness and training
- Data Security
- Information protection and procedures
- Maintenance
- Protective Technology

DETECT
- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER
- Recovery Planning
- Improvements
- Communications

CSAT Approach

CSAT’s Questionnaire

IDENTIFY FUNCTIONAL CAPABILITIES & CLOUD ACTORS’ RESPONSIBILITIES

SELECT SECURITY CONTROLS (NIST & FEDRAMP BASELINES)
CSAT supports SSP generation providing traceable information for each instance of the SP 800-53 security controls of WHERE (for what purpose) the controls is needed. (Implementation details are necessary).

- CSAT supports 2 different views of the SSP:
  - FISMA compliance view (focused on baselines)
  - Hierarchical view for enhanced security assessment (focused on components and capabilities)

- Ready for use with the Open Security Controls Assessment Language (OSCAL)
  - OSCAL supports automation – will be introduced later!
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Role</strong></td>
<td><strong>Question</strong></td>
<td><strong>Response</strong></td>
<td></td>
</tr>
<tr>
<td>CIO</td>
<td>Does the organization maintain an up-to-date inventory of all IT hardware assets?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Sysadmin</td>
<td>Does the system provide location services reporting the physical location of assets, resources, facilities, people, etc.?</td>
<td>Yes</td>
<td></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>Yes</td>
<td></td>
</tr>
<tr>
<td>CIO</td>
<td>Does the organization categorize and label its data, servers, endpoints, and other assets based on their sensitivity and value in accordance with organizational policy?</td>
<td>Yes</td>
<td></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>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization document its information security program's capabilities and map these capabilities to what the business does?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</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 honor these agreements?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Legal</td>
<td>Are there standards for the purpose of specifying terms and conditions, security classifications, and any other requirements that apply to contracts?</td>
<td>Yes</td>
<td></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>
<td></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 registry?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Has the organization defined its approach to governance, risk, and compliance, and relies that approach as needed?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Sysadmin</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>
<td></td>
</tr>
<tr>
<td>CISO</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>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization manage information security threats, including identifying, categorizing, and characterizing known threats and vulnerabilities?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization use risk management principles to identify, assess, prioritize, and track risks?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization determine how to counter threats through a systematic, repeatable, documented approach?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>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?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization maintain an up-to-date inventory of all IT hardware assets?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Sysadmin</td>
<td>Does the system provide location services reporting the physical location of assets, resources, facilities, people, etc.?</td>
<td>Yes</td>
<td></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>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization categorize and label its data, servers, endpoints, and other assets based on their sensitivity and value in accordance with organizational policy?</td>
<td>Yes</td>
<td></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>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization have processes and resources in place to support contracts, including standard issues for system security and privacy?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</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 honor these agreements?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Legal</td>
<td>Are there standards for the purpose of specifying terms and conditions, security classifications, and any other requirements that apply to contracts?</td>
<td>Yes</td>
<td></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>
<td></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 registry?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Has the organization defined its approach to governance, risk, and compliance, and relies that approach as needed?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Sysadmin</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>
<td></td>
</tr>
<tr>
<td>CISO</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>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization manage information security threats, including identifying, categorizing, and characterizing known threats and vulnerabilities?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization use risk management principles to identify, assess, prioritize, and track risks?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization determine how to counter threats through a systematic, repeatable, documented approach?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>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?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization maintain an up-to-date inventory of all IT hardware assets?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Sysadmin</td>
<td>Does the system provide location services reporting the physical location of assets, resources, facilities, people, etc.?</td>
<td>Yes</td>
<td></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>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization categorize and label its data, servers, endpoints, and other assets based on their sensitivity and value in accordance with organizational policy?</td>
<td>Yes</td>
<td></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>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization have processes and resources in place to support contracts, including standard issues for system security and privacy?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</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 honor these agreements?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Legal</td>
<td>Are there standards for the purpose of specifying terms and conditions, security classifications, and any other requirements that apply to contracts?</td>
<td>Yes</td>
<td></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>
<td></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 registry?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Has the organization defined its approach to governance, risk, and compliance, and relies that approach as needed?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Sysadmin</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>
<td></td>
</tr>
<tr>
<td>CISO</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>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization manage information security threats, including identifying, categorizing, and characterizing known threats and vulnerabilities?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization use risk management principles to identify, assess, prioritize, and track risks?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization determine how to counter threats through a systematic, repeatable, documented approach?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>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?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>Question</td>
<td>Response</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>CO</td>
<td>Does the organization maintain an up-to-date inventory of all IT hardware assets?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</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>
<td></td>
</tr>
<tr>
<td>Sysadmin</td>
<td>Does the organization have processes in place to support contracts? A contract template is in place that includes contract clauses for system security and privacy.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CO</td>
<td>Does the organization have processes in place to support contracts? A contract template is in place that includes contract clauses for system security and privacy.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CISO</td>
<td>Does the organization have processes in place to support contracts? A contract template is in place that includes contract clauses for system security and privacy.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Sysadmin</td>
<td>Does the organization have processes in place to support contracts? A contract template is in place that includes contract clauses for system security and privacy.</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

