Doc No.: D-SOP/ITG/61
Process Owner: Information Technology Group
Version No.: 1.00
Last Reviewed on: 31-07-2019
Next Review Date: 30-07-2021

Standard Operating Procedures

for

Program Change Management

1.0 Name of standard operating procedure

Program Change Management operating guidelines

2.0 Scope of applicability:

Program Change Management encompasses the request initiation, documentation of changes, evaluation, impact analysis, development and implementation to a system. Standardization of Program Change Management process would help in maintaining controls and traceability of change requests thus ensuring that information resources are protected against undocumented and unauthorized modifications before, during and after change implementation.

3.0 Distribution list

Name of the Group/Team	Team Head	Team Lead	FPR
IT Governance	Madhavi Purandare	Girish Sunthankar	Ashwin Paldano Vishnu Burra
Application Team	Ramesh Kumar	Deven Pathare	Anita Jiandaney
Business Technology Operations(BTO)	Ganesh Balasubramanian	Ashok Thiagarajan	Jitender Kumar Samitkumar Das

4.0 Procedures for the Process:

A workflow based application, "Whizible Initiative" has been implemented for ensuring adherence to the process/procedures and the documentation detailed in the operating guidelines on Change Management.

The terminologies involved in the Program Change Management Process are defined as follows:

Change Request (CR) is a request to initiate a change in Production, Fallback & DR environment (as applicable). The change may be a scheduled change or an emergency change.

A scheduled change is one where a formal notification is received, reviewed and approved in advance of the change being made in an application on account of a/an

- New functionality – New functionalities/ features in the application.
- Automation requirement – To eliminate manual process or usage of spreadsheets
- Fixing a software error/bug – To fix an issue reported / found in the application
- Compliance requirements – Building controls to address compliance/ governance requirements due to audit/ regulatory guidelines
- Performance tuning – To enhance the performance of the application

An emergency Change Request necessitates the immediate resolution of system failure or a security vulnerability, where obtaining formal sign-off is not feasible due to urgency of the requirement and paucity of time. The emergency change may be initiated on obtaining verbal/ email confirmation from the technology person who is from the leadership team.

Applicable roles:

Business User (BU)	The business group/team who would initiate a CR and also perform User Acceptance Testing (UAT)
Business User Head (BUH)	Approver from the business team
Application Owner (AO)	The technology team personnel, responsible for managing the application and performing impact analysis of the change
Technology Group Head (TGH)	Approver from the technology team
Configuration Controller Head (CCH)	The Deployment Team leader, who reviews the impact of the change on the infrastructure and also verifies the correctness and completeness of the deployment notes, system test cases, UAT sign off before the request is forwarded to the deployment team for deployment
Deployment team (DT)	The team has privileges on the systems/ applications to perform deployment as per the change request
Dev Delivery Group Lead (DEV DGL) / Development Delivery Lead (DEV PL)	Approvers from development team side. DEV DGL / DEV PL provides the patch for deployment

Change Management Documentation:

Business Requirement Specification (BRS)	Details the change requirement/ what is required in terms of functionalities/ features in the application
Test Case Scenario	lists the various scenarios based on which the testing of the change would be carried out during various phases of implementation of the change like during system testing or the UAT phase
Deployment notes	provide the documentation of the deployment steps/ procedures to the Deployment team (DT)
UAT Result(s)	Lists the results of the testing done by the requester based on the Test Case Scenarios (TCS) document
System Testing result(s)	Lists the results of the testing done by the Application Owner (AO)
Approach document	Details the practices and techniques that will be used while change is designed, built and tested

1. The Program Change Management process involves the following three teams / groups, with proper segregation of duties:

   Business Group - It is the business /operations group that is the information or data owner of the application.

Business Technology Group - The Technology team that is the custodian of the data in the application and responsible for deploying the required changes.

Technology Infrastructure Group - The team that is responsible for the maintenance of infrastructure used for the functioning of the application.

2. A program Change Request could be initiated by -
   Business User (BU) for business requirements and requires approval of both business User Head (BUH) and Technology Group Head (TGH).

   Application Owner (AO) for technology requirements and requires approval of Technology Group Head (TGH).

