Cloudy with Showers of Business Opportunities and and a Good Chance of Security and Accountability

Not All Clouds are Equal – Can You Tell the Difference?
Security and Privacy Controls for Cloud-based Federal Information Systems

Dr. Michaela Iorga,
Senior Security Technical Lead for Cloud Computing
Co-Chair, Cloud Security WG
Co-Chair, Cloud Forensics Science WG

May, 2015
The World is changing...

There I was, stuck in a Chinese firewall, when suddenly our router lit up like the Fourth of July... Bots to the left of me, Trojans to the right... We lost some good servers that day.

FUTURE WAR STORIES
Many Shades of Cloud Views...
Security & Privacy may mean different things to different people...

Navy

Army

Marines

Air Force

Slide courtesy of Bill Murray, AWS, Amazon
Balancing Cloud Benefits and Risks ...

... is not easy but it can be done.

- Reduce Capital Cost
- Improve Business Agility
- Increase Productivity & Collaboration
- Increase Competitiveness
- Lower Staff Cost

- Preserve Security Posture
- Improve Security
- Minimize Business Risk
- Increase Availability
- Preserve Privacy
## NIST Risk Management Standards

- Standards for Security Categorization of Federal Information and Information Systems (FIPS 199); Feb 2004
- Guide for Mapping Types of Information and Information Systems to Security Categories (SP 800-60 Rev. 1); Aug 2008
- Minimum Security Requirements for Federal Information and Information Systems (FIPS 200); Mar 2006
- Security Considerations in the System Development Life Cycle (SP 800-64 Rev. 2); Oct 2008
- Managing Information Security Risk: Organization, Mission, and Information System View (SP 800-39); Mar 2011
- Guide for Conducting Risk Assessments (SP 800-30 Rev. 1); Sep 2012
- Security and Privacy Controls for Federal Information Systems and Organizations (SP 800-53 Rev. 4); Apr 2013
Other Related NIST Special Publications

• Performance Measurement Guide for Information Security (SP 800-55 Rev. 1); Jul 2008
• Contingency Planning Guide for Federal Information Systems (SP 800-34 Rev. 1); May 2010
• Information Security Continuous Monitoring for Federal Information Systems and Organizations (SP 800-137); Sep 2011
• Computer Security Incident Handling Guide (SP 800-61 Rev. 2); Aug 2012

New NIST Special Publications (Drafts)

• DRAFT Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems (SP 800-160 Draft); May 12, 2014
• NIST SP 500-299: NIST Cloud Computing Security Reference Architecture (draft)
• NIST SP 800-173: Guide for Applying the Risk Management Framework to Cloud-based Federal Information Systems; work in progress
• NIST SP 800-174: Security and Privacy Controls for Cloud-based Federal Information Systems; work in progress
NIST CC Security Reference Architecture - Approach

NIST Security Reference Architecture – formal model

NIST Security Reference Architecture – security components

TCI Reference Architecture

Mapping components to architecture
NIST CC Reference Architecture (SP 500-292) with Cross Cutting Concerns shown

Cloud Consumer

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 Broker

Service Intermediation

Service Aggregation

Service Arbitrage

Cloud Carrier

Cross Cutting Concerns: Security, Privacy, etc
NIST Security Reference Architecture – formal model
NIST SWG leverages Cloud Security Alliance’s Enterprise Architecture (before: Trusted Cloud Initiative - Reference Architecture)

**NIST Security Reference Architecture**

- security components -

| Components descriptions available on CSA’s interactive site: [https://research.cloudsecurityalliance.org/coi/explore/](https://research.cloudsecurityalliance.org/coi/explore/) |

