



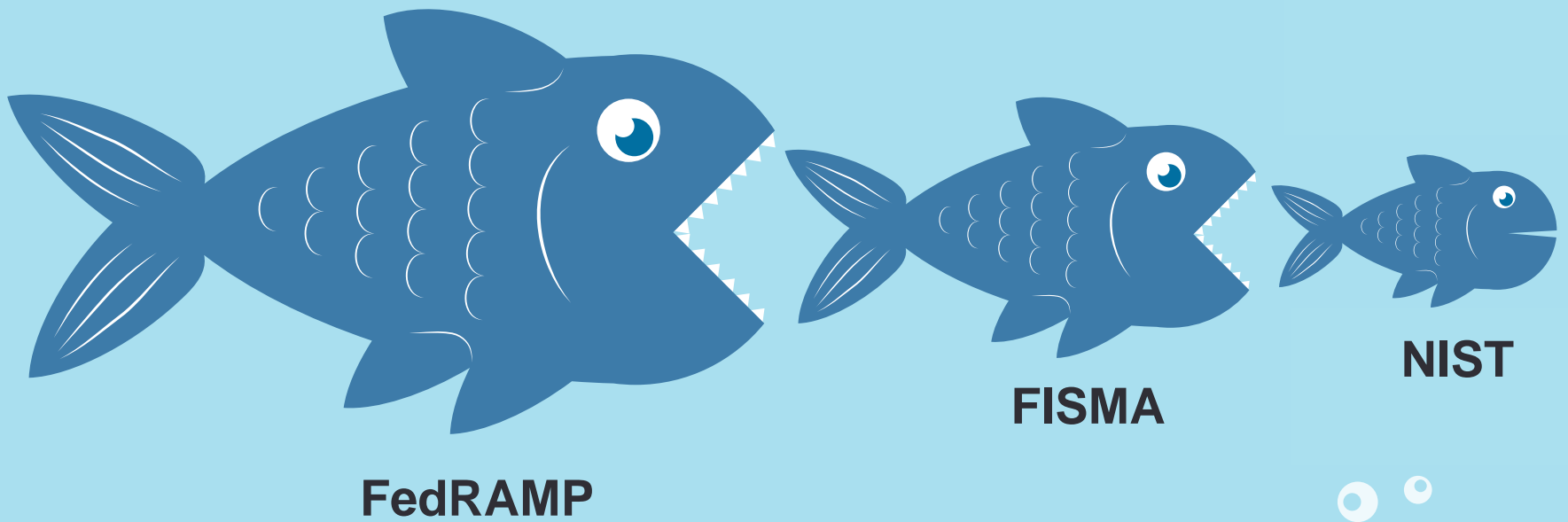
Agile ATO: A New Approach to FedRAMP Documentation

Mike Brown



excella.com | @excellaco

What is FedRAMP?



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

https://www.coalfire.com/Documents/Whitepapers/FISMA-vs-FedRAMP_Controls-authorizations

