Tier 1 Control Standards (State-Wide)

Change Management

Control Number
IOT-CS-ARC-002

Published Date
6/13/2018

Effective Date
1/30/2017

Last Updated
6/13/2018

Next Review Date
6/13/2019

Policy
09.0 Information Protection Processes and Procedures (PR.IP)
   09.3 PR.IP-3
       09.3.1 Change Management

Purpose
Control changes to service assets and configuration items across the whole service lifecycle.

Scope
IOT Supported Entities

Statement
The management of any installation or alteration which adds to, deletes from, or modifies any production environment that the Indiana Office of Technology manages is subject to the requirements of this standard. This includes, but is not limited to:

- Application changes
- Hardware changes
- Visual changes
- System or software changes
- Firewall changes
- Network changes impacting many users and/or multiple agencies
- Environmental changes
- Documentation changes
- Shared environments (production and non-production)
- Services and tools in support of production systems, procedures or environmental facilities
Change Requester

The IOT or agency resource who requests a given change. Change management requests (CMRs) submitted for the upcoming window must be “manager approved” within the system prior to the start of the Change Advisory Board (CAB) meeting to be considered as a non-emergency change. Late submissions will be rejected and must be resubmitted as either an emergency or submitted in a subsequent change window.

Change Advisory Board (CAB)

A team of people made up of IOT managerial staff and subject matter experts with additional members included depending on the change being analyzed. The CAB is chaired by the IOT Change Administrator and assisted by IOT Change Coordinator.

The mission of the Change Advisory Board is to perform the following functions for all changes:

- Plan, approve and monitor CMRs
- Review Post Mortem, Emergency and Failed CMRs
- Review the previous week’s 24 hr. daily system and network change reports

The IOT Change Coordinator is responsible for coordination and communication between agencies and IOT departments. The CAB will meet on a weekly basis to review and approve any changes that will occur within a scheduled change window. Emergency changes will be handled by the IOT Change Administrator and will potentially call an emergency meeting if the change is significant enough. A pre-implementation meeting will also be held weekly to address any approved changes that have the potential of impacting each other. The meeting will consist of the change implementers, IOT Change Coordinator and IOT Change Administrator. It is the change requester’s responsibility to thoroughly review all other potentially conflicting changes prior to the Thursday meeting and have any concerns ready for discussion.

Firewall Advisory Board (FAB)

The FAB is made up of a team of IOT staff, primarily subject matter experts, which have the in-depth knowledge to adequately approve and monitor firewall changes. All firewall changes that are viewed to have considerable impact or risk may be brought before the CAB for final approval.

Change Request Types

**Emergency Change** – Changes that are vital to ensure that IOT & agencies committed service levels are maintained.
- Approved by:
  - Manager of requesting user
  - IOT Change Administrator or emergency CAB meeting
  - All Emergency Changes must be post implementation reviewed by CAB

**Normal Change** - Changes that require full Change Management review. They are reviewed and approved or rejected by CAB (DEFAULT).

**Standard Change** – Preauthorized and reoccurring change that is relatively common and follows a procedure or work instruction (Ex. Windows security or previously installed software updates). Must reference SOP in the request, Reviewed only by IOT Change Administrator.

All requests that are unsuccessful or experience unexpected results will be post reviewed by the CAB.

Rating CMR’s

CMR’s will be rated by determining the impact and complexity involved in the execution of the CMR. The impact and complexity will be classified based upon the criteria below. Those scores will then be combined to determine the overall risk rating for the CMR, known as the Risk Assessment (RA) value. You can view the full Risk Assessment document also attached in here.
IMPACT classifications – HIGH, MEDIUM, LOW
Answer the following question to determine the impact of a given change: “If your change would be unsuccessful or the process of your change could negatively affect systems, the result would be?”

COMPLEXITY classifications – HIGH, MEDIUM, LOW
The potential complexity associated with the change; i.e. dependencies, ability to rollback, previous issues with system(s) and non-production testing. Please answer the following question to determine the Complexity of your change. “Which complexity level best describes your change?”

CMR Risk Assessment Matrix
Using the values identified as Impact and Complexity, determine the overall Risk Assessment of your CMR from the matrix below.

<table>
<thead>
<tr>
<th>Complexity</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Impact</td>
<td>HIGH</td>
<td>HIGH</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Medium Impact</td>
<td>HIGH</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Low Impact</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>LOW</td>
</tr>
</tbody>
</table>

CMR Risk Rating Review Period
Note: Normal Changes (non-emergency or standard change) are to follow the rating review period guidelines.
- **HIGH** – There will be a minimum of a four weeks review period
- **MEDIUM** – There will be a minimum of a two weeks review period
- **LOW** – There will be a minimum of a one week review period
CMR’s submitted as Emergency or Standard changes will be reviewed and processed accordingly based on all information provided and are subject to different review periods than Normal changes.
Standard Changes (Changes that have an approved and published SOP) may be implemented earlier than the Normal Change window when possible.

Scheduled Change Windows*
- All changes will be on Sunday 6-10 AM unless valid reasons dictate otherwise. The CAB will determine if it will be necessary to allow requests to be implemented outside of the normal window.
- All firewall changes will be on Thursday 6-10 AM unless valid reasons dictate otherwise.
- **All software changes will begin on Friday at 8pm and run until Sunday at 6pm unless otherwise notified.

*Although currently being discussed for changes, this is the published standard and should be followed whenever possible.

**(published in the IOT Service Catalog yet not the CMR Standard)

Note: this information may change based on data submitted and leadership approval

Roles
IOT Personnel
Information Asset Owners/System Owners
Responsibilities
All IOT personnel that have the ability to make changes to the production IT environment shall be required to follow and participate in all outlined required change management meetings and documentation. Agency System Owners must work with appropriate IOT personnel to submit a change management requests on behalf of agency when promoting production code.

Management Commitment
Management shall ensure all outlined change management requirements are enforced.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT Liaison to submit change management requests on behalf of agency.

Compliance
IOT and Agencies shall review respective system ownership to determine production changes that require to be part of change.

Exceptions
Exceptions will be handled on a case by case basis through the Director of Risk & Compliance, State CISO and the IOT Architecture team.

Associated Documents
Risk Assessment