<table>
<thead>
<tr>
<th>BOSS</th>
<th>Human Resource</th>
<th>Roles and Responsibilities</th>
<th>PS</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOSS</td>
<td>Human Resource</td>
<td>Employee Code of Conduct</td>
<td>PS</td>
</tr>
<tr>
<td>BOSS</td>
<td>Compliance</td>
<td>Information Systems Regulatory</td>
<td>RA</td>
</tr>
<tr>
<td>BOSS</td>
<td>Data Governance</td>
<td>Data Ownership - Personnel</td>
<td>RA</td>
</tr>
<tr>
<td>BOSS</td>
<td>Data Governance</td>
<td>Data Classification</td>
<td>RA</td>
</tr>
<tr>
<td>BOSS</td>
<td>Security Monitoring</td>
<td>Managed (Outsourced) Security</td>
<td>SA</td>
</tr>
<tr>
<td>BOSS</td>
<td>Security Monitoring</td>
<td>Honey Pot</td>
<td>SC</td>
</tr>
<tr>
<td>BOSS</td>
<td>Security Monitoring</td>
<td>Real Time Internetwork Defense</td>
<td>SC</td>
</tr>
<tr>
<td>BOSS</td>
<td>Data Governance</td>
<td>Rules for Data Retention</td>
<td>SI</td>
</tr>
<tr>
<td>BOSS</td>
<td>Security Monitoring</td>
<td>SIEM Platform</td>
<td>SI</td>
</tr>
<tr>
<td>BOSS</td>
<td>Security Monitoring</td>
<td>Anti Phishing</td>
<td>SI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actors Analysis validated</th>
<th>Actors Analysis reorg</th>
<th>CC Ecosystem validated</th>
<th>CC Ecosystem reorg</th>
<th>800-53 r4 control families</th>
<th>800-53 r4 controls</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>S &amp; RM</th>
<th>Privilege Management</th>
<th>Authentication Services</th>
<th>Out-of-The-Box (OTB) Auth</th>
<th>IA</th>
</tr>
</thead>
<tbody>
<tr>
<td>S &amp; RM</td>
<td>Privilege Management</td>
<td>Privilege Usage Management</td>
<td>Keystroke/Session Logging</td>
<td>IA</td>
</tr>
<tr>
<td>S &amp; RM</td>
<td>Privilege Management</td>
<td>Privilege Usage Management</td>
<td>Password Vaulting</td>
<td>IA</td>
</tr>
<tr>
<td>S &amp; RM</td>
<td>Threat and Vulnerability</td>
<td>Compliance Testing</td>
<td>Network Authentication</td>
<td>IA</td>
</tr>
<tr>
<td>S &amp; RM</td>
<td>Infrastructure Protection</td>
<td>End-Point</td>
<td>Forensic Tools</td>
<td>PA</td>
</tr>
<tr>
<td>S &amp; RM</td>
<td>Infrastructure Protection</td>
<td>End-Point</td>
<td>Media Lockdown</td>
<td>MP</td>
</tr>
<tr>
<td>S &amp; RM</td>
<td>InfoSec Management</td>
<td>Residual Risk Management</td>
<td>PL</td>
<td></td>
</tr>
<tr>
<td>S &amp; RM</td>
<td>Governance Risk &amp; Policy Management</td>
<td>Exceptions</td>
<td>FA</td>
<td></td>
</tr>
<tr>
<td>S &amp; RM</td>
<td>Governance Risk &amp; Policy Management</td>
<td>Sell Assessment</td>
<td>FA</td>
<td></td>
</tr>
<tr>
<td>S &amp; RM</td>
<td>InfoSec Management</td>
<td>Risk Dashboard</td>
<td>RA</td>
<td></td>
</tr>
<tr>
<td>S &amp; RM</td>
<td>Threat and Vulnerability</td>
<td>Vulnerability Management</td>
<td>application</td>
<td>RA</td>
</tr>
<tr>
<td>S &amp; RM</td>
<td>Threat and Vulnerability</td>
<td>Artifacts Management</td>
<td>Internal</td>
<td>RA</td>
</tr>
<tr>
<td>S &amp; RM</td>
<td>Threat and Vulnerability</td>
<td>Penetration Testing</td>
<td>External</td>
<td>RA</td>
</tr>
</tbody>
</table>
## NIST Security Reference Architecture

