Agile ATO: A New Approach to FedRAMP Documentation

Mike Brown

Excella
excella.com | @excellaco
What is FedRAMP?
FedRAMP

FISMA

NIST
**FISMA**
A law that covers all processing and storage of federal data, and each federal Agency must implement the law via NIST requirements, standards and guides.

**FedRAMP**
A government - wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services

ATO: Authority To Operate
ATO Role Players

**Developers**
Implement and document system implementation

**Independent Assessor**
Review system documentation and implementation, create assessment

**Authorizing Official**
Review security assessment, grant ATO
Other Important Roles

Leadership (CIO, CTO)
Provide funding, define roadmap

Internal Security Team
Provide feedback on controls before assessment
High Level ATO Process

1. **Development**: design, develop, and secure the system.
2. **Document**: record state of system architecture, procedures, and security compliance.
3. **Assessment**: have an independent assessor perform a security assessment.
4. **Authorization**: review assessment and grant authority to operate (ATO).
5. **Continuous Monitoring**: ensure system design continues to match documentation, resolve deficiencies.
DEVELOP

DOCUMENT

ASSESS

AUTHORIZE

MONITOR

Repeat as necessary
Agile should be both 
iterative and incremental
DEV + OPS

WALL OF UNCERTAINTY

ASSESSORS
There must be a better way.
"Our highest priority is to satisfy the customer through early and continuous delivery of valuable software."

The Agile Manifesto
Security Documentation

**TODO**
- Contingency Plan
- Rules of Behavior
- E-Auth Worksheet
- Configuration Management Plan
- Incident Response Plan

**Writing**
- System Security Plan
  
**Security Review**
- Inventory Worksheet
- Privacy Impact Assessment
- FIPS 199

**Done**
- Separation of Duties Matrix

Add a card...
The Problem: System Security Plan
AC-7 UNSUCCESSFUL LOGON ATTEMPTS

The information system:

a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and

b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.
<table>
<thead>
<tr>
<th><strong>AC-7</strong></th>
<th><strong>Control Summary Information</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Role:</td>
<td>Chief Technical Officer (CTO)</td>
</tr>
<tr>
<td>Parameter AC-7(a)-1:</td>
<td>3</td>
</tr>
<tr>
<td>Parameter AC-7(a)-2:</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Parameter AC-7(b)-1:</td>
<td>Automatically locks the account</td>
</tr>
<tr>
<td>Parameter AC-7(b)-2:</td>
<td>15 minutes</td>
</tr>
</tbody>
</table>

Implementation Status (check all that apply):
- [ ] Implemented
- [ ] Partially implemented
- [ ] Planned
- [ ] Alternative implementation
- [ ] Not applicable

Control Origination (check all that apply):
- [ ] Service Provider Corporate
- [ ] Service Provider System Specific
- [ ] Service Provider Hybrid (Corporate and System Specific)
- [ ] Configured by Customer (Customer System Specific)
- [ ] Provided by Customer (Customer System Specific)
- [ ] Shared (Service Provider and Customer Responsibility)
- [ ] Inherited from pre-existing FedRAMP Authorization for [Click here to enter text.], Date of Authorization
### AC-7 What is the solution and how is it implemented?

<table>
<thead>
<tr>
<th>Part a</th>
<th>An Active Directory authentication provider is configured to the specified lockout settings. This will prevent user access to all services that utilize AD for authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part b</td>
<td>Active Directory is configured to unlock user accounts automatically after 15 minutes. If the user cannot wait for an unlock, the user can contact the help desk for immediate assistance.</td>
</tr>
</tbody>
</table>
For a moderate impact system, there are 324 controls.

648 check boxes  1407 text boxes
The template provided by FedRAMP is 384 pages long.
Every single control is difficult.
Difficult Questions to Answer

• How many controls are Partially Implemented?
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Implementation Status</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-01</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-02</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-02 (01)</td>
<td>Partially Implemented</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-02 (02)</td>
<td>Planned</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-02 (03)</td>
<td>Alternative Implementation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-02 (04)</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-02 (05)</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-02 (07)</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-02 (09)</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-02 (10)</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-02 (12)</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-03</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-04</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-04 (21)</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-05</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-06</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-06 (01)</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-06 (02)</td>
<td>In Place</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ANTIPATTERN!
"Every piece of knowledge must have a single, unambiguous, authoritative representation within a system."

The Pragmatic Programmer by Andy Hunt and Dave Thomas
Difficult Questions to Answer

- How many controls are Partially Implemented?
- How many controls do we still need to write?
- What changed since _____?
- How many controls are waiting for review?
There must be a better way.
18F’s OpenControl Initiative
The 18F Mission

“Deliver websites, applications, and strategies that help agencies provide excellent value to the public.”

