§ 3541. Purposes

The purposes of this subchapter are to—

(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the Federal Government and the Federal Information Systems, and federal information security policies and procedures across agency boundaries;

(3) foster the development and maintenance of minimum controls required to protect Federal information and information systems;

(4) provide a mechanism for improved oversight of Federal agency information security programs;

(5) acknowledge that continuous improvement of information security for Federal systems, not just robust, but effective information security solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation, that are designed, built, and operated by the private sector; and

(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.


Effective Date

### Security Controls Traceability Matrix - Down-selected 20160106

| Column | A1 | B1 | C1 | D1 | E1 | F1 | G1 | H1 | I1 | J1 | K1 | L1 | M1 | N1 | O1 | P1 | Q1 | R1 | S1 | T1 | U1 | V1 | W1 | X1 | Y1 | Z1 |
|--------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Row    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |

- **A1** Access Control: The system shall implement an access control mechanism that restricts access to authorized users only.
- **B1** Authentication: The system shall implement mechanisms to authenticate users and ensure that only authorized users are granted access.
- **C1** Authorization: The system shall implement a mechanism to control access to resources based on user roles and privileges.
- **D1** Encryption: The system shall implement encryption to protect data in transit and at rest.
- **E1** Integrity: The system shall implement mechanisms to ensure data integrity and prevent unauthorized modifications.
- **F1** Availability: The system shall implement mechanisms to ensure availability of services and resources.
- **G1** Non-repudiation: The system shall implement mechanisms to ensure non-repudiation of actions.
- **H1** Confidentiality: The system shall implement mechanisms to ensure confidentiality of data.
- **I1** Authentication and Accountability: The system shall implement mechanisms to authenticate and account for actions performed.
- **J1** Data Security: The system shall implement mechanisms to protect data from unauthorized access.
- **K1** Resource Security: The system shall implement mechanisms to protect resources from unauthorized access.
- **L1** System and Communications Security: The system shall implement mechanisms to protect the system and communications from unauthorized access.
- **M1** Privacy: The system shall implement mechanisms to protect privacy of individuals.
- **N1** System Security: The system shall implement mechanisms to ensure the security of the system.
- **O1** Operational Security: The system shall implement mechanisms to ensure security during operations.
- **P1** Security Assessment: The system shall implement mechanisms to assess security risks periodically.
- **Q1** Security Management: The system shall implement mechanisms to manage security policies and procedures.
- **R1** Security Awareness and Training: The system shall implement mechanisms to ensure security awareness and training for employees.
- **S1** Security Configuration Management: The system shall implement mechanisms to manage security configuration.
- **T1** Security Incident Management: The system shall implement mechanisms to manage security incidents.
- **U1** Security Architecture: The system shall implement mechanisms to ensure security architecture is robust.
- **V1** Security Controls: The system shall implement mechanisms to ensure security controls are in place.
- **W1** Security Policy: The system shall implement mechanisms to ensure security policies are in place.
- **X1** Security Risk Management: The system shall implement mechanisms to manage security risks.
- **Y1** Security Testing: The system shall implement mechanisms to test security controls periodically.
- **Z1** Security Training: The system shall implement mechanisms to ensure security training is provided.

- **Note:** The matrix indicates compliance with the security controls based on the down-selected criteria.
The OpenShift Compliance Guide

About

OpenShift is a container management platform based on Docker containers and the Kubernetes container cluster manager. OpenShift adds developer and operational centric tools to enable rapid application development, easy deployment and scaling, and long-term lifecycle maintenance for small and large teams and applications.

Built atop Red Hat Enterprise Linux (RHEL), OpenShift is very secure. For users who must comply with the Federal Information Security Management Act (FISMA), there is additional configuration burden.

This guide can help you secure your OpenShift cluster to comply with the FISMA moderate confidentiality, integrity, and availability requirements.

While the configurations and Security Control Traceability Matrix (SCTM) documented in this guide could be implemented in any environment, the reference architecture is Amazon Web Services.

Table of Contents

1. Security CONOPS
2. Security Controls
3. Customer Responsibility Matrix
4. Ansible

http://tinyurl.com/ocpcg
WHAT’S IN THE COMPLIANCE GUIDE?