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

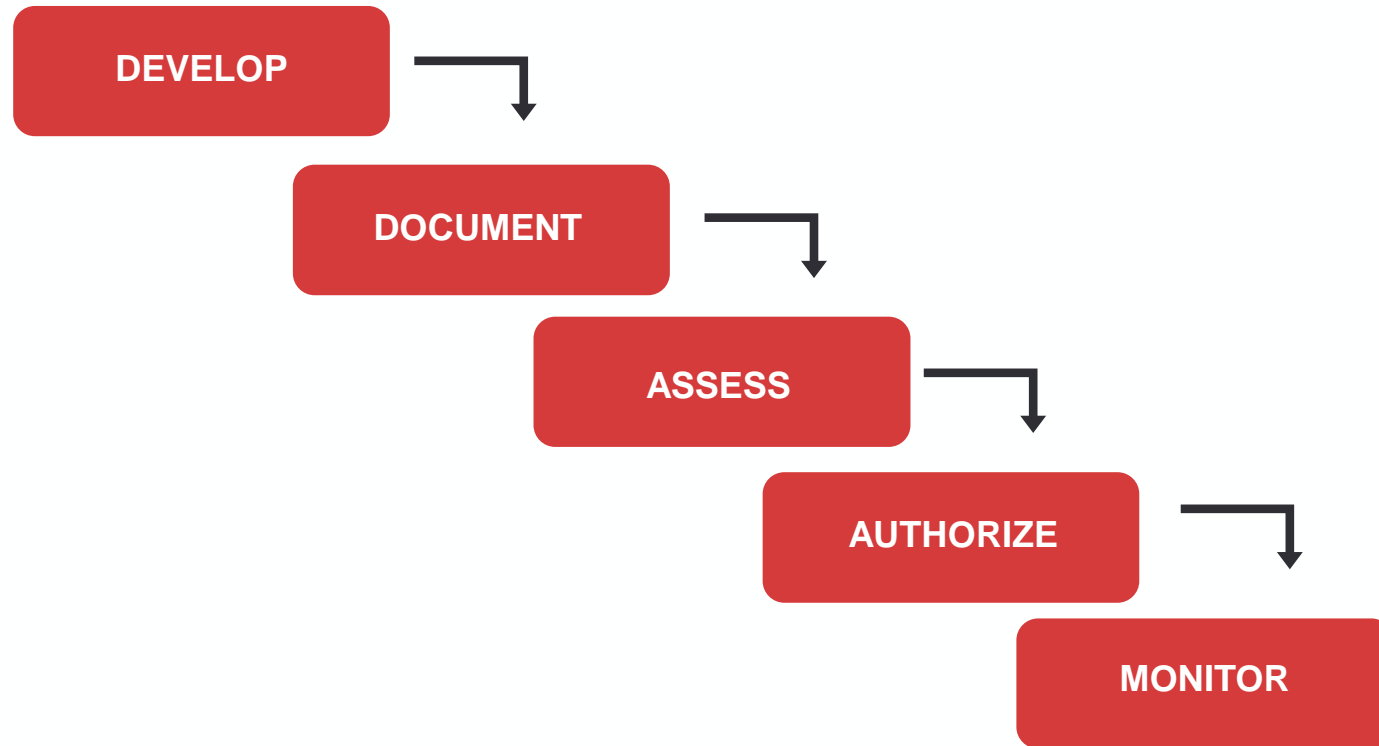


Internal Security Team

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.



 Repeat as necessary

Agile should be both
iterative and *incremental*

DEV + OPS



WALL OF UNCERTAINTY

ASSESSORS

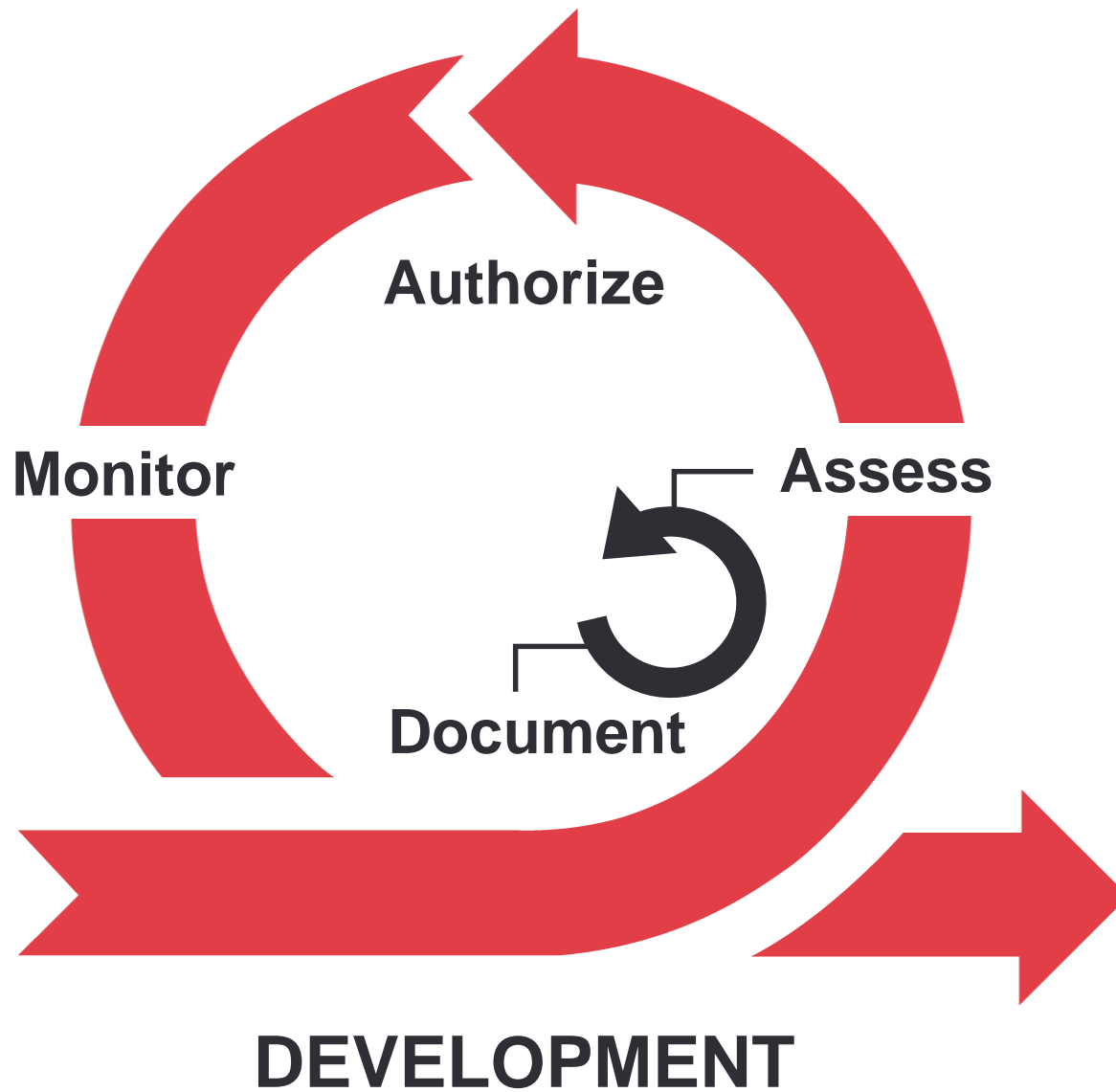


**There must be
a better way.**

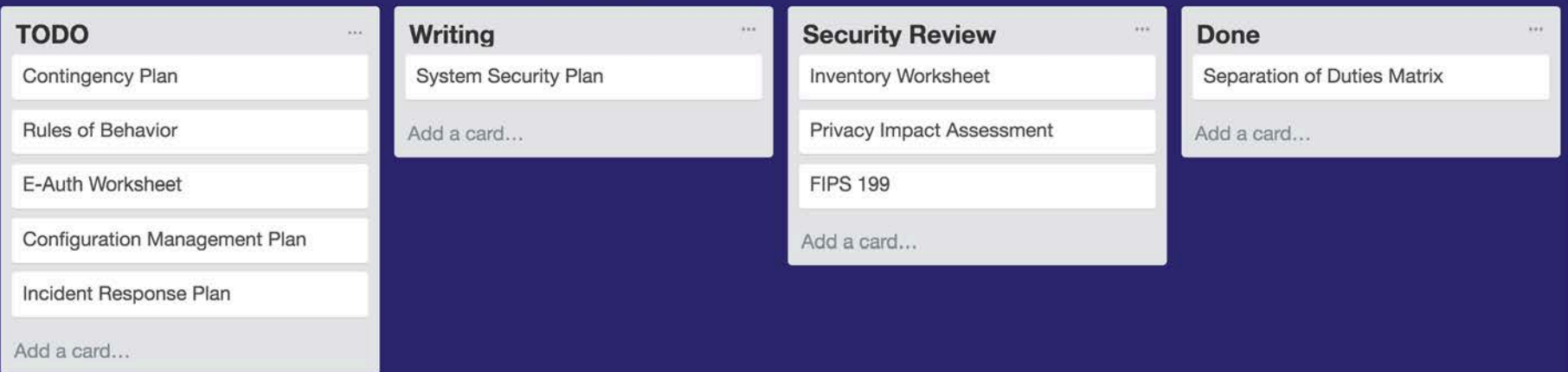
"Our highest priority is to satisfy the customer through early and continuous delivery of valuable software."



