# AWS System Administration and Support Standard Operating Procedure (SOP)

## Training Requirements (Ensure a training item is created for both new and revised SOPs. If this is for a new system, a new Curriculum may also be needed.)

|  |
| --- |
| Place an “X” in the appropriate box. |
| (Note: Effective date in Regulus should be 30 days from date of approval). Check a box below as appropriate.  **New Procedure**  Training Required Yes  No  **Revised Procedure**  Retraining Required Yes  No |

## APPROVERS

## Subject Matter Expert

Your electronic signature attests that this procedure is accurate and complete.

## System Custodian

Your electronic signature attests that you have reviewed this document and attest that you understand the content and acknowledge your responsibilities.

*SC approval is required if pre-approved changes are included in this document.*

## System Owner

Your electronic signature attests that you understand and agree with the pre-approved changes.

*SO approval is required if pre-approved changes are included in this document.*

## Computer System Quality Assurance (CSQA) Representative

Your electronic signature attests that this document complies with applicable Corporate Computer Systems (CCS) Lilly Quality Standards and Practices.

CSQA approval required for GMP systems.

## Business Quality Assurance (BQA)

Your electronic signature attests that you understand and agree with the pre-approved changes.

*BQA approval is required if pre-approved changes are included in this document*

# PURPOSE

The purpose of this Standard Operating Procedure (SOP) is to describe processes and procedures necessary to maintain and support [insert system acronym] to ensure it remains in a validated state.

# IN SCOPE

The following are in scope:

* System administration of the AWS Platform.

# OUT OF SCOPE

The following are out of scope:

* Software or applications that run on the platform (i.e. LC3)

## AREAS INVOVLED

*<Insert areas or groups that need the training item (BET) for this SOP listed on their Training Plan>*

# CONTACT

For any questions related to this SOP, contact *< insert name of “owning SME” >*

# ACRONYMS AND DEFINITIONS

The terms and acronyms in this document are defined at their first occurrence.

Additional terms should be defined within the text of the document. Acronyms must be spelled out upon first mention in the document text with the acronym in parentheses immediately after it. (Example: Master Document List (MDL)). Use the acronym alone thereafter.

Table of Contents

[1. Risks 7](#_Toc487464655)

[2. Change Management 7](#_Toc487464656)

[2.1 Change Control Board 7](#_Toc487464657)

[2.2 Pre-Approved Changes 7](#_Toc487464658)

[2.3 Vulnerability Patches 7](#_Toc487464659)

[3. INCIDENT Management 8](#_Toc487464660)

[4. PROBLEM Management 8](#_Toc487464661)

[5. Source Code Management 8](#_Toc487464662)

[5.1 Code Migration and Software Installation 8](#_Toc487464663)

[5.2 Automated Tool 9](#_Toc487464664)

[6. Required Software 9](#_Toc487464665)

[7. Deployment Method 9](#_Toc487464666)

[8. Periodic Review 9](#_Toc487464667)

[9. System Inventory 9](#_Toc487464668)

[10. sUPPLIER Contact Information 9](#_Toc487464669)

[11. Infrastructure and interface support information 10](#_Toc487464670)

[11.1 Infrastructure Support 10](#_Toc487464671)

[11.2 Necessary Support Accounts 10](#_Toc487464672)

[12. Routine Administration Tasks 10](#_Toc487464673)

[13. System-specific Process 10](#_Toc487464674)

[13.1 [Name] Process 10](#_Toc487464675)

[14. REFERENCES 11](#_Toc487464676)

# Change Management

Changes to the system (hardware and software changes), data and documentation will be made according to ITC-SOP-Change Management-412. The tool used to manage change requests associated with this system is ServiceNow.