### Security Index System

<table>
<thead>
<tr>
<th>BOSS</th>
<th>Security Index System</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Compliance: Intellectual Property</td>
</tr>
<tr>
<td>5</td>
<td>Data Governance: Handling/Labeling/Security</td>
</tr>
<tr>
<td>6</td>
<td>Data Governance: Clear Desk Policy</td>
</tr>
<tr>
<td>7</td>
<td>Data Governance: Rules for Information</td>
</tr>
<tr>
<td>9</td>
<td>Human Resource Security: Employee Awareness</td>
</tr>
<tr>
<td>9</td>
<td>Security Monitoring Services: Market Threat Intelligence</td>
</tr>
<tr>
<td>10</td>
<td>Security Monitoring Services: Knowledge Base</td>
</tr>
<tr>
<td>11</td>
<td>Compliance: Audit Planning</td>
</tr>
<tr>
<td>12</td>
<td>Compliance: Internal Audits</td>
</tr>
<tr>
<td>13</td>
<td>Security Monitoring Services: Event Mining</td>
</tr>
<tr>
<td>14</td>
<td>Security Monitoring Services: Event Correlation</td>
</tr>
<tr>
<td>15</td>
<td>Security Monitoring Services: Email Journaling</td>
</tr>
<tr>
<td>16</td>
<td>Security Monitoring Services: User Behaviors and Profile</td>
</tr>
<tr>
<td>17</td>
<td>Legal Services: E-Discovery</td>
</tr>
<tr>
<td>18</td>
<td>Legal Services: Incident Response Legal</td>
</tr>
<tr>
<td>19</td>
<td>Internal Investigations: Forensic Analysis</td>
</tr>
<tr>
<td>20</td>
<td>Internal Investigations: e-Mail Journaling</td>
</tr>
<tr>
<td>21</td>
<td>Compliance: Independent Audits</td>
</tr>
<tr>
<td>22</td>
<td>Compliance: Third Party Audits</td>
</tr>
<tr>
<td>23</td>
<td>Operational Risk Management: Business Impact Analysis</td>
</tr>
<tr>
<td>24</td>
<td>Operational Risk Management: Business Continuity</td>
</tr>
<tr>
<td>25</td>
<td>Operational Risk Management: Crisis Management</td>
</tr>
<tr>
<td>26</td>
<td>Operational Risk Management: Risk Management</td>
</tr>
<tr>
<td>27</td>
<td>Operational Risk Management: Independent Risk</td>
</tr>
<tr>
<td>28</td>
<td>Security Monitoring Services: Database Monitoring</td>
</tr>
<tr>
<td>29</td>
<td>Security Monitoring Services: Application Monitoring</td>
</tr>
<tr>
<td>30</td>
<td>Security Monitoring Services: End-Point Monitoring</td>
</tr>
<tr>
<td>31</td>
<td>Security Monitoring Services: Cloud Monitoring</td>
</tr>
<tr>
<td>32</td>
<td>Data Governance: Secure Disposal of Data</td>
</tr>
</tbody>
</table>
NIST Security Reference Architecture
– Aggregated Security Index System – Heat Map
ISO/IEC based CC Security Reference Architecture

ISO/IEC Security Reference Architecture – formal model

Mapping components to architecture

RMF2C + methodology

ISO/ICE Reference Architecture

TCI Reference Architecture -> functional capabilities
OUR APPROACH IS MODULAR – YOU CAN SUBSTITUTE COMPONENTS

E.g. ISO/IEC based CC Security Reference Architecture -

ISO/IEC Security Reference Architecture – formal model

ISO/IEC Reference Architecture

RMF2C + methodology

YOUR OWN SET OF COMPONENTS
OR
USE CSA'S CCM!!
<table>
<thead>
<tr>
<th>Control Domain</th>
<th>CCM V3.0 Control ID</th>
<th>Control Specification</th>
<th>Domain &gt; Container &gt; Capability</th>
<th>Public</th>
<th>Private</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datacenter Security Unauthorized Persons Entry</td>
<td>DCS-08</td>
<td>Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.</td>
<td>SRM &gt; Policies and Standards &gt; Information Security Policy (Facility Security Policy)</td>
<td>provider</td>
<td>x</td>
</tr>
<tr>
<td>Datacenter Security User Access</td>
<td>DCS-09</td>
<td>Physical access to information assets and functions by users and support personnel shall be restricted.</td>
<td>Infra Services &gt; Facility Security &gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption &amp; Key Management Entitlement</td>
<td>EKM-01</td>
<td>All entitlement decisions shall be derived from the identities of the entities involved. These shall be managed in a corporate identity management system. Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.</td>
<td>SRM &gt; Cryptographic Services &gt; Key Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption &amp; Key Management Key Generation</td>
<td>EKM-02</td>
<td>Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place)</td>
<td>SRM &gt; Key Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption &amp; Key Management Sensitive Data Protection</td>
<td>EKM-03</td>
<td>Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.</td>
<td>SRM &gt; Data Protection &gt; Cryptographic Services - Data-At-Rest Encryption, Cryptographic Services - Data-in-Transit Encryption</td>
<td>shared</td>
<td>x</td>
</tr>
<tr>
<td>Encryption &amp; Key Management Storage and Access</td>
<td>EKM-04</td>
<td>Strong encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.</td>
<td>SRM &gt; Cryptographic Services &gt; Key Management</td>
<td>shared</td>
<td>x</td>
</tr>
<tr>
<td>Governance and Risk Management Baseline Requirements</td>
<td>GRM-01</td>
<td>Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized.</td>
<td>SRM &gt; Governance Risk &amp; Compliance &gt; Technical Standards</td>
<td>shared</td>
<td>x</td>
</tr>
<tr>
<td>Governance and Risk Management Data Focus Risk Assessments</td>
<td>GRM-02</td>
<td>Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements</td>
<td>BOSS &gt; Operational Risk Management &gt; Independent Risk Management</td>
<td>shared</td>
<td>x</td>
</tr>
<tr>
<td>Governance and Risk Management Management Oversight</td>
<td>GRM-03</td>
<td>Managers are responsible for maintaining awareness of, and complying with, security policies, procedures and standards that are relevant to their area of responsibility.</td>
<td>BOSS &gt; Human Resources Security &gt; Roles and Responsibilities</td>
<td>shared</td>
<td>x</td>
</tr>
</tbody>
</table>
INFORMATION SECURITY POLICIES