The Agile Manifesto



Security Documentation



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.

AC-7	Control Summary Information
Responsible Role:	Chief Technical Officer (CTO)
Parameter AC-7(a)-1:	3
Parameter AC-7(a)-2:	5 minutes
Parameter AC-7(b)-1:	Automatically locks the account
Parameter AC-7(b)-2:	15 minutes
<p>Implementation Status (check all that apply):</p> <p><input checked="" type="checkbox"/> Implemented</p> <p><input type="checkbox"/> Partially implemented</p> <p><input type="checkbox"/> Planned</p> <p><input type="checkbox"/> Alternative implementation</p> <p><input type="checkbox"/> Not applicable</p>	
<p>Control Origination (check all that apply):</p> <p><input checked="" type="checkbox"/> Service Provider Corporate</p> <p><input type="checkbox"/> Service Provider System Specific</p> <p><input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific)</p> <p><input type="checkbox"/> Configured by Customer (Customer System Specific)</p> <p><input type="checkbox"/> Provided by Customer (Customer System Specific)</p> <p><input type="checkbox"/> Shared (Service Provider and Customer Responsibility)</p> <p><input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization</p>	

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

Part 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.

Part 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.

**For a moderate impact
system, there are
324 controls.**

648	1407
check boxes	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?

FedRAMP CIS for SSP Low

Control ID	Implementation Status					Service Provider System Spec
	In Place	Partially Implemented	Planned	Alternative Implementation	N/A	
AC-01	X					
AC-02	X					
AC-02 (01)			X			X
AC-02 (02)			X			X
AC-02 (03)						X
AC-02 (04)		X				X
AC-02 (05)	X					
AC-02 (07)	X					X
AC-02 (09)						
AC-02 (10)						X
AC-02 (12)						X
AC-03			X			X
AC-04						X
AC-04 (21)	X					X
AC-05	X	X				
AC-06			X			X
AC-06 (01)			X			X
AC-06 (02)			X			X

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.”



The OpenControl Project

"A YAML-Powered Antidote To Bureaucracy"

"A set of tools that restructure the process of writing, updating, and reviewing compliance documentation."

Machine Readable 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

YAML in 30 seconds

```
>>> animals = yaml.load(document)["animals"]
```

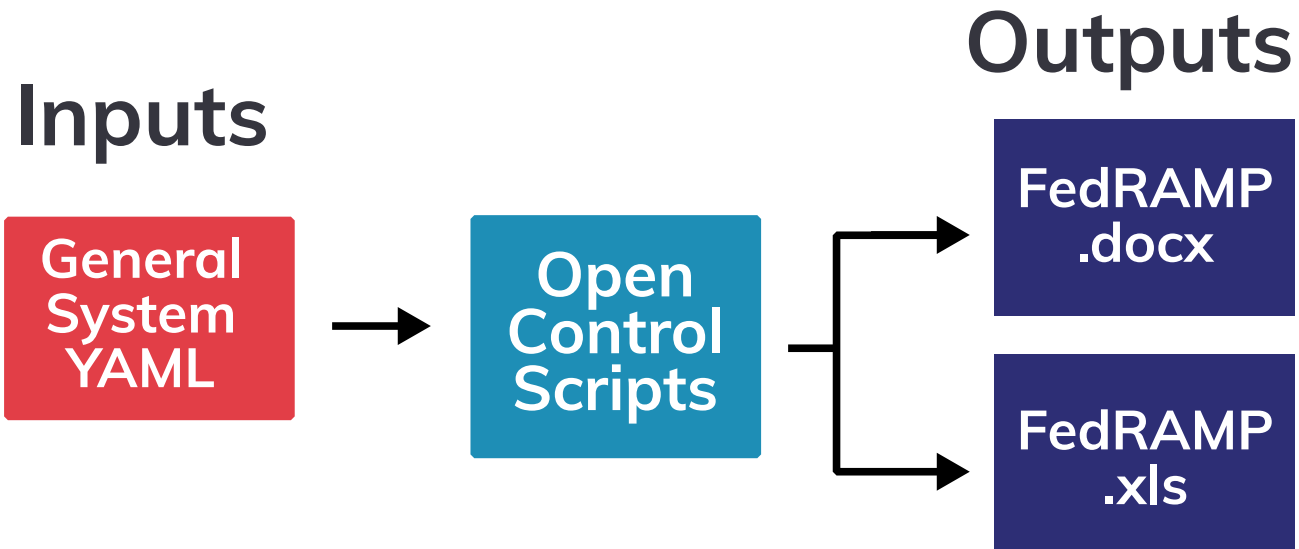
```
>>> animals[0]['name']
```

```
'dog'
```

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

```
["I heard a bark", "I heard a meow"]
```

OpenControl Process



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:

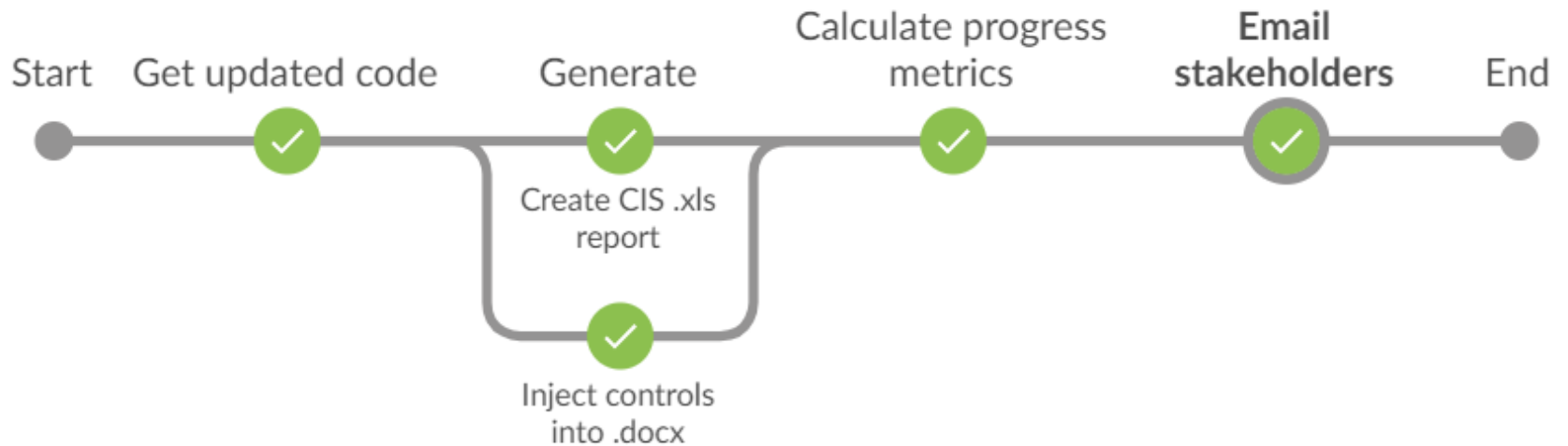
- key: a

text: An Active Directory authentication provider is...

- key: b

text: Active Directory is configured to unlock user...

Continuous Integration Pipeline



AC-7	Control Summary Information
Responsible Role: Chief Technical Officer (CTO)	
Parameter AC-7(a)-1: 3	
Parameter AC-7(a)-2: 5 minutes	
Parameter AC-7(b)-1: Automatically locks the account	
Parameter AC-7(b)-2: 15 minutes	
Implementation Status (check all that apply): <input checked="" type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable	
Control Origination (check all that apply): <input type="checkbox"/> Service Provider Corporate <input checked="" type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> 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?	
Part a	<p data-bbox="357 1086 479 1118"><u>System X:</u></p> <p data-bbox="357 1162 1644 1229">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.</p>
Part b	<p data-bbox="357 1253 479 1285"><u>System X:</u></p> <p data-bbox="357 1329 1673 1396">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.</p>

**Suppose I add a COTS tool
to the system...**

**Suppose it does not
support Active Directory for
authentication.**

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

Part 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.

Part 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.

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...

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

Part a

System X:

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.

COTS Tool Y:

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.

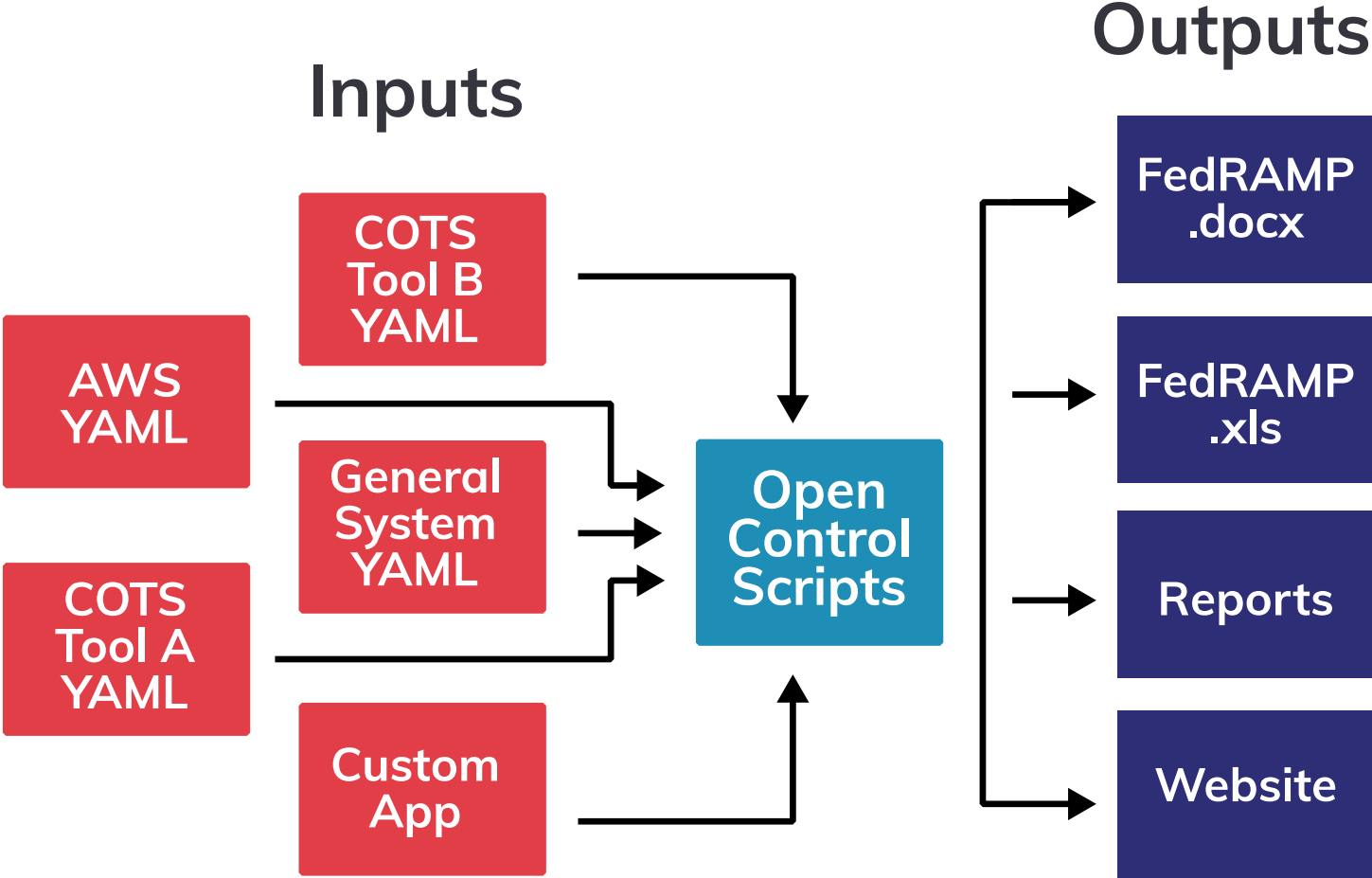
Part b

System X:

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:

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.



**Reports are great for
aiding communication.**

Difficult Questions to Answer



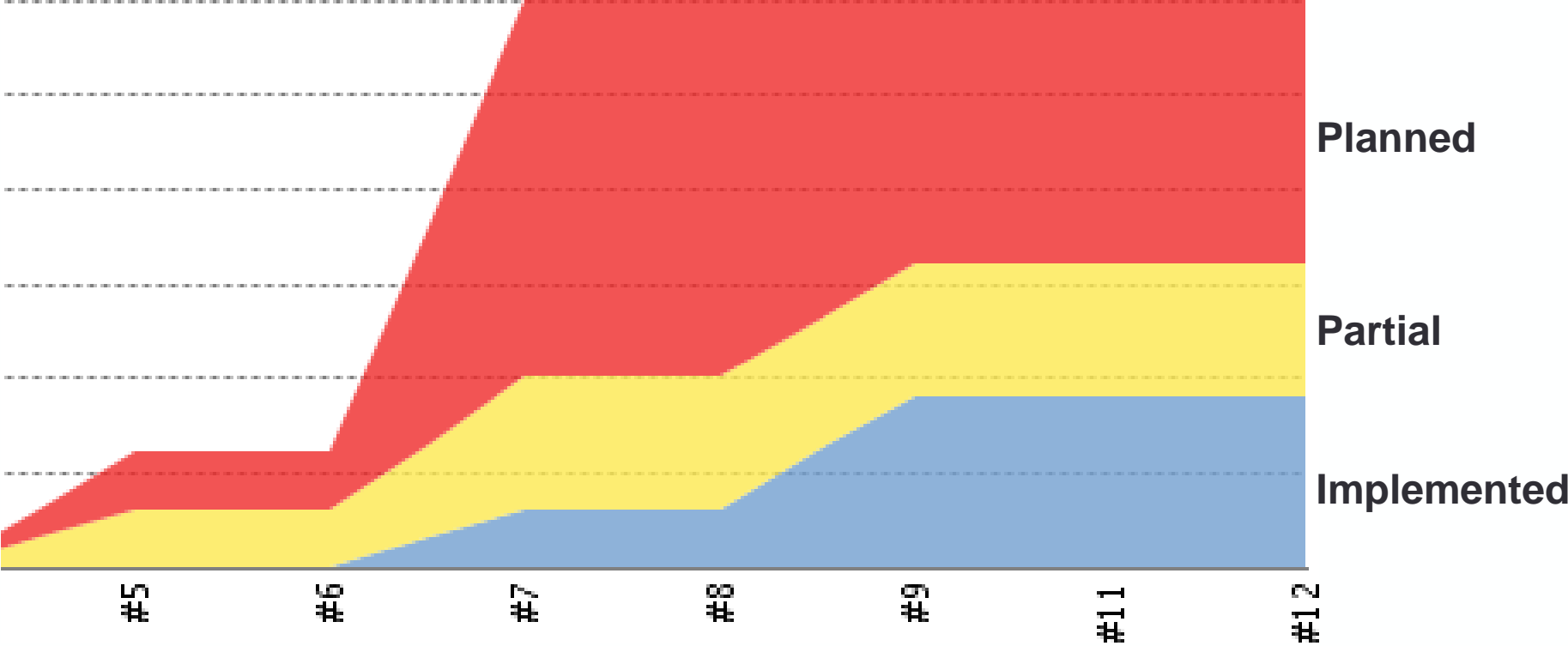
Developers



**Leadership
(CIO, CTO)**

- How many controls are Partially Implemented?
- How many controls do we still need to write?

Continuous Integration Metrics



**Velocity: controls
written per week**

**Sanity Checks: are any controls
missing a check box?**

Difficult Questions to Answer



Developers



**Internal
Security Team**

- What changed since _____?


```

@@ -10,16 +10,16 @@ satisfies:
 10 10 - key: a
 11 11   text: |
 12 12     The 18F Program Office develops, documents, and disseminates
 13 13 -   to all 18F staff, the 18F Access Control Policy which addresses purpose, scope,
 13 13 +   to all 18F staff the 18F Access Control Policy which addresses purpose, scope,
 14 14     roles, responsibilities, management commitment, coordination among organizational
 15 15 -   entities, and compliance and procedures to facilitate the implementation of
 16 16 -   the access control policy and associated access controls. The 18F access control
 17 17 -   policy is listed within 18F's private Github repository and the docs.cloud.gov
 15 15 +   entities, compliance, and procedures to facilitate the implementation of
 16 16 +   the access control policy and associated access controls. The 18F Access Control
 17 17 +   Policy is listed within 18F's private Github repository and the docs.cloud.gov
 18 18     site that is accessible to all 18F staff.
 19 19 - key: b
 20 20   text: |
 21 21     The 18F Program Office
 22 22 -   will review and update the current 18F Access control policy at least every
 22 22 +   will review and update the current 18F Access Control Policy at least every
 23 23     3 years and any documented access procedures at least annually.
 24 24     standard key: NTST-800-53

```

Difficult Questions to Answer



Developers



**Internal
Security Team**

- What changed since _____?
- How many controls are waiting for review?

**Add business logic to the
YAML data without affecting
the generated document.**

name: System X

- standard_key: NIST-800-53

control_key: AC-7

implementation_status: implemented

control_origin: service_provider_system_specific

author: Mike Brown

reviewed_by: null

priority: high

narrative:

- key: a

text: 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



FedRAMP-high

AC

[AC-1 - Access Control Policy A...](#)[AC-2 - Account Management](#)[AC-2 \(1\) - Automated System A...](#)[AC-2 \(2\) - Removal Of Tempora...](#)[AC-2 \(3\) - Disable Inactive Acco...](#)[AC-2 \(4\) - Automated Audit Acti...](#)[AC-2 \(5\) - Inactivity Logout](#)[AC-2 \(7\) - Role-Based Schemes](#)[AC-2 \(9\) - Restrictions On Use ...](#)[AC-2 \(10\) - Shared / Group Acc...](#)[AC-2 \(11\) - Usage Conditions](#)[AC-2 \(12\) - Account Monitoring ...](#)[AC-2 \(13\) - Disable Accounts F...](#)[AC-3 - Access Enforcement](#)[AC-4 - Information Flow Enforc...](#)[AC-4 \(8\) - Security Policy Filters](#)[AC-4 \(21\) - Physical / Logical S...](#)[AC-5 - Separation Of Duties](#)[AC-6 - Least Privilege](#)[AC-6 \(1\) - Authorize Access To ...](#)[AC-6 \(2\) - Non-Privileged Acce...](#)[AC-6 \(3\) - Network Access To P...](#)[AC-6 \(5\) - Privileged Accounts](#)[AC-6 \(7\) - Review Of User Privil...](#)[AC-6 \(8\) - Privilege Levels For ...](#)[AC-6 \(9\) - Auditing Use Of Privil...](#)[AC-6 \(10\) - Prohibit Non-Privile...](#)[AC-7 - Unsuccessful Logon Att...](#)[AC-7 \(2\) - Purge / Wipe Mobile ...](#)[AC-8 - System Use Notification](#)[/ / Certifications / FedRAMP-high / AC / AC-7](#)

AC-7 - Unsuccessful Logon Attempts

Control AC-7**Standard** NIST-800-53**Certifications** FedRAMP-high

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

Component	Name	Status
system-x	System X	implemented
tool-y	COTS Tool Y	planned

Details

System X implemented

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 Y 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
- 

Instance: **i-0f6b5d77745a3063d**

- Description
- Status Checks
- Monitoring
- Tags

Instance ID	i-0f6b5d77745a3063d	Public DNS (IPv4)	ec2-54-172-129-174.compute-1.amazonaws.com
Instance state	running	IPv4 Public IP	54.172.129.174
Instance type	t2.nano	IPv6 IPs	-
Elastic IPs		Private DNS	ip-172-31-11-50.ec2.internal
Availability zone	us-east-1d	Private IPs	172.31.11.50
Security groups	launch-wizard-2 . view inbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-429fef25
AMI ID	amzn-ami-hvm-2018.03.0.20180508-x86_64-gp2 (ami-14c5486b)	Subnet ID	subnet-c7fb008e

Inventory Worksheet Fields

- OS name
- Location
- Asset type
- Software Vendor
- Function
- System Owner

Instance: **i-0f6b5d77745a3063d**

Description

Status Checks

Monitoring

Tags

Add/Edit Tags

Key

Value

Function

Python Web Server

System-Owner

Mike Brown

Speaker Info:
Michael Brown
330-206-5711
Excella
Brown.3.mike@gmail.com