The following table provides the type of information from ServiceNow used to support this process.

| Information from ServiceNow | Details |
| --- | --- |
| Fields in addition to those defined in SOP | List the fields used in addition to those already defined. For example:   * Change Number * Configuration Item * Approval State * Business Justification * Change Reason |
| Impact Classification | *[Insert from ServiceNow]* |
| Queue or Assignment Group | [Insert from ServiceNow] |
| Configuration Item (CI) | *[Insert CI from ServiceNow]* |
| Change Approval Group(s) | *[Insert group name from ServiceNow. There may be more than one]* |

## Change Control Board

If a change control board exists for the system, provide the list of names and their responsibilities here. If this is documented in ServiceNow indicate that here.

## Pre-Approved Changes

Describe how pre-approved changes will be managed and documented. Reference the system’s Pre-Approved Changes List, if applicable.

If there are **no pre-approved changes**, the following can be used: There are no pre-approved changes for this system.

## Vulnerability Patches

Describe how vulnerability patches will be managed.

Select one of the two scenarios below and delete the other.

Vulnerability patches are not managed though Change Control. Refer to the Product Research and Development Vulnerability Patch Management Strategy document for additional information.

OR

Vulnerability patches are managed through Change Control.

# INCIDENT Management

Incidents are logged via the Incident Management application in ServiceNow. Selecting the correct Configuration Item (CI) will automatically populate the incident with information indicating the business criticality and assist with the Assessment and Investigation of the incident. Every CI has a related Support Group. The CI value can also be used to route an incident to the appropriate Assignment Group. Closed incidents remain available in ServiceNow as a historical resource for System Administrators to use when diagnosing and/or resolving future issues.

For other requests where a standard service is to be performed, a Service Request is raised. If a catalog item exists, Service Requests will be logged through the Service Catalog; if not, non-catalog Service Request items will be logged through an incident. The [*ITC-SOP-Incident Management*](http://in1rglscrpa1.am.lilly.com/DCA/ViewerExternalProcessor.aspx?VersionUID=873D06EE-C77A-4E3D-A863-0616A5D7EC62&PublicView=1&KioskAccount=1&DocBase=CENTRAL02&Name=ITC-SOP-Problem%20Management-389)*-388* will be followed for incident management.

If the system’s validation package includes a Standard Service Offering containing further detail around incident management (for example, core support hours), reference that document here.

| Type of Information | Details |
| --- | --- |
| Priority | Priority is used for incidents only. Service Request Service Level Agreements (SLA) will be determined on a case-by-case basis. Within Service Requests, there will be Standard and enhanced SLAs, if appropriate.  For Service Requests, the catalog item will automatically determine the SLA and no documentation are needed other than referring to the catalog item. *Note: SLAs will be associated with the Priority rating for Incident Management.* |
| Assignment Group | *[Insert from ServiceNow]* |
| Configuration Item Display Name | *[*Insert *Application CI ID from ServiceNow]* |

# PROBLEM Management

Problem Management aims to resolve the root cause of incidents and to manage the lifecycle of a problem. In ServiceNow, the problems are created and managed by the Problem application. Problems can be created as standalone problems through analysis or linked with an incident (or group of similar incidents). Closed problem tickets remain available in ServiceNow as a historical resource for System Administrators to refer for root cause of the issues.  Problems can be flagged as a deviation by the Computer System Quality Assurance (CSQA) Representative. [*ITC-SOP-Problem Management*](http://in1rglscrpa1.am.lilly.com/DCA/ViewerExternalProcessor.aspx?VersionUID=873D06EE-C77A-4E3D-A863-0616A5D7EC62&PublicView=1&KioskAccount=1&DocBase=CENTRAL02&Name=ITC-SOP-Problem%20Management-389)*-389* describes how the problem tickets are used versus an incident. Refer to ServiceNow for the assignment groups.

# Infrastructure as code Management

## Code Migration and Software Installation

Describe the process to document and verify proper installation. Reference the system Installation and Verification Instructions (IVI), if applicable.

Add the following, if applicable:

For more information on code migration and software installation, see the [insert system acronym] Installation and Verification Instructions (IVI).

Code migration and software installation, as well as the processes used to document and verify proper installation, are governed by the applicable code language standards.

OR

This is a COTS system. Refer to the supplier’s development and installation documentation.

OR

This is a COTS system. The supplier is responsible for development and installation.

## Automated Tool

The following automated tools are used to manage source code:

* GitHub
* Jenkins

# Required Software

The following software required to develop, troubleshoot and fix issues with the system:

* AWS Command Line Tools
* Python (tooling script used to spin-up and modify stacks)
  + Database snapshots, listing and reviewing apps, managing docker images, creating read replicas for DBs
* Bash (Bourne Again Shell) – (Scripting and automation)
* Secure shell (SSh) (Remote Access)
* PSQL (Database management)

# Deployment Method

Describe the deployment method. Indicate where details for deployment are documented. Some deployment information is often located in Installation and Verification Instruction (IVI). If so, reference here. Next to each deployment method, indicate Yes or No. For COTS installed by a supplier, indicate what part of deployment is the supplier responsibility and which part if any, are Lilly responsibility.

| Deployment Method | Used? |  | Deployment Method | Used? |
| --- | --- | --- | --- | --- |
| Application Server | Yes  No |  | Database Server | Yes  No |
| Automated Delivery (Altiris) | Yes  No |  | Lab Workstation | Yes  No |
| Automated Delivery (CAMS) | Yes  No |  | Unix Server | Yes  No |
| Automated Delivery (SMS) | Yes  No |  | Unix Workstation | Yes  No |
| Business Computer | Yes  No |  | VMWare | Yes  No |
| Citrix Server | Yes  No |  | Web Server | Yes  No |

# Periodic Review

Periodic reviews for this system will follow frequency as defined in the *ITC-SOP-IT Periodic Review-8494*.

# System Inventory

The Configuration Management Database (CMDB) in ServiceNow is the asset inventory tool used to manage this system.

# SUPPLIER Contact Information

If the system is Commercial Off-the-Shelf (COTS), list the contact information for the software supplier in this section and any special requirements for how to report software problems to the supplier. If a Supplier Management Plan (SMP) exists for the supplier, reference it here. The preferred approach is to document customer support number, not contact names.

| Supplier Name | Contact Information |
| --- | --- |
| [Insert Supplier name] | Supplier Address: [Insert Address]  Customer Support Contact Information: [Insert Customer Support Phone Number and Email]  Supplier Website: [Insert Website] |

# Infrastructure and interface support information

## Infrastructure Support

If the system requires enterprise infrastructure support or has interfaces to other systems, include them here or reference where this information can be found.

## Necessary Support Accounts

# Routine Administration Tasks

Routine administrative tasks are activities that are necessary for the ongoing maintenance and do not represent a change to software or hardware of the system. The following are routing tasks which must be performed:

* Private certificate rotation is a routine administration task completed every 90 days
* Public certificate rotation is a routine administration task completed every 18 months.
* Copying new docker images to a separate region is also scripted but manually triggered daily.

ASSOCIATED DOCUMENTS LIST:

*The documents listed in this table are associated with this procedure and will be categorized as either appendices or attachments. If category = appendix, the document will be included within the APPENDICES section of this SOP. If category = attachment, the document will receive its own unique document identifier, be stored separately and may have required approvals that are different than the SOP it is associated with. The required approvals for an attachment (if different than the SOP) must be specified below this table.*

|  |  |  |
| --- | --- | --- |
| **Document Identifier** | **Category** | **Title/Description** |
|  |  |  |

# References

|  |  |
| --- | --- |
| Reference Number | Title |
| PDS–SOP–00300 | *MMA/SaMD and EmbSW Change Management* |
| PDS–SOP–00318 | *MMA/SaMD and EmbSW Anomaly Management* |
| PDS–SOP–00301 | *MMA/SaMD and EmbSW Design Control and Commercialization* |
| **Attachments** | |
|  |  |

# Revision History

|  |  |  |
| --- | --- | --- |
| Version: 0 | Author: Joyce Licorish | Change Number: Doc Only |
| Change Summary:   * Initial draft. | | |