Broad statements of management intent that guide the information security operations of an organization. Policies are implemented by standards and procedures and compliance can be verified through audit.

Cloud Controls Matrix (CCM) Data

FS-01 | Facility Security | Policy

CONTROL SPECIFICATION +
ARCHITECTURAL RELEVANCE +
CORP GOV RELEVANCE +
CLOUD SERVICE DELIVERY MODEL APPLICABILITY +
SP 500-299: Cloud Security Reference Architecture

RMF2C + Methodology

"Guide for Applying Risk Management Framework to Cloud-based Federal Information Systems"
NIST SP 800-173

HELPS SELECT BEST-FITTING CLOUD ARCHITECTURE
Guide for Applying Risk Management Framework to Cloud-based Federal Information Systems

NIST SP 800-173
- work in progress -

Learn how to build trust & how FedRAMP or STAR can help..
NIST: Research – Challenging Security Requirements for the USG Cloud Adoption, (whitepaper)

MeriTalk:
We asked 150 Federal IT leaders what stopping them back from committing to the cloud. The answers may surprise you:

1. 5-year-long-term contracts keep them in line
2. 75% fear losing control of data

1.... If I like it, it's mine.
2.... If it's in my hand, it's mine.
3.... If I can take it from you, it's mine.
4.... If I had it a little while ago, it is mine.
5.... If it's mine, it must not appear to be yours in any way.
6.... If I'm doing or building something, all the pieces are mine.
7.... If it looks just like mine, it's mine.
8.... If I saw it first, it's mine.
9.... If you are playing with something and you put it down, it automatically becomes mine.
10.... If it is broken, it's yours.

NO TRUST RELATION
BUILD TRUST
SUCCESS
“Trust is an important concept related to risk management. How organizations approach trust influences their behaviors and their internal and external trust relationships. [...] The reliance on IS services results in the need for trust relationships among organizations” *

① Validated Trust. One organization obtains a body of evidence regarding the actions of another organization and uses that evidence to establish a level of trust with the other organization.

② Direct Historical. The track record exhibited by an organization in the past is used to establish a level of trust with other organizations.

③ Mediated Trust. An organization establishes a level of trust with another organization based on assurances provided by some mutually trusted third party.

④ Mandated Trust. An organization establishes a level of trust with another organization based on a specific mandate issued by a third party in a position of authority.

⑤ Hybrid Trust. An organization uses one of the previously described models in conjunction with another model(s).

*NIST SP 800-39: Managing Information Security Risk; Organization, Mission, and Information System View*
Trustworthiness requires visibility into Provider’s practices and risk/information security decisions to understand risk tolerance. But level of trust can vary & the accepted risk depends on the established trust relation.
NIST’s Work – Helps Consumer Deal With an Iceberg Architecture

Risk Management Framework (SP 800-37 Rev1):
Step 1: Categorize Information System
Step 2: Select Security Controls
Step 3: Implement Security Controls
Step 4: Assess Security Controls
Step 5: Authorize Information System
Step 6: Monitor Security Controls
(Repeat process as necessary)