### NIST Interactive Questionnaire Results

<table>
<thead>
<tr>
<th>Column A: CO Subcategory ID</th>
<th>Column B: CISP Technology Description</th>
<th>Column C: Capability (pass or fail)</th>
<th>Column D: Revised Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMA-1</td>
<td>Prevalent Devices and Systems within the organization are inventoried</td>
<td>Automated Asset Discovery</td>
<td></td>
</tr>
<tr>
<td>EMA-2</td>
<td>Software platforms and applications within the organization are inventoried</td>
<td>Automated Asset Discovery</td>
<td></td>
</tr>
</tbody>
</table>

### Additional Suggested Controls

- **Contract Management**: Ensure that all contracts related to the organization's IT assets include clauses on system security and privacy.
- **Data Classification**: Implement data classification policies to identify sensitive data and apply appropriate security controls.
- **User Access Controls**: Implement strong user access controls to limit access to sensitive systems and data.
- **Physical Security**: Ensure physical security measures are in place to protect IT assets and data centers.
- **Incident Response**: Develop and maintain an effective incident response plan to quickly address security breaches and minimize impact.

### Key Findings

- The organization's inventory of IT assets is up-to-date and includes physical and digital assets.
- The software platforms and applications within the organization are inventoried and classified.
- There are standardized processes for specifying terms and conditions, including a privacy policy and intellectual property agreements.
- The organization associates 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.
- The organization manages 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.
# CLOUD SECURITY ARCHITECTURE TOOL (CSAT)

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

<table>
<thead>
<tr>
<th>NIST Interactive Questionnaire Results</th>
<th>SP 800-53 RA security controls for LOW-IMPACT SYSTEMS</th>
<th>SP 800-53 RA security controls for MODERATE-IMPACT SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identify Asset Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Physical devices and systems within the organization are inventoried</strong></td>
<td>CA-7.DM-2</td>
<td>CA-7.DM-2</td>
</tr>
<tr>
<td><strong>Cloud Security Architecture Tool (CSAT)</strong></td>
<td>CM-3</td>
<td>CM-3</td>
</tr>
<tr>
<td><strong>ITDS Service Support</strong></td>
<td>CA-7.DM-2</td>
<td>CA-7.DM-2</td>
</tr>
<tr>
<td><strong>Configuration Management</strong></td>
<td>CM-3</td>
<td>CM-3</td>
</tr>
<tr>
<td><strong>Automated Asset Discovery</strong></td>
<td>CA-7.DM-2</td>
<td>CA-7.DM-2</td>
</tr>
<tr>
<td><strong>CM-3</strong></td>
<td>CM-3</td>
<td>CM-3</td>
</tr>
<tr>
<td><strong>Functional controls</strong></td>
<td>CA-7.DM-2</td>
<td>CA-7.DM-2</td>
</tr>
<tr>
<td><strong>CM-3</strong></td>
<td>CM-3</td>
<td>CM-3</td>
</tr>
<tr>
<td><strong>SP 800-53 RA user</strong></td>
<td>CA-7.DM-2</td>
<td>CA-7.DM-2</td>
</tr>
<tr>
<td><strong>CM-3</strong></td>
<td>CM-3</td>
<td>CM-3</td>
</tr>
<tr>
<td><strong>Software platforms and applications within the organization are monitored</strong></td>
<td>CA-7.DM-2</td>
<td>CA-7.DM-2</td>
</tr>
<tr>
<td><strong>SP 800-53 RA user</strong></td>
<td>CM-3</td>
<td>CM-3</td>
</tr>
<tr>
<td><strong>CM-3</strong></td>
<td>CM-3</td>
<td>CM-3</td>
</tr>
<tr>
<td><strong>Identify Business Environment</strong></td>
<td>CA-7.DM-2</td>
<td>CA-7.DM-2</td>
</tr>
<tr>
<td><strong>SP 800-53 RA user</strong></td>
<td>CM-3</td>
<td>CM-3</td>
</tr>
<tr>
<td><strong>CM-3</strong></td>
<td>CM-3</td>
<td>CM-3</td>
</tr>
</tbody>
</table>