3. A Change Request (CR) can be classified into two types :

   (i) Scheduled Change Request
   (ii) Emergency Change Request

i) A scheduled Change Request could further be categorized into the following CR types:

A. External Change Request - It is initiated by the Business User (BU) and the detailed requirements for the change, i.e. the BRS (Business requirement specifications) and TCS (Test Case Scenarios) are mandatory to be submitted while raising the Change Request. Reference links should be provided for test cases used along with the test results where attachment cannot be uploaded in the Change Management application due to size constraints. The cost benefit analysis by the BU is mandatory at this stage.
Post this change, the application owner does the feasibility and cost analysis of the CR and sets the timelines for the change. The cost analysis by AO (application owner) is mandatory at the feasibility analysis and timelines stage. The AO needs to ensure that the impact analysis and approach document are uploaded at this stage followed by an approval from the TGH and the BUH. Both TGH and BUH approve the business benefits, CR cost and the time-lines set for delivery of the requirement.

Post approvals, the development team works on the code or configuration level changes of the requirement. Once development is complete, the patch is provided to the AO. For applications which are proprietary products, the service provider maintains the version control for the code. For applications customized for ICICI, the version control of code is maintained through SVN (subversion). The AO deploys the patch in the UAT environment and performs testing, uploads the results of the testing and releases the system for testing by business users. The business users test the system functionality and upload their test results document along with a UAT sign-off document certifying that the UAT was successful. On receipt of the UAT signoff, AO uploads the deployment notes for deployment/configuration of the patch in the Live / Production and Fall-back / Disaster Recovery (DR) environment by the Deployment Team (DT). The AO should also provide a roll-back plan along with applicable backup requirements to the configuration control team, which will be executed in case of any eventuality caused during deployment of the patch. The DT confirms that the backup has been taken as per the backup requirements specified by AO and captures the date and time of the deployment.

The BU is intimated on completion of the deployment of the Change Request in the production environment. The BU verifies and confirms on the functioning of the requirement. The CR can be pushed back up to AO-UAT stage if the deployment is unsuccessful.

B. Internal Change Request- It is initiated by the Application Owner and the detailed requirements for the change, i.e. the BRS (Business Requirement Specifications) and TCS (Test Case Scenarios) are mandatory to be submitted while raising the Change Request. Reference links are to be provided for test cases used along with the test results where attachments cannot be uploaded in the Change Management tool due to size limitations. Post approval from the TGH, approach document and impact analysis are mandatorily submitted at this stage by the AO.

The business team is kept apprised of changes initiated by the technology team.

Post approval by the TGH, the development team works on the code or configuration level changes of the requirement. For applications which are proprietary products, the service provider maintains the version control of the software. For applications customized for ICICI, the software's version control is maintained through SVN. Once development is complete, the patch is provided to the AO. The AO performs both system testing and UAT based on approved Test Case Scenarios and uploads the test case results.

Further to that, the production movement is planned and the application team has to mandatorily provide the deployment notes including the roll-back plan to the configuration control team for configuring the change. The Deployment Team (DT) confirms that the requisite backups have been taken as per the backup requirements specified by AO and captures the date and time of the deployment post which the deployment team deploys the patch in production. Once post production verification of the code/functionality is successfully done by the technology team, the change request is completed and closed.

C. MIS Workflow - It is initiated for catering to MIS requests from business teams for which functionality is not available at the application's front end. The request is initiated by the Business User and detailed requirements for the change, i.e. the BRS (Business Requirement Specifications) and TCS (Test Case Scenarios) are submitted while raising the Change Request. Thereafter, the Application Owner checks the feasibility of the MIS requirement and carries out the cost analysis and sets the timelines for the change. Post this, an approval from the TGH and BUH is obtained subsequent to which, the development team develops the code and releases the code to the AO. The AO does the system testing and then releases the patch in the UAT environment for testing by the BU.

The BU performs the UAT and Change Request following is further approved by BUH which is considered as the UAT signoff. Post this, the TGH provides approval for deploying the patch in the live environment wherein the AO uploads the MIS dump in the deployment path from where the BU can download it for their perusal. The impact analysis and system test cases document are not mandatory for this change.

A. Scoping Call - This kind of Change Request is raised to analyze the feasibility of a particular change or a business requirement. The request is initiated by the BU with the mandatory details of the requirements or changes submitted in the form of BRS and Test Case Scenarios. Post this, the application team subsequently checks the technical feasibility of the CR and closes the CR with their suggestion/feedback. Based on the suggestions of the application team, the business team may subsequently raise a new Change Request to implement the change.