Cloud-adapted Risk Management Framework (SP 800-173, draft):
Step 1: Categorize: System to be migrated
Step 2: Select: Security Requirements, perform a Risk Assessment & select Security Controls
Step 3: Identify: best-fitting Cloud Architecture
    Implement Cloud-based solution
Step 4: Assess Service Provider(s) & Controls
Step 5: Authorize Use of Service
Step 6: Monitor Service Provider [on-going, near-real-time] (Repeat process as necessary)
Applying Risk Management Framework to Cloud-based Federal Information Systems

**Risk Management Framework (SP 800-37 Rev1):**

- **Step 1:** Categorize Information System
- **Step 2:** Select Security Controls
- **Step 3:** Implement Security Controls
- **Step 4:** Assess Security Controls
- **Step 5:** Authorize Information System
- **Step 6:** Monitor Security Controls
  
  (Repeat process as necessary)

**Cloud-adapted Risk Management Framework (SP 800-173, draft):**

- **Step 1:** Categorize: System to be migrated
- **Step 2:** Select: Security Requirements, perform a Risk Assessment & select Security Controls
- **Step 3:** Identify: best-fitting Cloud Architecture
  Implement Cloud-based solution
- **Step 4:** Assess Service Provider(s) & Controls
- **Step 5:** Authorize Use of Service
- **Step 6:** Monitor Service Provider [on-going, near-real-time] (Repeat process as necessary)

A&A or C&A Authorities provide a standardized approach to security assessment or certification and authorization.
Applying Risk Management Framework to Cloud-based Federal Information Systems

(NIST SP 800-173)

Table of Contents

CHAPTER ONE .................................................................................................................. 3
INTRODUCTION .............................................................................................................. 3
1.1 BACKGROUND ........................................................................................................ 4
1.1.1 Risk-based Assessment and Risk Management for IT Systems ....................... 5
1.2 PURPOSE AND APPLICABILITY.............................................................................. 6
1.3 TARGET AUDIENCE ............................................................................................... 7
1.4 ORGANIZATION OF THE DOCUMENT .................................................................. 8
CHAPTER TWO ............................................................................................................... 9
THE FUNDAMENTALS ............................................................................................. 9
2.1 INTEGRATED CLOUD ECOSYSTEM WIDE RISK MANAGEMENT ................... 10
2.1.1 Security Conservation Principle ...................................................................... 11
2.1.2 Privacy Conservation Principle ......................................................................... 12
2.1.3 Cloud Actors and Risk Management ................................................................. 13
2.1.4 Cloud Deployment Model and Risk Management ............................................. 14
2.1.5 Cloud Service Models and Risk Management .................................................. 14
2.1.6 Cloud Ecosystem and Risk Management .......................................................... 16
2.2 CLOUD ECOSYSTEM DEVELOPMENT LIFECYCLE .................................... 21
2.3 CLOUD-BASED INFORMATION SYSTEM BOUNDARIES ............................ 23
2.3.1 The Unique Characteristics of Cloud Computing .............................................. 24
2.3.2 Cloud Computing Impact on the Information System Boundaries .................. 24
2.3.3 Establishing Boundaries for Cloud-based Information System ...................... 27
2.3.4 Boundaries for Complex Cloud-based Information Systems .......................... 36
2.3.5 Evolving Cloud Technology and the Effect on Information System Boundaries 37
2.4 SECURITY CONTROLS ALLOCATION ............................................................ 37
CHAPTER THREE ....................................................................................................... 39
THE PROCESS ............................................................................................................ 39
3.1 CRMF STEP 1: CATEGORIZE THE CONSUMER’S INFORMATION SYSTEM OF SERVICE 39
3.2 CRMF STEP 2: IDENTIFY SECURITY REQUIREMENTS FOR THE CONSUMER’S INFORMATION SYSTEM OF SERVICE 39
3.3 CRMF STEP 2: SELECT A CLOUD ECOSYSTEM ARCHITECTURE ................... 40
3.4 CRMF STEP 4: ASSESS AND RISK (?: CLOUD VENDORS/SOLUTIONS (?: 41
3.5 CRMF STEP 5: AUTHORIZE THE LIST OF THE CLOUD VENDORS ..................... 42
3.6 CRMF STEP 6: MONITOR the CLOUD VENDOR’S SECURITY CONTROLS (..... 42
Applying Risk Management Framework to Cloud-based Federal Information Systems

