Doc No.: D-SOP/ITG/62
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

Logical Access Management

Doc No.: D-SOP/ITG/62 Process Owner: Information Technology Group Version No.: 1.00 Last Reviewed on: 31-07-2019 Next Review Date: 30-07-2021

1.0 Name of standard operating procedure

Logical Access Management operating guidelines

2.0 Scope of applicability:

The logical access management process/guideline encompasses controlling all possible logical access paths to the information of the ICICI Bank by preventing, detecting, and minimizing the effects of unintended or unauthorized access. Access to ICICI Bank's computer systems is based on the principles of least privileges and "need to know", and is administered to ensure that the appropriate level of access control is applied to protect the information of the ICICI Bank. The level of control imposed reflects the nature and importance of the information to be protected.

The process/guideline covers the following procedures:

1. Access control and Authorization Matrix
2. User Access Creation/ Deletion/ Modification
3. Unlock ID or Resetting of Password
4. User Access Review
5. Integration of transfer and resignation module
6. Logical Access for agents/merchants of ICICI Bank accessing through internet
7. Prevention of access roles that constitute a toxic combination

3.0 Distribution list:

Groups involved in the execution of the process:

Sl. No.	Name of Group	Team head	Team lead	FPR
1	IT Governance	Madhavi Purandare	Girish Sunthankar	Ashwin Paldano/Vishnu Burra
2	Application Team	Ramesh Kumar	Deven Pathare	Anita Jiandaney
3	Business Technology Operations (BTO)	Ganesh Balasubramanian	Ashok Thiagarajan	Jitender Kumar

4.0 Procedures for the Process:

I) Process:

The Logical Access Management process/guideline is "to manage the end-to-end life cycle of user identities and their access rights in applications across the enterprise, thus protecting the information assets and data resources of ICICI Bank from unauthorized usage"

The activities performed for providing access to an application through its frontend forms part of the process and are as follows:

- User Access Creation
- User Access Deletion
- User Access Modification
- Unlock ID

- Reset Password

For the above mentioned activities, a formal request with the access requirement details needs to be raised by the requester, either for self or for another user. The request form should have the mandatory fields clearly identified ("*" is used for indicating the mandatory fields in the form).

LAM (Logical Access Management) application is the system-based workflow that facilitates the management of Logical Access rights process in various applications. The request form will have to be duly approved by the authorized approver defined in the Authorization & Access Control Matrix (ACM) of the application.

User management activities for all applications should be carried out through the LAM application. Wherever feasible, applications should be integrated with LAM through an automated LAM service for automatically performing user management activities. However, if there are technical challenges in implementing this automated service, an approval has to be obtained from the Head- Business Technology Group with reasons/rationale for such exception/deviation.

The logical access management activity for users of OS & DB, is also managed through the LAM application.

A) Authorization and Access Control Matrix:

Authorization and Access Control Matrix (ACM) document should consist of:

- the authorized approvers for the various access roles in the application
- the listing of the access roles and the respective privileges associated with those roles

Each Application should maintain an ACM document. The respective Application Owner and business owners would be responsible for initiating creation / review of the ACM document. The ACM document would require to encompass the following information:

- Name of the application
- Application owner of the application
- Business Owner of the business process supported by the application
- Technology Owner of the application
- Access roles and their respective privileges defined in the application

- Authorization matrix defining the authorized approvers for the various activities like create/ delete/ modify/ unlock/ reset password requests for the application
- Authorization Matrix defining the role-based authorized approvers for the application
- Application URL for the user access administration in the application

This ACM document needs to be reviewed periodically at least annually. However, the ACM document may be initiated for a review more frequently due to any of the following reasons:

- Change in Business / Technology Owner of the application
- Change in Authorized Approvers defined in the existing ACM of the application
- Addition / Deletion / Modification of Roles in the application
- Change in the application URL for the user access administration in the application

The version history of the ACM should capture the version number of the document and the changes undertaken in each of the review. During the mandated annual review, if the document has not undergone any changes, the version history should capture "No Changes".

A grade based approval mechanism will be applicable for approval of application roles, wherein for critical applications (tier 1/tier 2), the ACM should be approved by a Bank employee in the grade of AGM or from Leadership team and for non-critical applications, the ACM should be approved by a Bank employee in the grade of CM-II or AGM or from Leadership team.

Application roles in ACM should be categorized as either business/functional or technology and based on this classification, the approving authority should be respectively from the business or technology function. Grade restrictions of approvers would continue to apply over this restriction.

The ACM has to be approved by the identified Business Owner for the application. The approved ACM will be referred by the respective LAM administration teams while servicing the various access related requests. If the requests are not approved as per the approved ACM, the LAM admin team would reject the request.