1. Reference Architecture (Security Concept of Operations (CONOPS))
2. Security Controls
   • Procedurally generated from the Security Control Traceability Matrix (SCTM) spreadsheet
3. Customer Responsibility Matrix (CRM)
4. Ansible Automation

Note: Certification and Accreditation (C&A) terminology replaced by Assessment and Authorization (A&A) in new DoD Information Assurance Risk Management Framework (DIARMF) (cf. NIST SP800-37r1).
REFERENCE ARCHITECTURE
<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Number Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>A control that is satisfied by the hosting organization. This includes enterprise services such as LDAP, the Audit and Logging solution, etc.</td>
<td>423</td>
</tr>
<tr>
<td>IaaS</td>
<td>A control that is satisfied by the Organization’s Infrastructure as a Service implementation. In the Security CONOPS reference architecture, this is AWS, or the Landlord’s Landlord.</td>
<td>11</td>
</tr>
<tr>
<td>OpenShift Landlord</td>
<td>Container Platform’s implementation. This includes tools such as Ansible Tower and OpenSCAP.</td>
<td>187</td>
</tr>
<tr>
<td>OpenShift Tenant</td>
<td>Controls that need to be implemented by the programs hosted on the OpenShift Container Platform. These controls are listed in the Customer Responsibility Matrix.</td>
<td>73</td>
</tr>
<tr>
<td>Total unique controls</td>
<td>All unique technical controls tracked by this guide.</td>
<td>658</td>
</tr>
</tbody>
</table>

SECURITY CONTROLS
Workaround example:

```
JavaScript
```

```
Banner
iframe
```

```
Actual OCP Web Console
```
CUSTOMER RESPONSIBILITY MATRIX
RA-3 - Risk Assessment

Requirement: RISK ASSESSMENT Control: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; c. Reviews risk assessment results [Assignment: organization-defined frequency]; d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Control Summary Information

Role: OpenShift Tenant
Status: Not implemented
Origin: Tenant SSP
ANSIBLE
rhtps

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>800-53</td>
<td>This role will apply 800-53 to your EL hosts.</td>
</tr>
<tr>
<td>bind</td>
<td>your description</td>
</tr>
<tr>
<td>dns-server</td>
<td>Ansible role for creating a DNS server</td>
</tr>
<tr>
<td>gluster-node</td>
<td>Ansible role for Red Hat Gluster nodes</td>
</tr>
<tr>
<td>private-aws</td>
<td>private-aws role</td>
</tr>
<tr>
<td>registry</td>
<td>Installs docker-registry and loads images from the tarballs in a disconnected way.</td>
</tr>
<tr>
<td>vnc</td>
<td>TigerVNC role</td>
</tr>
<tr>
<td>yum</td>
<td>yum role</td>
</tr>
</tbody>
</table>

https://galaxy.ansible.com/rhtps
- name: AC-17(8) Uninstall Unnecessary Package
  yum:
    name: "{{ item }}"
    state: absent
    with_items: "{{ ac_uninstall_packages }}"
  tags:
    - conf-low
    - conf-medium
    - conf-high
    - int-low
    - int-medium
    - int-high

- name: AC-3,AC-3(3),AC-4,AC-6 Enable SELinux
  selinux:
    policy: targeted
    state: enforcing
  tags:
    - conf-low
    - conf-medium
    - conf-high
    - int-low
    - int-medium
    - int-high

- name: Set SELinux to Enforcing
  command: /usr/sbin/setenforce 1
  when: ansible_selinux.mode == 'permissive'

- name: AC-17(8) Remove Rssh Trust Files - /etc/hosts.equiv
  file:
    dest: /etc/hosts.equiv
    state: absent
  tags:
    - conf-low
    - conf-medium
    - conf-high
FAQS
Q: Is this “official?”
A: No, not yet.

Q: Does this mean OpenShift is “accredited out of the box”
A: No, nothing is.

Q: Is this complete?
A: Nope.

Q: Can I contribute?
A: Yes! It’s open source.
QUESTIONS?