## Key Considerations
- **Identify Asset Management**
- **Physical devices and systems within the organization are inventoried**
- **Cloud Security Architecture Tool (CSAT)**
- **ITDS Service Support**
  - **Configuration Management**
  - **Automated Asset Discovery**
  - **Functional controls**
    - CA-7.DM-2
    - CM-3
- **Software platforms and applications within the organization are monitored**
  - CA-7.DM-2
  - CM-3
- **Identify Business Environment**
  - CA-7.DM-2
  - CM-3

**Notes:**
- The table above outlines suggested functional capabilities and security controls based on the answers to the Questionnaire.
- For detailed descriptions and additional controls, refer to the SP 800-53 RA security controls for LOW-IMPACT and MODERATE-IMPACT SYSTEMS.
- Each entry represents a recommended security control or capability.
- The table includes references to specific controls and standards, such as NIST 800-53 RA.
CLOUD SECURITY ARCHITECTURE TOOL (CSAT)
Cloud Security Architecture Tool on GitHub

CSAT can leverage Open Security Controls Assessment Language (OSCAL) to assist with System Security Plans’ (SSP) generation & to support assessments’ automation and continuous monitoring.
What is OSCAL?

- A new “Standard of Standards” that normalizes how system security controls and corresponding assessment information are represented;

  - **Standardized**: OSCAL provides an open, standardized way of representing security control, control implementation, and assessment information that can be used by both humans and machines.

  - **Interoperable**: OSCAL is well-defined allowing development of OSCAL-enabled tools that are interoperable and use information consistently.

  - **Easy to use**: OSCAL machine-readable content can be converted to human-readable formats, and developed OSCAL-enabled tools are available for organizations to build, customize, and use OSCAL information.

- Improves the efficiency, accuracy, and consistency of system security assessments.
OPEN SECURITY CONTROLS ASSESSMENT LANGUAGE (OSCAL)
**OSCAL Workflow**

**Control Documentation**
- Select appropriate catalog(s) of controls
  - NIST 800.53
  - COBIT 5
  - ISO/IEC 27001/2
  - etc.

**Baseline Documentation**
- Select an appropriate existing baseline
- Tailor the selected baseline for implementation
- Create a custom baseline

**System Security Plan (SSP)**
- Align and implement baseline against OSCAL-enabled system components
- Address gaps

**Security Assessment Plan (SAP)**
- Identify and use questionnaires and automated tests to demonstrate compliance (e.g. OCIL, SCAP)

**Security Assessment Results (SAR)**
- Produce automated Audit Results and POA&Ms based on test plan and assessed implementation

**System Security Plan (SSP)**
- Align and implement baseline against OSCAL-enabled system components
- Address gaps

**Security Assessment Results (SAR)**
- Produce automated Audit Results and POA&Ms based on test plan and assessed implementation

**Catalog / Framework**
- Select an appropriate existing baseline

**Profile**
- Tailor the selected baseline for implementation

**Implementation**
- Align and implement baseline against OSCAL-enabled system components

**Assessment**
- Identify and use questionnaires and automated tests to demonstrate compliance (e.g. OCIL, SCAP)

**Assessment Results**
- Produce automated Audit Results and POA&Ms based on test plan and assessed implementation
An Example OSCAL Information Flow

- Provide requirements traceability from control definition through assessment
- Allows control, implementation, and assessment data to be provided by and linked to by different organizations
Parallel approach:

* From the top down

FedRAMP SSP

Ch 1-12 (GSA team)

Ch 13: Controls

SSP in OSCAL

*From the bottom up

Component Definition

- Provided by the owner or CSP
- Examples of Component Diagrams
  https://diagrams.fr.cloud.gov/

