

About me

<https://apporima.com/>

Trevor Bryant (personal)

- Configuration Management expert
- Security minded DevOps nerd
- CTF Beginner
- Instructor @DC_TOOOL
- Organizer / Volunteer *too many* conferences (BSidesDC/Charm/NOVA, DEFCON)
- Infosec mentor

Trevor Bryant (professional)

- FISMA expert
- Knight of NIST
- Lead without title
- Manager without title
- Tech policy & tech literacy
- Auditor, Analyst, Engineer, Architect
- Ent. CM, CI/CD, ULP, Audit strategy, OCIO policy x2, @USPTO
- Consular Systems Modernization, Information Sharing strategy, Fast Track ATO @State

What is Configuration Management?

...the practice of handling changes systematically so that a system maintains its integrity over time.

Configuration management embodies two concepts:

- 1. the configuration management of items and their defining technical requirements and design documents, referred to herein as configuration documentation; and*
- 2. the application of CM principles to digital data in general.*

MIL-HDBK-61 / MIL-HDBK-61A / MIL-HDBK-61B

What is Change Management?

1. *procedures are employed to systematically evaluate each proposed engineering change; or*
2. *requested deviation to baselined documentation, to assess the total change impact (including costs)*
3. *coordination with affected functional activities, to disposition the change or deviation and provide timely approval or disapproval*
4. *to assure timely implementation of approved changes by both parties.*

MIL-HDBK-61 / MIL-HDBK-61A / MIL-HDBK-61B

Adding Culture

- Chairing culture development within an organization
- Humans have to be involved in what we do
- Knowing when weaknesses are introduced to systems
- Understanding and providing education on scan results
- Identifying underlying issues to solve multiple problems
- It's ok to refactor



Crawl, Walk, Run



Compliance as Code Projects

- Everything in OpenControl
- Tim Spencer (18F)
 - GCP App Engine template – <https://github.com/18F/gcp-appengine-template/blob/master/Compliance.md>
 - GSA LATO SSP Template – [../gcp-appengine-template/compliance/markdowns](https://github.com/18F/gcp-appengine-template/blob/master/compliance/markdowns)
- John Jediny
 - NIST OSCAL – <https://github.com/usnistgov/OSCAL>
 - OSCAL integrated Li-SaaS – https://github.com/opencontrol/fedramp-ssp/blob/master/_pages/fedramp-tailored.md
- Elliot DeMatteis
 - CIS-Generator – <https://github.com/brasky/CIS-Generator>
 - python-ssp – <https://github.com/brasky/python-ssp>
- GSA
 - GSA/datagov-ckan-multi – https://github.com/GSA/datagov-ckan-multi/tree/master/_data/opencontrol
- Archived
 - 18F/cg-application-ssp-example – <https://github.com/18F/cg-application-ssp-example>
 - 18F/10x-ssp-parse-prototype – <https://github.com/18F/10x-ssp-parse-prototype>
 - <https://compliance.cloud.gov>
 - 18F/boise – <https://github.com/18F/before-you-ship>
 - 18F/risk management framework – <https://github.com/18F/risk-management-framework>

Allan & Amelie Agree (A&AA)

The image shows a screenshot of a Twitter thread. On the left, a tweet from Trevor Bryant (@apporima) is visible, containing a GIF of two women from the TV show 'The Mindy Project' and the text: "If you're doing this by PDFs, you're doing this wrong. It's got to be automatic." Below this is a retweet of a tweet from @allanfriedman about SBOM and BSidesLV. On the right, a reply from Amélie E. Koran (@webjedi) is shown, discussing the Open Data Initiative and portable formats. The tweet includes engagement metrics like 1 reply, 2 retweets, and 7 likes.

Trevor Bryant @apporima

"If you're doing this by PDFs, you're doing this wrong.
It's got to be automatic."

[@allanfriedman](#) sharing to champions of [#SBOM](#) [#BSidesLV](#)



6:47 PM · Aug 6, 2019 · [Twitter for Android](#)

Amélie E. Koran @webjedi

Replying to [@apporima](#) and [@allanfriedman](#)

Part of the whole desire of the Open Data Initiative is portable and, well, open and passable formats. Some industries have been built to suppr this, others have cottage industries converting archives of old data and formats to this. It should be baked in and "Time 0"

12:46 PM · Aug 7, 2019 · [Twitter for iPhone](#)