1. Follows NIST RMF (SP 800-37 Rev1) structure
2. Discusses the impact of cloud computing architecture (deployment model & service type), and cloud characteristics (multi-tenancy, resource-pooling, elasticity, etc.) on “Information System Boundary”.
3. Discusses the notion of TRUST in a cloud ecosystem, and introduces the notion of TRUST BOUNDARY
4. Introduces the “Security Conservation Principle” & “Privacy Conservation Principle”
Applying Risk Management Framework to Cloud-based Federal Information Systems

**Step 1:** Categorize Federal Information System

**Step 2:** Select: Security Requirements, perform a Risk Assessment & select Security Controls deemed necessary.

**Step 3:** Identify best-fitting Cloud Architecture & Implement cloud-based solution

Step 4: Assess Service Provider(s) & Broker (if applicable) → leverage FedRAMP P-ATOs or Agency-ATOs, or assess the controls → build necessary TRUST that the residual risk is acceptable

Step 5: Authorize Use of Service → negotiate SLAs & Security SLA

Step 6: Monitor Service Provider(s) (on-going, near-real-time); Repeat process as necessary
Security and Privacy Controls for Cloud-based Federal Information Systems

NIST SP 800-174
- work in progress -

Controls allocation matters ...
Controls’ Allocation Matters...

IaaS
- Presentation Modality
- Presentation Platform
- APIs
- Applications
- Data
- Metadata
- Content
- Integration and Middleware
- Facilities

Provider’s implemented baseline

PaaS
- Presentation Modality
- Presentation Platform
- APIs
- Applications
- Data
- Metadata
- Content
- Integration and Middleware
- Facilities

Core Connectivity and Delivery
Abstraction

Consumer’s additional needs

SaaS
- Presentation Modality
- Presentation Platform
- APIs
- Applications
- Data
- Metadata
- Content
- Integration and Middleware
- Facilities

Core Connectivity and Delivery
Abstraction

Stack image source: Cloud Security Alliance specification, 2009
Clouds are not identical ...

even when implementing same baseline controls

Stack image source: Cloud Security Alliance specification, 2009

A&A or C&A Authorities provide a standardized approach to security assessment or certification and authorization.
NOW: Identifying SP 800-53 Security and Privacy Controls for Cloud Capabilities

<table>
<thead>
<tr>
<th>Capability implementation</th>
<th>Information Protection</th>
<th>PM Controls</th>
<th>Low (info protection)</th>
<th>Moderate (info protection)</th>
<th>High (info protection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low (Capability)</td>
<td>Low (Capability)</td>
<td>Low (info</td>
<td>AC-1, AC-2, AC-3, AC-</td>
<td>AC-1, AC-2, AC-3, AC-</td>
<td>AC-1, AC-2, AC-3, AC-</td>
</tr>
<tr>
<td>Moderate (Capability)</td>
<td>Moderate (Capability)</td>
<td>Moderate</td>
<td>6, AC-17, AC-18, AC-19</td>
<td>6, AC-17, AC-18, AC-19</td>
<td>6, AC-17, AC-18, AC-19</td>
</tr>
<tr>
<td>High (Capability)</td>
<td>High (Capability)</td>
<td>High (info</td>
<td>AC-20</td>
<td>AC-20</td>
<td>AC-20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **SP 800-53 Rev4**
- **PM Controls**
- **Low (info protection)**
- **Moderate (info protection)**
- **High (info protection)**
<table>
<thead>
<tr>
<th>Capability Implementation</th>
<th>Reviewed Low(Capability implementation)</th>
<th>Reviewed Moderate(Capability implementation)</th>
<th>Reviewed High(Capability implementation)</th>
<th>PM Controls</th>
<th>Information Protection Low (info protection)</th>
<th>Moderate (info protection)</th>
<th>High (info protection)</th>
</tr>
</thead>
</table>
Security and Privacy Controls for Cloud-based Federal Information Systems (SP 800-174) & CSA’s STAR

FedRAMP

NIST SP 800-53 R4

NIST Cloud Computing Security Reference Architecture

TBD
Overview of NIST’s Current & Future Work

- SP 800-174: Security and Privacy Controls for Cloud-based Federal Information Systems
  1. Identify Security Controls
  2. Provide Implementation Guidance
  3. Provide Assessment Guidance

- SP 500-299: Guide to Applying Risk Management Framework to Cloud-based Federal Information Systems

- Security SLA

- Security Metrics

- Security Intelligence & Continuous Monitoring
Questions?

Thank you!

Additional Information

NIST Cloud Home Page:
http://www.nist.gov/itl/cloud

NIST Cloud Computing Collaborative Twiki: