when devops meets regulation: integrating 'continuous' with 'government'

@jezhumble

public domain slides courtesy @noahkunin, infrastructure director, 18F / GSA TTS
Let us know what you think

Click ‘engage’ to rate sessions and ask questions

Join the conversation #gotocph
The ability to get changes—features, configuration changes, bug fixes, experiments—into production or into the hands of users *safely* and *quickly* in a *sustainable* way.
devops movement

a cross-functional community of practice dedicated to the study of building, evolving and operating rapidly changing, secure, resilient systems at scale
Let’s ship it!
Or not.
Shipping software isn’t rocket science
Is the launch checklist working?
The U.S. Government's Digital Launch Checklist
Records Management
Records Schedule
Privacy Act
Paperwork Reduction Act
Section 508 and Accessibility Standards
Federal Acquisition Regulation
Anti-deficiency Act
Economy Act
E-Government Act
Computer Matching Act
National Cyber Protection System
Guidance for Agency Use of Third-Party Websites and Applications
Social Media and Web-Based Interactive Technologies
Office of Management Budget Circular A-130 Appendix 3
Federal Information Security and Management Act
Federal Information Processing Standard (FIPS) 199
Federal Information Processing Standard (FIPS) 200
Federal Information Processing Standard (FIPS) 140-2
Special Publication 800-37
Special Publication 800-53 Revision 4
Special Publication 800-60 Volume 1
Special Publication 800-60 Volume 2
Security and Privacy Controls for Federal Information Systems and Organizations

http://dx.doi.org/10.6028/NIST.SP.800-53r4
My friend, you can clearly see the intention of FIPS 140-2 Annex A was to deprecate SHA-1 on the lunar new year...
<table>
<thead>
<tr>
<th>Control Name</th>
<th>LOW</th>
<th>MOD</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness and Training</td>
<td>P1</td>
<td>AF 1</td>
<td>AF 1</td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td>P1</td>
<td>X1</td>
<td>X1</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>P1</td>
<td>CM 1</td>
<td>CM 1</td>
</tr>
<tr>
<td>Incident Response</td>
<td>P1</td>
<td>IR 1</td>
<td>IR 1</td>
</tr>
</tbody>
</table>

http://dx.doi.org/10.6028/NIST.SP.800-53r4
http://dx.doi.org/10.6028/NIST.SP.800-53r4
<table>
<thead>
<tr>
<th>CONTROL</th>
<th>CONTROL NAME</th>
<th>INITIAL CONTROL RANKING</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1.1</td>
<td>System and Information Integrity/Network Access Controls</td>
<td>P1</td>
</tr>
<tr>
<td>S1.2</td>
<td>Access Control</td>
<td>P1</td>
</tr>
<tr>
<td>S1.3</td>
<td>Multi Factor Authentication</td>
<td>P1</td>
</tr>
<tr>
<td>S1.4</td>
<td>Information System Monitoring</td>
<td>P1</td>
</tr>
<tr>
<td>S1.5</td>
<td>Identity and Access Management</td>
<td>P1</td>
</tr>
<tr>
<td>S1.6</td>
<td>Security Baseline Verifier</td>
<td>P1</td>
</tr>
<tr>
<td>S1.7</td>
<td>Information System Inventory</td>
<td>P1</td>
</tr>
<tr>
<td>S1.8</td>
<td>Information Security Management</td>
<td>P1</td>
</tr>
<tr>
<td>S1.9</td>
<td>Security Management Activities</td>
<td>P1</td>
</tr>
<tr>
<td>S1.10</td>
<td>Security Awareness and Training</td>
<td>P1</td>
</tr>
<tr>
<td>S1.11</td>
<td>Security Incident Response</td>
<td>P1</td>
</tr>
<tr>
<td>S1.12</td>
<td>Security Incident Handling and Resolution</td>
<td>P1</td>
</tr>
<tr>
<td>S1.13</td>
<td>Physical Security Controls</td>
<td>P1</td>
</tr>
<tr>
<td>S1.14</td>
<td>Physical Access Controls</td>
<td>P1</td>
</tr>
<tr>
<td>S1.15</td>
<td>Security Object Controls</td>
<td>P1</td>
</tr>
<tr>
<td>S1.16</td>
<td>Information Security Controls</td>
<td>P1</td>
</tr>
<tr>
<td>S1.17</td>
<td>Information Security Controls</td>
<td>P1</td>
</tr>
</tbody>
</table>

http://dx.doi.org/10.6028/NIST.SP.800-53r4
<table>
<thead>
<tr>
<th>CNTL NO.</th>
<th>CONTROL NAME</th>
<th>WITHDRAWN</th>
<th>LOW</th>
<th>MOD</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-1</td>
<td>Access Control Policy and Procedures</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2</td>
<td>Account Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(1)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>AUTOMATED SYSTEM ACCOUNT MANAGEMENT</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>AC-2(2)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>AC-2(3)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>DISABLE INACTIVE ACCOUNTS</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(4)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>AUTOMATED AUDIT ACTIONS</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(5)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>INACTIVITY LOGOUT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(6)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>DYNAMIC PRIVILEGE MANAGEMENT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(7)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>ROLE-BASED SCHEMES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(8)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>DYNAMIC ACCOUNT CREATION</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(9)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(10)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(11)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>USAGE CONDITIONS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(12)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>ACCOUNT MONITORING / ATYPICAL USAGE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-2(13)</td>
<td>ACCOUNT MANAGEMENT</td>
<td>ACCOUNT MONITORING / ATYPICAL USAGE</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CONFIDENCE CONTROL

The organization:

a. Establishes the type of changes to the information systems that are authorized.

b. Reviews proposed configuration control decisions for the information system and approves or disapproves such changes with respect to organizational security requirements.

c. Documents configuration change decisions associated with the information system.

d. Implements approved configuration controlled changes to the information system.

e. Maintains records of configuration-controlled changes to the information system for "Audit Trail" purposes.

f. Audits and reviews activities associated with configuration-controlled changes to the information system.

g. Coordinates and provides oversight for configuration change control activities through "Assignee: organization-defined configuration change control agency (e.g., compliance, audit)" that ensures "Implementation of configuration controlled changes to the information system is performed." (Assignee: organization-defined configuration change control agency)

Security and Compliance: Configuration change control involves organizational information systems and the systems owners, developers, system administrators, security managers, and owners of configuration controlled changes to the information system for "Configuration change control is performed." (Assignee: organization-defined configuration change control agency)

Central Environments:

<table>
<thead>
<tr>
<th>Configuration Change Control</th>
<th>Security Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>The organization employs automated mechanisms to:</td>
<td>The environment ensures that all security functions and policy requirements are managed.</td>
</tr>
<tr>
<td>a. Document proposed changes to the information system.</td>
<td>The configuration change control process is implemented.</td>
</tr>
<tr>
<td>b. Notify [Assignee: organization-defined approval authority] of proposed changes to the information system and request change approval.</td>
<td>The configuration change control process is implemented.</td>
</tr>
<tr>
<td>c. Highlight proposed changes to the information system that have not been approved or disapproved by [Assignee: organization-defined approval authority].</td>
<td>The configuration change control process is implemented.</td>
</tr>
<tr>
<td>d. Provide changes to the information system until disapproved changes are received.</td>
<td>The configuration change control process is implemented.</td>
</tr>
<tr>
<td>e. Document all changes to the information system.</td>
<td>The configuration change control process is implemented.</td>
</tr>
<tr>
<td>f. Identify inappropriate organization personnel when approved changes to the information system are completed.</td>
<td>The configuration change control process is implemented.</td>
</tr>
</tbody>
</table>

[1] CONFIGURATION CHANGE CONTROL | SECURITY ENVIRONMENT

The organization employs automated mechanisms to:

a. Document proposed changes to the information system.

b. Notify [Assignee: organization-defined approval authority] of proposed changes to the information system and request change approval.

c. Highlight proposed changes to the information system that have not been approved or disapproved by [Assignee: organization-defined approval authority].

d. Provide changes to the information system until disapproved changes are received.

e. Document all changes to the information system.

f. Identify inappropriate organization personnel when approved changes to the information system are completed.

[2] CONFIGURATION CHANGE CONTROL | SECURITY ENVIRONMENT

The organization employs automated mechanisms to:

a. Document proposed changes to the information system.

b. Notify [Assignee: organization-defined approval authority] of proposed changes to the information system and request change approval.

c. Highlight proposed changes to the information system that have not been approved or disapproved by [Assignee: organization-defined approval authority].

d. Provide changes to the information system until disapproved changes are received.

e. Document all changes to the information system.

f. Identify inappropriate organization personnel when approved changes to the information system are completed.

[3] CONFIGURATION CHANGE CONTROL | SECURITY ENVIRONMENT

The organization employs automated mechanisms to:

a. Document proposed changes to the information system.

b. Notify [Assignee: organization-defined approval authority] of proposed changes to the information system and request change approval.

c. Highlight proposed changes to the information system that have not been approved or disapproved by [Assignee: organization-defined approval authority].

d. Provide changes to the information system until disapproved changes are received.

e. Document all changes to the information system.

f. Identify inappropriate organization personnel when approved changes to the information system are completed.


Central Environments:

1. CONFIGURATION CHANGE CONTROL [ RFC 2046 ] - CONFIGURATION CONTROL: FUNCTION AND CHANGES

The organization employs automated mechanisms to:

- Document all approved changes to the information system.

- Notify all approved change requests to the information system.

- Highlight personnel changes to the information system and request change approval.

- Document all changes to the information system and request change approval.

- Notify all approved organization components when changes approved by the information system are completed.

2. CONFIGURATION CHANGE CONTROL [ RFC 2046 ] - SECURITY POLICY DOCUMENT MANAGEMENT

The organization employs automated mechanisms to control changes to the information system before implementing the changes on the information system.

3. CONFIGURATION CHANGE CONTROL [ RFC 2046 ] - SECURITY POLICY DOCUMENT MANAGEMENT

The organization employs automated mechanisms to control changes to the information system before implementing the changes on the information system.

4. CONFIGURATION CONTROL [ RFC 2046 ] - SECURITY POLICY DOCUMENT MANAGEMENT

The organization employs automated mechanisms to control changes to the information system before implementing the changes on the information system.
MEDIA MARKING

Criteria: The organization:

a. Marks information system media indicating the distribution limitations, handling controls, and applicable security markings (if any) of the information and

b. Exempts [Assignment: organization-defined types of information system media] from marking as long as the media remain within [Assignment: organization-defined controlled areas].

Supplemental Guidance: The term security marking refers to the application of human-readable security attributes. The term security labeling refers to the application of security attributes with regard to internal data structures within information systems (see AC-16). Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/ removable hard disk drives, flash drives, compact discs, and digital video discs. Non digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable. Marking of information system media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: AC-16, PL-3, RA-3.

Criteria Enhancements: None.

References: FIPS Publication 199.

PRIORITY AND BASELINE ASSIGNMENT:

| P2 | LOW | Not Selected | MOD | NP-3 | HIGH | NP-3 |

WATER DAMAGE PROTECTION

Criteria: The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations. Related control: AT-3.

Criteria Enhancements:

1. WATER DAMAGE PROTECTION | AUTOMATION SUPPORT

The organization employs automated mechanisms to detect the presence of water in the vicinity of the information systems and alerts [Assignment: organization-defined personnel or roles].

Supplemental Guidance: Automated mechanisms can include, for example, water detection sensors, alarms, and notification systems.

References: None.

PRIORITY AND BASELINE ASSIGNMENT:

| P1 | LOW | PE-15 | MOD | PE-15 | HIGH | PE-15 (1) |
How long is this going to take?
6 - 14 months to ship
Speed is the new security.
The Government Innovation Platform

The open source cloud platform built for the federal government.

Cloud deployment is better. But that doesn’t make it easy.
FedRAMP System Security Plan

18F - Cloud.Gov

- About the SSP
- Cloud.gov System Classification
- Cloud.gov General System Description

Standards

- NIST-800-53 - AC
  - AC - Access Control Policy and Procedures
  - AC - Account Management
  - AC - Account Management | Automated System Account Management
  - AC - Account Management | Removal of Temporary / Emergency Accounts
what this gets you

teams can deploy into a production-like environment from day 1

architectural paradigm designed for distributed systems

push-button deployments

most of the controls taken care of at the platform level

templates for all your compliance documentation
Please

Remember to rate this session

Thank you!

Join the conversation #gotocph