System Specification

(=aggregation of Capabilities)

Capability Specification

(=aggregation of Components)

Components Specification

Examples of Component Diagrams
https://diagrams.fr.cloud.gov/
OSCAL Documentation: https://pages.nist.gov/OSCAL/

OSCAL Overview

Before explaining what OSCAL is, it is important to define three key OSCAL terms:

- **Control**: A safeguard or countermeasure designed to satisfy a set of defined security and/or privacy requirements. While this is based on the NIST Special Publication (SP) 800-53 definition of “control”, in the context of OSCAL it refers to a similar kind of requirement from a control catalog.
- **Catalog**: A set of security control definitions. Examples include the hundreds of controls in NIST SP 800-53 Revision 4 Appendix F, the 100+ controls in ISO 27002, and the practices in COBIT 8.
- **Profile**: A set of security requirements, where meeting each requirement necessitates implementing one or more security controls. Also called a baseline or overlay. Examples include the control baselines in NIST SP 800-53, the FedRAMP baselines, and the PCI DSS requirements.

The purpose of OSCAL

OSCAL is attempting to address a number of challenges around security controls and security control assessment. The core challenge, and one of the primary reasons for creating OSCAL, is that concepts like security controls and profiles are represented today largely in proprietary ways. In many cases they are written in prose documents that are imprecise, lead to differences in interpretation, and are not machine-readable, meaning that the prose instructions require someone to do data entry into a tool in order for the tool to use the information.

Organizations are also struggling with information systems that have many different components. Some components require the use of different profiles per component; this is commonly the case with cloud environments. Also, cloud environments can be multitenant or have mixed ownership of components. We need to be able to assess the security of these systems against a number of requirements, owners, etc.—to do that simultaneously and provide these views to stakeholders.

On top of that there are situations where a single system needs to support multiple regulatory frameworks. For example, the U.S. Department of Veterans Affairs is a federal agency (Federal Information Security Modernization Act (FISMA) and NIST Cybersecurity Framework requirements) and a healthcare institution (Health Insurance Portability and Accountability Act (HIPAA) requirements) that has credit card transactions (Payment Card Industry Data Security Standard (PCI DSS)). There is no shortage of requirements for some organizations that have multiple regulatory frameworks.

Assessing all these security controls is extremely complex. Because of that complexity, it’s largely a manual process today. The OSCAL project is trying to change that by standardizing how security controls are represented, how a control implementation for a given system is represented, and how that information is best used and reported generated in a standardized way that can be used by both humans and machines. That means formats are needed that can be generated by machines for communicating with other machines, but can also easily be reformatted so humans can read the information. By standardizing the representation of this information, OSCAL information can be interoperable by having a well-defined specification with information that’s going to be used, imported, and used interoperably for security control assessments. The goal is to keep OSCAL as simple as possible and provide extensive automation for tools to use.
Profile Example 1

This example shows an excerpt of the profile corresponding to the NIST SP 800-53 low baseline. This excerpt omits additional `<call control>` lines but is otherwise complete. This profile has a title, imports the NIST SP 800-53 catalog, and specifies numerous controls from that catalog. This is a very simple example.

Profile Example 2

This example shows an excerpt of a more complex profile than the previous example. This example is based on the FedRAMP low baseline, which can be found at https://www.fedramp.gov/resources/documents-2016-under-key-cloud-service-provider-csp-documents. The first notable difference from the first example is that this profile references two other profiles: SP800-53-LOW-baseline and SP800-53-MODERATE-baseline. A single profile can reference zero or more catalogs and zero or more other profiles. (For brevity, the lists of controls referenced from each profile have been truncated.) The second notable difference is that this profile modifies the controls (via the `<modify>` element) by setting parameters for particular controls (using `<set-param>` elements) and altering the language of other controls (using the `<alter` and `<augment>` elements). This causes the profile to be customized to meet the specific needs of the parties using it.
Questions?

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

CLOUD SECURITY ARCHITECTURE TOOL ON GITHUB:
HTTPS://GITHUB.COM/USNISTGOV/CLOUDSECURITYARCHITECTURETOOL

OSCAL ON GITHUB: HTTPS://GITHUB.COM/USNISTGOV/OSCAL

OSCAL-SPECIFIC INQUIRIES: OSCAL@NIST.GOV

THANK YOU!