B. Minor Change Request - A minor CR can be initiated for any change for which the estimated effort is less than or equal to four man-days or for changes that are on account of

software bugs or to make configuration level changes. This is further divided into two types of workflows:

1. External Change Request- Minor: This workflow is available to Business User (BU) and is raised for a business initiated Change Request.
2. Internal Change Request - Minor: This workflow is available to Application Owner (AO) and is raised for a technology initiated Change Request.

For both the aforementioned type of change requests, only information fields like case title, application name, module name, beneficiary entity, CR category, requested go-live date, business group and business benefits(only in case of external change request) need to be filled while initiating a change. The number of CR categories available for minor CRs are business enhancement, bug fix, technology enhancement, audit & compliance and MIS & onetime extract. The rest of the CR workflow for minor CRs is same as the workflow for respective external and internal workflows for a regular CR. The impact analysis document is not mandatory for this CR.

ii) An Emergency Change Request is raised in the event of a system failure or the discovery of security vulnerability, when a program change may be required to be carried out in the application without the physical sign-off of the BUH and/or TGH due to the urgency to fix the issue in the application to avoid associated business losses. The program change will be initiated on verbal/mail confirmation from the technology person from the leadership team. Subsequently, necessary approval needs to be taken from the BUH and/or TGH within two working days.

The approval sought from the BUH and/ or TGH is for regularizing the program change request documentation and hence would capture the details of the verbal approval taken and the deployment files and details performed on the production/ live environment.

The business user or application owner who is initiating the emergency change will be responsible for regularizing the CR within 2 working days. In case of an emergency change request, approach document and impact analysis document are not mandatory.

iii) Based on the application tiering (tier categorization is taken from APM module of App360 application), the following fields in the Change Request form will be captured during the deployment of a CR

For tier 1 or tier 2 applications: AO and DT confirmation for DR/Fallback deployment should have the value as "Yes"

For tier 3 or tier 4 applications: AO and DT confirmation for DR/Fallback deployment should have the value as "Yes/No/NA"

iii) All major changes to an application Tier 1/ Tier 2) have to undergo Security Risk Assessment and deployed in the production environment only after obtaining the RRR (Residual Risk Report) sign-off from the Information Security Group (ISG) of the Bank. Major CR will be pushed to IRIS at the Acceptance Testing and request for production deployment (for Technology Initiated CRs) and UAT Testing (for Business initiated CRs)

iii) A CR can be broadly classified as major if it meets any of the following criteria:

- If there is a major change in the underlying platform/architecture of the application (OS/DB/Webserver etc.). For example, change to the Operating Systems (e.g. Windows

to UNIX), Database – e.g. (Oracle to AIX), Application/Web Server (IIS to WebLogic), Development (e.g. Java to .Net). However, this would exclude platform (OS/DB/Webserver) version upgrades for tier1/2 or internet facing applications (for e.g. Oracle 10g to 11g, Windows 2k3 to 2k8)

- If there is a change to the mechanism of authentication of the application (From Non - AD to AD authentication, from single factor to dual/multiple factor authentication)
- If there is an application movement from the corporate zone to DMZ
- If a new instance (geography or module) of the application is created
- If the application software undergoes a major version upgrade

When a major CR is raised in Whizible Initiative, the CR number, the application CAN ID and the application name will be triggered to IRIS and the ASLC will be initiated for that application. IRIS takes the BIA feed from App360 for identifying the criticality and sensitivity of the application. In the Residual Risk Report (RRR), the CR number will be displayed in the annexure.

For all in-house developed applications, it is mandatory that developers refer to the guidelines containing secure coding practices for developing code.

For identifying and mitigating the risk arising from application security vulnerabilities, a third party security assessment team has been engaged as 'first line of defence', whereby the security testing of identified applications and major changes (CRs) in those applications is done. The security assessment of identified critical applications is done on quarterly basis. The applications that would undergo such testing are identified based on various factors like whether the application is internet facing or is classified as tier 1/tier 2 or is critical from a financial perspective. The list of applications is reviewed annually and could vary between periods based on appropriate senior management approvals. The scope of this assessment is web security assessment and encompasses testing of all functionalities and pages like transactional, non-transactional, logged in and non-logged in sections.

The security assessment process for the in-scope applications also includes the CRs before being deployed in production, besides full review of all identified applications, on quarterly basis. The assessment is performed based on OWASP recommendations to ensure the CR is free from vulnerabilities before being deployed in production. During the CR assessment process, the identified vulnerabilities are remediated before go live.

In cases of business exigency, where the CR has to go live with the approval of seniors (an employee from the leadership team) and without a security assessment being conducted, an assessment should still be completed within a month's time. During the quarterly assessment of all applications, the high and medium vulnerabilities should be fixed within a period 15 days and 30 days of reporting for high and medium vulnerabilities respectively. A systemic change has been implemented in the Change Management workflow in Whizible. This would ensure that all changes in the identified list of applications are routed through the application security assessment team for conducting a security assessment before being made live.

vi) For an external change request, business teams shall create and perform test scenarios/cases mimicking production conditions. Test cases created by the business units should be reviewed by technology teams for their completeness before initiating the UAT.

vii) In order to maintain sufficient oversight by senior management before the development of a change is commenced, a systemic control has been implemented in Whizible Initiative to restrict the privilege of the Business User Head (BUH)/change approver to the grade of CMII and above for Business and Operations unit.

viii) Any Change Request that has reached the live deployment stage and is pending in the post production verification stage, will be auto closed within 3 days.

ix) Application owner is responsible for keeping the data sanitized.

x) Comprehensive testing guidelines for performing application level and security testing attached as Annexure A-1 and Annexure A-2 can be referred to by application/business teams

Migration:

Each migration activity would require the change management process to be followed. Migration may include activities not limited to application migration, data migration, infrastructure upgrades, etc.

All migration projects should have documentation indicating the requirement of roadmap/ migration plan / methodology for migration (which includes verification of completeness, consistency and integrity of the migration activity and pre and post migration activities along with responsibilities and timelines for completion of same). Explicit sign offs from users/application owners need to be obtained after each stage of migration and after complete migration process. Audit trails need to be available to document the conversion, including data mappings and transformations. Migration checklist attached in the annexure A-1 can be referred for detailed requirement of migrations.

Infrastructure Changes

Process for carrying out infrastructure changes is documented in the Standard Operating Procedures (SOP) for the Data Center.

II) **Validation to be performed, if applicable:** As detailed in the process outlined in this note

5.1 Submission of information to Principal Group (if applicable):

iProcess memo

5.2 Annexures, if applicable:

Sl No.	Annexure
1.	Annexure A-1 : Migration checklist
2.	Annexure A-2 : General testing principles and guidelines
3.	Annexure A-4 : Guidelines for achieving efficiency in testing
4.	Annexure A-3: Security testing principles and guidelines

Annexure A - 1

Migration Checklist	
S. No	Item
1	Identification of need for migration for a specific project
2	Approvals and clearances - PAC
3	Set up of a migration project team and definition of roles and & responsibility of the team members with appropriate segregation of duties.
4	Documentation of project plan
4.1	Current Process and Gap analysis (functional gaps if any, additional customizations done) – This document must record all the processes or modules that were evaluated during the study. The process should be signed off by group heads or representatives authorized to sign off on their behalf. The process note should record accounting impact as well and signed by respective groups
4.2	Identification of key data fields and data mapping; Identification of data as critical/non critical before for migration - list to be prepared and approved by the Business Head
4.3	User/ Role migration - In case users/ roles are migrated from legacy application, the privileges associated with the roles/ users in the existing system will be mapped against those in the proposed system. An authorization sign off shall be obtained for the roles to be assigned to the migrated users in the new application.
4.4	Documentation of validation parameters of Data Migration (Critical success factors) :Reconciliation and testing of migrated data from existing system to the new system I.e., From old system to New System following reconciliations to be in place like Trial Balance Reconciliation, Key data field level reconciliation, Migration Control Account reconciliation, etc.
4.5	Documentation of Reports required: Identification of Reports critical for go live.
5	Raising of Change Request (CR) in the Whizible Initiative system: BRS for the required changes from the business user/ application owner is required. CR to be raised for each migration
6	Design of the workflows/ processes/ configuration/ modules (e.g. portfolio setups, accounting rules, control totals, etc.) :As per the BRS raised by the business
7	Set-up of the workflows/ processes/ configuration/ modules
8	Testing of the workflows/ processes/ configuration/ modules :Separately by Technology team and Business
9	Testing of the processing scripts for migration data upload : to be done in test environment
10	Errors during Test phase :Tracking sheet to be maintained for errors reported during testing and subsequent rectification

11	Documentation for Functional Testing: Test cases should be comprehensive and cover all the scenarios and functionality required from the new application. The results of the testing must also be maintained. Test checking of important process must also be done on the migrated data and evidence for the same should also be made available. The audit trails preserved should facilitate comparison of post migration test results with pre-migration actual results of key (a) data/ field validations, (b) file updates, (c) reports; The functionality testing documents, its results and subsequent
12	Test results needs to be documented. Reference links to be provided for test cases used along with the test results where attachment cannot be uploaded in the Change Management application due to size limitation.
13	Roll back plan: steps for roll back, database backups, freezing of backups, etc. to be defined.
14	Migration of data to live. Complete transaction data and audit trails from the old system needs to be migrated to the new system. Else, there should be a capability to access the older transactional data and piece together with the transaction trail between older and newer systems.
15	Post-migration sign-off: Data Migration Validations – post migration. This must include a confirmation that the migration has been error free. If errors were observed, the details of the same to be reported and the steps taken to correct the same. The error logs need to be preserved. This is an interim sign off where the errors /ing items are not show stoppers
16	Error logs at the time of migration: Error log and audit trails at the time of migration to be collated. The audit trail of how the errors were resolved to satisfaction of concerned parties and signed off
17	Final Migration sign-off to be provided by the end-users after rectification of errors and all pending items.
18	The last copy of the data before conversion from the old platform and the first copy of the data after conversion to the new platform are to be maintained separately in the archive for any future reference.

Annexure A - 2

I. General testing principles and guidelines:

The following is the list of types of testing to be done for various changes. One or more of these may be adopted as deemed appropriate commensurate with the quantum and complexity of the change request:

S. No	Item
1	Unit testing - Testing of the program modules in isolation with the objective to find discrepancy between the programs and the program specifications. The responsibility of carrying out unit testing is with the respective service providers/vendors.
2	Link/Integration Testing - Testing of the linkages or interfaces between tested program modules with the objective to find discrepancy between the programs and system specifications.
3	Function Testing - Testing of the integrated software on a function by function basis with the objective to find discrepancy between the programs and the function specifications.
4	System Testing - Testing of the integrated software with the objective to find discrepancy between the programs and the original objectives with regard to the operating environment of the system (e.g. Recovery, Security, Performance, Storage, regression etc.)
5	Acceptance Testing - Testing of the integrated software by the end users (or their proxy) with the objective to find discrepancy between the programs and the end user needs.
6	Regression Testing - Testing that verifies that software previously developed and tested still performs correctly after it was changed or interfaced with other software. Changes may include software enhancements, patches, configuration changes, etc.
7	Stress/performance testing might be carried out depending on the size and complexity of change or during the induction of a new application as applicable.

Annexure A-3

II. Guidelines for achieving efficiency in testing:

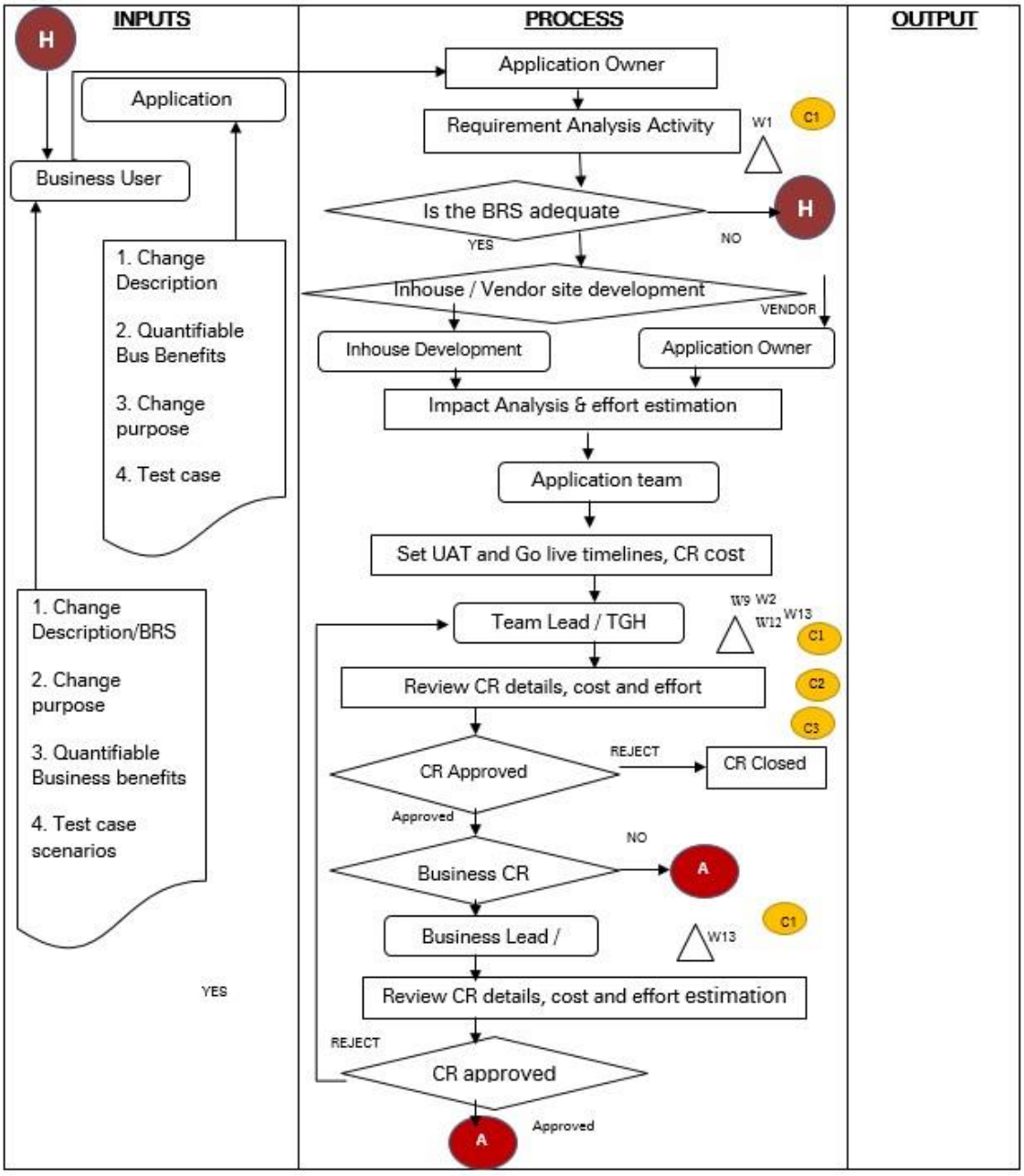
S. No	Item
1	Test cases must be written for positive and negative test cases. A good test case is one that has a high probability of detecting undiscovered errors. A successful test case is one that detects an undiscovered error.
2	A necessary part of a test case is defining the expected outputs or results.
3	Testing effort should not be planned on an assumption that no errors will be found.
4	If much more errors are discovered in a particular section of a program than other sections, it is advisable to spend additional testing efforts on this error prone section as further errors are likely to be discovered there.
5	Testing should be done both with correct data, then with flawed data.
6	If there are critical sections of the program, design the testing sequence such that these sections are tested as early as possible. A 'critical section' might be a complex module, a module with a new algorithm, or an I/O module.
7	A unit testing will be considered as completed if the following criteria are satisfied: (i) all test cases are properly tested without any errors; (ii) there is no discrepancy found between the program unit and its specification; and (iii) program units of critical sections do not have any logical and functional errors.
8	Well-documented test cases can be reused for testing at later stages.
9	Test cases and their results can be appropriately stored for future reference.

Annexure A - 4

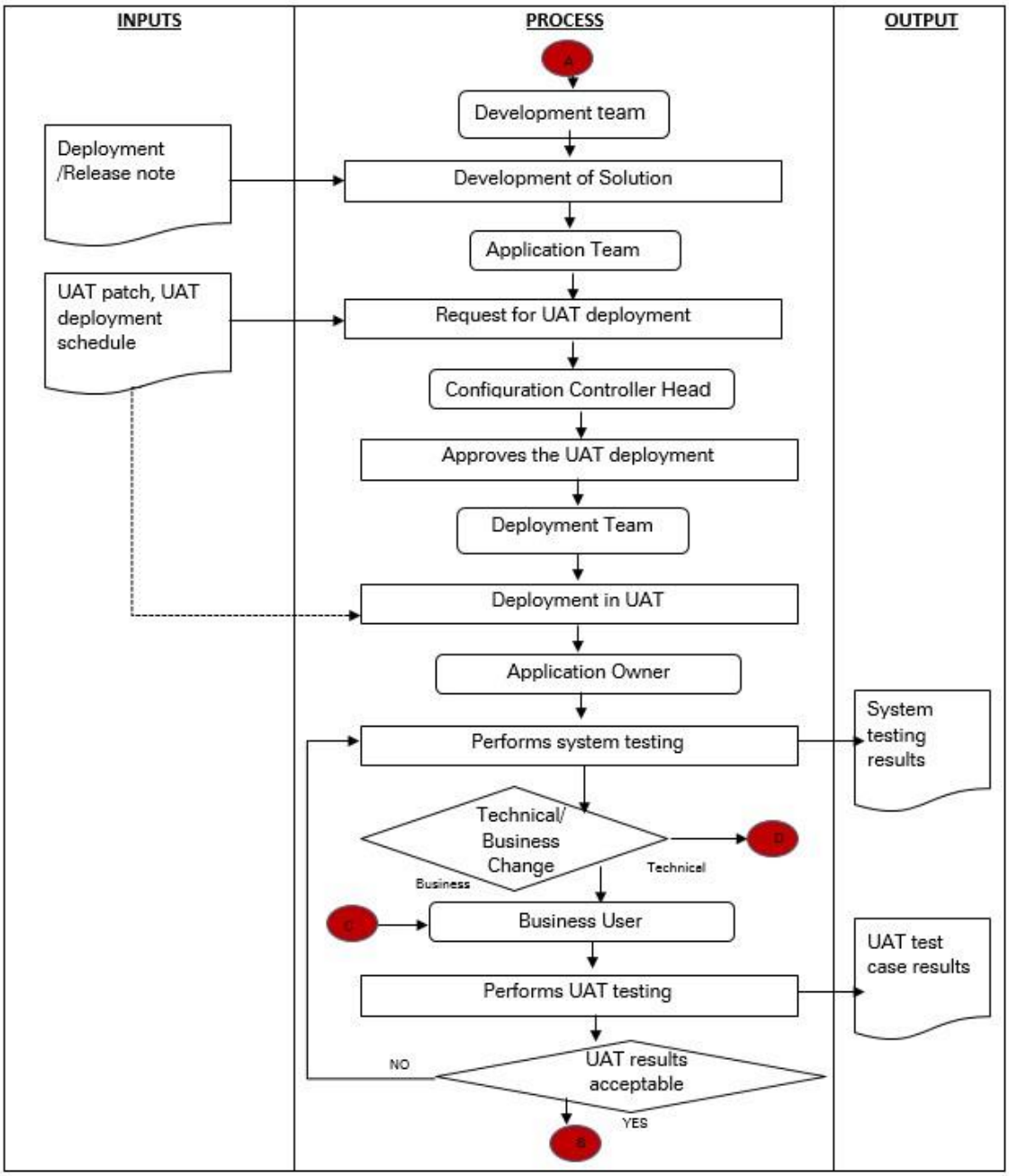
Security testing principles and guidelines:

S. No	Item
1	Session token should not be present in URL.
2	Session should expire on logout (or) after closing the browser.
3	Password should follow the ICICI password policy.
4	There should be no helpful error message at login page that can help user enumeration.
5	Browser history should not reveal sensitive information
6	Internet website not hosted on HTTPS.
7	Application pages should not be accessible without logging in.
8	Application should notify user of last login time / date.
9	Change password feature should be implemented and verify old password.
10	Logout feature should be present in the application.
11	Test / Default files should not be present on the webserver.
12	The application should not support default usernames and passwords for logging in the application.
13	Critical information should not be sent in URL.
14	Temporary account lockout feature should be implemented.
15	Autocomplete should not be enabled on create user page.
16	Session timeout within 15 minutes of inactivity should be implemented.
17	Runtime error message or database error message should not be thrown.
18	The site should not use a self-signed SSL certificate.
19	2nd factor of authentication should be implemented on sensitive actions.
20	Application should validate file content before uploading and not allow executable files formats to be uploaded.

Process: Program Change



Process: Program Change



Process: Program Change