LOGIN.GOV  CLOUD.GOV
The OpenControl Project

"A YAML-Powered Antidote To Bureaucracy"

"A set of tools that restructure the process of writing, updating, and reviewing compliance documentation."
Using a defined schema increases the potential for automation and collaboration.
Intro to YAML in 30 seconds

animals:

- name: dog
  sound: bark
  feet: 4

- name: cat
  sound: meow
  feet: 4
>>> animals = yaml.load(document)["animals"]

>>> animals[0]["name"]
'dog'

>>> 
"I heard a " + x["sound"] for x in animals

["I heard a bark", "I heard a meow"]
OpenControl Process

Inputs

- General System YAML

Outputs

- FedRAMP .docx
- FedRAMP .xls
Documenting security controls in YAML
name: System X
- standard_key: NIST-800-53
  control_key: AC-7
  implementation_status: implemented
  control_origin: service_provider_system_specific
narrative:
  - key: a
    text: An Active Directory authentication provider is...
  - key: b
    text: Active Directory is configured to unlock user...
Continuous Integration Pipeline

1. Start
2. Get updated code
3. Generate
   - Create CIS .xls report
   - Inject controls into .docx
4. Calculate progress metrics
5. Email stakeholders
6. End
<table>
<thead>
<tr>
<th>AC-7</th>
<th>Control Summary Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Responsible Role: Chief Technical Officer (CTO)</td>
</tr>
<tr>
<td></td>
<td>Parameter AC-7(a)-1: 3</td>
</tr>
<tr>
<td></td>
<td>Parameter AC-7(a)-2: 5 minutes</td>
</tr>
<tr>
<td></td>
<td>Parameter AC-7(b)-1: Automatically locks the account</td>
</tr>
<tr>
<td></td>
<td>Parameter AC-7(b)-2: 15 minutes</td>
</tr>
<tr>
<td></td>
<td>Implementation Status (check all that apply):</td>
</tr>
<tr>
<td></td>
<td>• Implemented</td>
</tr>
<tr>
<td></td>
<td>□ Partially implemented</td>
</tr>
<tr>
<td></td>
<td>□ Planned</td>
</tr>
<tr>
<td></td>
<td>□ Alternative implementation</td>
</tr>
<tr>
<td></td>
<td>□ Not applicable</td>
</tr>
<tr>
<td></td>
<td>Control Origination (check all that apply):</td>
</tr>
<tr>
<td></td>
<td>□ Service Provider Corporate</td>
</tr>
<tr>
<td></td>
<td>• Service Provider System Specific</td>
</tr>
<tr>
<td></td>
<td>□ Service Provider Hybrid (Corporate and System Specific)</td>
</tr>
<tr>
<td></td>
<td>□ Configured by Customer (Customer System Specific)</td>
</tr>
<tr>
<td></td>
<td>□ Provided by Customer (Customer System Specific)</td>
</tr>
<tr>
<td></td>
<td>□ Shared (Service Provider and Customer Responsibility)</td>
</tr>
<tr>
<td></td>
<td>□ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization</td>
</tr>
</tbody>
</table>

### AC-7 What is the solution and how is it implemented?

<table>
<thead>
<tr>
<th>Part a</th>
<th>System X:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>An Active Directory authentication provider is configured to the specified lockout settings. This will prevent user access to all services that utilize AD for authentication.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part b</th>
<th>System X:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active Directory is configured to unlock user accounts automatically after 15 minutes. If the user cannot wait for an unlock, the user can contact the help desk for immediate assistance.</td>
</tr>
</tbody>
</table>
Suppose I add a COTS tool to the system...

Suppose it does not support Active Directory for authentication.
<table>
<thead>
<tr>
<th>Part</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part a</td>
<td>An Active Directory authentication provider is configured to the specified lockout settings. This will prevent user access to all services that utilize AD for authentication.</td>
</tr>
<tr>
<td>Part b</td>
<td>Active Directory is configured to unlock user accounts automatically after 15 minutes. If the user cannot wait for an unlock, the user can contact the help desk for immediate assistance.</td>
</tr>
</tbody>
</table>
name: COTS Tool Y
- standard_key: NIST-800-53
  control_key: AC-7
narrative:
  - key: a
    text: Tool Y does not integrate with Active Directory…
  - key: b
    text: Tool Y does not integrate with Active Directory…
<table>
<thead>
<tr>
<th>Part a</th>
<th>System X:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>An Active Directory authentication provider is configured to the specified lockout settings. This will prevent user access to all services that utilize AD for authentication.</td>
</tr>
<tr>
<td></td>
<td>COTS Tool Y:</td>
</tr>
<tr>
<td></td>
<td>Tool Y does not integrate with Active Directory. Instead, the tool provides its own authentication system that locks a user automatically after five consecutive failures within an unlimited time period.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part b</th>
<th>System X:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active Directory is configured to unlock user accounts automatically after 15 minutes. If the user cannot wait for an unlock, the user can contact the help desk for immediate assistance.</td>
</tr>
<tr>
<td></td>
<td>COTS Tool Y:</td>
</tr>
<tr>
<td></td>
<td>Tool Y does not integrate with Active Directory. Instead, the tool provides its own authentication system that indefinitely locks the user until an administrator unlocks the account.</td>
</tr>
</tbody>
</table>
Reports are great for aiding communication.
Difficult Questions to Answer

Developers

Leadership (CIO, CTO)

• How many controls are Partially Implemented?
• How many controls do we still need to write?
Velocity: controls written per week

Sanity Checks: are any controls missing a check box?
Difficult Questions to Answer

• What changed since _____?

Developers

Internal Security Team
@@ -10,16 +10,16 @@ satisfies:

- key: a
  text: |
  The 18F Program Office develops, documents, and disseminates
- to all 18F staff, the 18F Access Control Policy which addresses purpose, scope,
- roles, responsibilities, management commitment, coordination among organizational
- entities, and compliance and procedures to facilitate the implementation of
- the access control policy and associated access controls. The 18F access control
- policy is listed within 18F’s private Github repository and the docs.cloud.gov
+ entities, compliance, and procedures to facilitate the implementation of
+ the access control policy and associated access controls. The 18F Access Control
+ Policy is listed within 18F’s private Github repository and the docs.cloud.gov

- site that is accessible to all 18F staff.
- key: b
  text: |
  The 18F Program Office
- will review and update the current 18F Access control policy at least every
+ will review and update the current 18F Access Control Policy at least every
  3 years and any documented access procedures at least annually.

standard key: NTST-800-53
Difficult Questions to Answer

- What changed since _____?
- How many controls are waiting for review?
Add business logic to the YAML data without affecting the generated document.
An Active Directory authentication provider is...
Automated security documentation is not inherently Agile.
DEV + OPS  WALL OF UNCERTAINTY  ASSESSORS
"Our highest priority is to satisfy the customer through early and continuous delivery of valuable software."

The Agile Manifesto
Treat the Security team as the customer
The Security team is the customer

Find ways to enable *iterative* and *incremental* feedback.

- Prioritize the controls
- Sprint review
- Access to the latest content
The Security team is the customer

Find ways to simplify the tracking and review of individual changes.
- Version control
- Break large content into components
- Utilize metrics and alerts
Make it easier to share information
People have different preferences for how to consume data

- Word/Excel
- YAML code
- metrics/charts
- Generated website
Continuous delivery for documentation is possible!
Thank you.
Backup Slides
AC-7 - Unsuccessful Logon Attempts

**Description**

"The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded."

**Satisfied By**

<table>
<thead>
<tr>
<th>Component</th>
<th>Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>system-x</td>
<td>System X</td>
<td>implemented</td>
</tr>
<tr>
<td>tool-y</td>
<td>COTS Tool Y</td>
<td>planned</td>
</tr>
</tbody>
</table>

**Details**

**System X Implementated**

a. An Active Directory authentication provider is configured to the specified lockout settings. This will prevent user access to all services that utilize AD for authentication.

b. Active Directory is configured to unlock user accounts automatically after 15 minutes. If the user cannot wait for an unlock, the user can contact the help desk for immediate assistance.

**COTS Tool Y Planned**

a. Tool X does not integrate with Active Directory. Instead, the tool provides its own authentication system that locks a user automatically.
Automating FedRAMP’s inventory worksheet
Inventory Worksheet Fields

- Unique identifier
- IP address
- Is public?
- DNS name
Inventory Worksheet Fields

- Unique identifier
- IP address
- Is public?
- DNS name
<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance ID</td>
<td>i-0f6b5d77745a3063d</td>
</tr>
<tr>
<td>Instance state</td>
<td>running</td>
</tr>
<tr>
<td>Instance type</td>
<td>t2.nano</td>
</tr>
<tr>
<td>Elastic IPs</td>
<td></td>
</tr>
<tr>
<td>Availability zone</td>
<td>us-east-1d</td>
</tr>
<tr>
<td>Security groups</td>
<td>launch-wizard-2, view inbound rules</td>
</tr>
<tr>
<td>Scheduled events</td>
<td>No scheduled events</td>
</tr>
<tr>
<td>AMI ID</td>
<td>amzn-ami-hvm-2018.03.0.20180508-x86_64-gp2 (ami-14c5486b)</td>
</tr>
<tr>
<td>Public DNS (IPv4)</td>
<td>ec2-54-172-129-174.compute-1.amazonaws.com</td>
</tr>
<tr>
<td>IPv4 Public IP</td>
<td>54.172.129.174</td>
</tr>
<tr>
<td>IPv6 IPs</td>
<td>-</td>
</tr>
<tr>
<td>Private DNS</td>
<td>ip-172-31-11-50.ec2.internal</td>
</tr>
<tr>
<td>Private IPs</td>
<td>172.31.11.50</td>
</tr>
<tr>
<td>Secondary private IPs</td>
<td></td>
</tr>
<tr>
<td>VPC ID</td>
<td>vpc-429fefe25</td>
</tr>
<tr>
<td>Subnet ID</td>
<td>subnet-c7fb008e</td>
</tr>
</tbody>
</table>
Inventory Worksheet Fields

- OS name
- Location
- Asset type
- Software Vendor
- Function
- System Owner
<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function</td>
<td>Python Web Server</td>
</tr>
<tr>
<td>System-Owner</td>
<td>Mike Brown</td>
</tr>
</tbody>
</table>
Speaker Info:
Michael Brown
330-206-5711
Excella
Brown.3.mike@gmail.com