3 Likes

Amélie E. Koran @webjedi · Aug 7

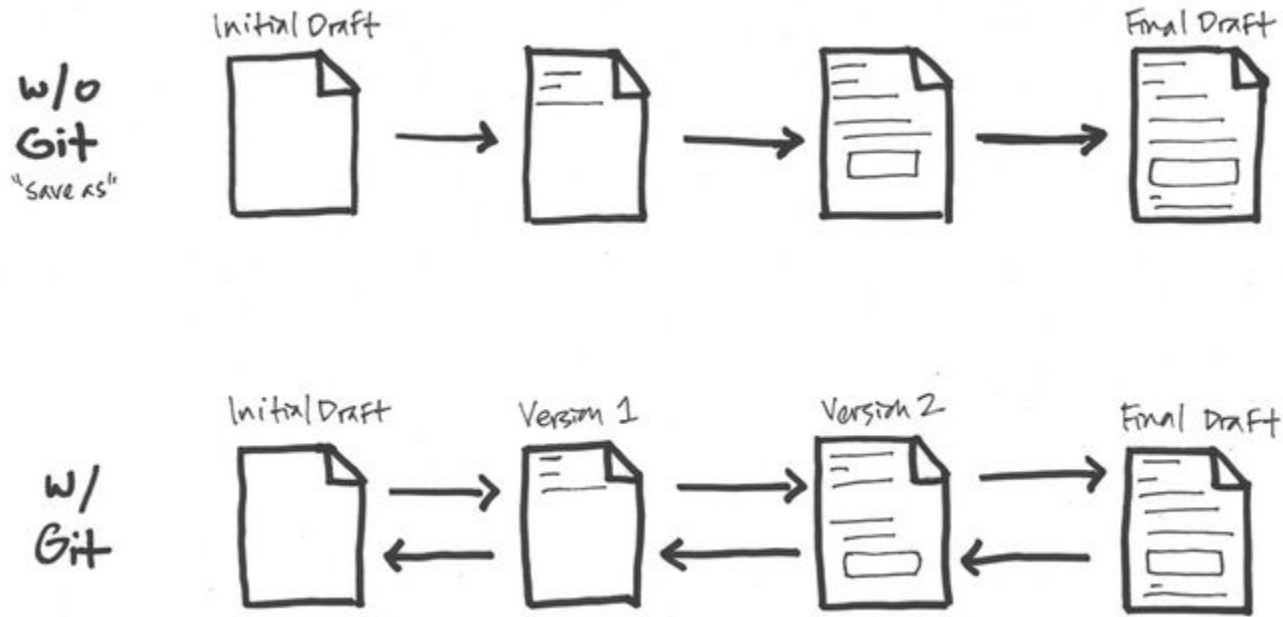
Replying to [@webjedi](#) [@apporima](#) and [@allanfriedman](#)

passable/parseable (stupid autocorrect)

Legacy Limitations

Key Assessor Documents	Baltimore Cyber Range (BCR) Technical Proficiency Activity: Phased Participation Requirements	This policy document describes the phased approach and required timeframe for FedRAMP 3PAO assessment teams to take and pass the Baltimore Cyber Range (BCR) Cybersecurity Technical Proficiency Exercise, a requirement for participation in FedRAMP.	 PDF	12/21/2018
FedRAMP Program Documents	FedRAMP Security Controls Baseline	This document provides the catalog of FedRAMP High, Moderate, Low, and Tailored LI-SaaS baseline security controls, along with additional guidance and requirements.	 EXCEL	8/28/2018
Key Cloud Service Provider (CSP) Documents	Significant Change Policies and Procedures	This document defines the FedRAMP policies and procedures for making significant changes. It provides requirements, guidance, and actions the FedRAMP PMO, AO, CSP, and 3PAO will take when a CSP wishes to make a significant change to its provisionally authorized cloud service.	 WORD	8/28/2018

Revisions and Version Control



<http://jmcglone.com/guides/github-pages/>

The Walk



FedRAMP Moderate versus NIST SP 800-53 rev4

IA-5 (1) CONTROL ENHANCEMENT (L) (M)

The information system, for password-based authentication:

(a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];

(p) Enforces at least the following number of changed characters when new passwords are created: [FedRAMP Assignment: at least one (1)];

(q) Stores and transmits only cryptographically-protected passwords;

(r) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum];

(s) Prohibits password reuse for [FedRAMP Assignment: twenty-four (24)] generations; and

(t) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

IA-5 (1) a and d Additional FedRAMP Requirements and Guidance:

Guidance: If password policies are compliant with NIST SP 800-63B Memorized Secret (Section 5.1.1) Guidance, the control may be considered compliant.

IA-5(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

The information system, for password-based authentication:

IA-5 (1)(a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];

IA-5 (1)(b) Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number];

IA-5 (1)(c) Stores and transmits only cryptographically-protected passwords;

IA-5 (1)(d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum];

IA-5 (1)(e) Prohibits password reuse for [Assignment: organization-defined number] generations; and

IA-5 (1)(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Markdown for Docs as Code

IA-5 (1) Control Enhancement (L) (M)

The information system, for password-based authentication:

```
<ol type="a">
<li>Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensi
characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including min
for each type];</li>
<li>Enforces at least the following number of changed characters when new passwords are created: [FedRAMP
least one (1)];</li>
<li>Stores and transmits only cryptographically-protected passwords;</li>
<li>Enforces password minimum and maximum lifetime restrictions of [Assignment: organization- defined num
minimum, lifetime maximum];</li>
<li>Prohibits password reuse for [FedRAMP Assignment: twenty-four (24)] generations; and</li>
<li>Allows the use of a temporary password for system logons with an immediate change to a permanent pass
<b>IA-5 (1) a and d Additional FedRAMP Requirements and Guidance:</b><br>
<b>Guidance:</b> If password policies are compliant with NIST SP 800-63B Memorized Secret (Section 5.1.1)
control may be considered compliant.
</ol>
```

IA-5 (1) Control Enhancement (L) (M)

The information system, for password-based authentication:

- Enforces minimum password complexity of [Assignment: organization-defined requirements for number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];
- Enforces at least the following number of changed characters when new passwords are created [Assignment: at least one (1)];
- Stores and transmits only cryptographically-protected passwords;
- Enforces password minimum and maximum lifetime restrictions of [Assignment: organization- defined number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];
- Prohibits password reuse for [FedRAMP Assignment: twenty-four (24)] generations; and
- Allows the use of a temporary password for system logons with an immediate change to a permanent password.

IA-5 (1) a and d Additional FedRAMP Requirements and Guidance:

Guidance: If password policies are compliant with NIST SP 800-63B Memorized Secret (Section 5.1.1) Guidance, the control may be considered compliant.

Trivial Search

```
trevor@hecate: ~/Documents/fedramp-ssp/_pages$ grep -rnw . -e JAB [119/1170]
./ca.md:70:<b>Requirement:</b> For JAB Authorization, must use an accredited Third Party Assessment
Organization (3PAO).
./ca.md:103:The organization accepts the results of an assessment of [FedRAMP Assignment: organizat
ion-defined information system] performed by [FedRAMP Assignment: any FedRAMP Accredited 3PAO] when
the assessment meets [FedRAMP Assignment: the conditions of the JAB/AO in the FedRAMP Repository].
./ca.md:183:<b>Guidance:</b> For JAB Authorization, CSPs shall include details of this control in t
heir architecture briefing.
./ca.md:228:<b>Guidance:</b> Significant change is defined in NIST Special Publication 800-37 Revis
ion 1, Appendix F (SP 800-37). The service provider describes the types of changes to the informat
ion system or the environment of operations that would impact the risk posture. The types of chang
es are approved and accepted by the JAB/AO.
./au.md:43:<b>Requirement:</b> Coordination between service provider and consumer shall be document
ed and accepted by the JAB/AO.
./au.md:64:Guidance: Annually or whenever changes in the threat environment are communicated to the
service provider by the JAB/AO.
./au.md:94:<b>Requirement:</b> The service provider defines audit record types [FedRAMP Assignment:
session, connection, transaction, or activity duration; for client-server transactions, the number
of bytes received and bytes sent; additional informational messages to diagnose or identify the ev
ent; characteristics that describe or identify the object or resource being acted upon]. The audit
record types are approved and accepted by the JAB.<br>
./cp.md:54:<b>Requirement:</b> For JAB authorizations the contingency lists include designated FedR
AMP personnel.
./cp.md:143:<b>Requirement:</b> The service provider develops test plans in accordance with NIST Sp
ecial Publication 800-34 (as amended) and provides plans to FedRAMP prior to initiating testing. T
est plans are approved and accepted by the JAB/AO prior to initiating testing.
[asdf] 0:bash- 1:[tmux]* "hecate" 10:00 30-Aug-19
```

Feedback

GitHub

- Received PRs fixing tables and typos
- Bots creating issues with fix to remediate dependency vulnerabilities

Sharing

- *SWEET!*
- *That looks pretty. :slightly_smiling_face:*
- *If we can get this stuff in a repo that can do PRs, can be cloned easily, etc, it will be a huge win.*
- *A&A as code ultimately, in however that can best, become real*

Crawl, Walk, Run

.docx – .xlsx – .pdf



data from pipelines
populating
templates, data
tagging, reusable
content

consistent template
generation as code

Internal Documentation Experience

Today

Doing many, using many

- 100s inconsistent RMF docs
- Custom SSP templates; manual efforts
- Difficult to manage and update
- No opportunity to specialize
- Challenges to dedicate to process improvement

Future

Do once, use many

- Integrate RMF into SDLC
- Consistent SSP templates; machine readable
- Automated document generation / data
- Plenty of growth opportunities
- CMMI Services maturity

gh-pages

demo dance