For applications wherein the logical access requests are routed through the LAM application, the ACM creation / review can be initiated online and stored in the system. The Business Owner approval for the ACM is captured online. This online approved ACM is available to the requesters, approvers and LAM administration teams for reference while servicing various requests. The authorized approvers as per the ACM are made effective for an application automatically once the ACM gets approved in LAM system.

Program Change Management section for LAM ACM will not be applicable for applications which use Whizible Initiative as the tool for program change management activities. The approval for the change in the program change management stakeholders is captured in Whizible Initiative itself.

B) Access requests and approvals:

An access request could be raised for the following activities:

- Creation of access based on various roles in the application
- Modification of existing access based on various roles in the application
- Deletion of existing access in the application
- Unlock locked/deactivated access in the application
- Reset Password

Any of the above request type could be for:

- Employee, or
- Non-employee

The access request for an employee could be initiated by:

- Self, or
- Another User

If the requester is requesting access to an application for self, then the first level approver for the request would be the requester's Reporting Authority or personnel above the Reporting Authority (RA) in the organizational hierarchy as per the Human Resources Management System (HRMS) database.

If the requester is requesting on behalf of another user who is an employee, then the first level approver for the request would be the user's (for whom the request has been raised) Reporting Authority or personnel above the Reporting Authority in the organizational hierarchy as per the HRMS database.

It should be ensured that the non-employee has duly accepted the Non-Disclosure Agreement (NDA) document in the system and the same has been approved by the non-employee’s reporting manager in the system. .

The native applications should have system-based controls that check for duplication while trying to create user IDs.

Additionally, create and modify requests would require a role-based approval by a second level authorized approver as defined in the approved ACM document.

For other requests like delete ID/ unlock ID/ reset password/ role delete, it is mandated to have at least one level of approval from the reporting authority as per Human Resources Management System (HRMS) database. Applications which require additional levels of approval for these activities need to define the approvers as per the defined levels in the ACM document and capture the same as part of the request.

The native applications should have system-based controls for:

- locking user IDs after certain number of unsuccessful logon attempts
- locking inactive user IDs after certain period of time

The threshold values for enabling account lock-outs should be as per the Information Security Standards and Procedures (ISSP) of the Bank.

The unlocking of user IDs should be performed on the basis of unlock requests approved by approving authority as per the ACM document.

For applications, wherein the logical access requests are routed through the LAM application, the requests are submitted through an online form having systemic checks for mandatory fields. For requests submitted for Non-employees, the online form captures the confirmation of the availability of the signed NDA document. For the Reporting Authority level approver, LAM request form will show all the reporting managers in the requester's / the user's (for whom the request is to be raised) hierarchy as mapped in the HR system except N-2. N-2 grade employee in the Reporting Authority level approver will only be shown in case the requester / the user for whom the request is to be raised is directly reporting to N-2 grade employee. (Where N is the level of MD&CEO)

For employee in the grade N-2 and above, only role based approvers as defined in the respective application's ACM would be required. The reporting manager's approval will be self-approved.

The role-based approvers in LAM could be mapped based on:

- Individual approver
- Designation-based approver
- Grade-based approver
- Group ID-based approver

Based on the type of role-based approver mapped for an application, the LAM request will automatically fetch the respective approvers.

In case of requests like delete ID/ unlock ID/ reset password/ role delete, only one level of approver (Reporting Authority) is captured as part of the online request. For any application requiring multiple levels of approval, as the case requires needs to be documented separately as part of the application's user management Standard Operating Procedures (SOP) and the approvals need to be captured offline, with reference to the LAM request number.

The approvers could either approve or reject the request. The intimation of the approval / rejection is communicated to the requester and should consist of the following details:

- Approver's confirmation (approved / rejected) along with the approved date and time
- In case of a rejection, the approver's comments are mandatory
- The contact details of logical access administration team who would action the request.

The communication to the requestor along with the above details, when a request is approved or rejected, is sent by the LAM application through system generated mails.

C) Access management:

The logical access administration team is responsible for the maintenance of user access in applications. The activity of provisioning / de-provisioning in the application is based on the access requests raised and approvals obtained as per authorization matrix. The team checks for the correctness / completeness of the details / approvals provided in the request form and performs the logical access activity in the respective native application.

The logical access administration team should have an independent role with frontend administration option in the native application for the user access management activity. The other roles in the native application should not have the privileges to perform user management activity.

The maker and checker activities need to be performed by independent personnel to maintain adequate controls for segregation of duties. The user management activity should have maker & checker workflow either through a system-based maker/checker control within native applications or by capturing the activity offline.

On completing the activity as per the approved request, the team closes the request with the following details:

- Confirmation with team member name along with the closure date and time
- In case of rejection, the team member's comments are mandatory

TAT defined for the closure of requests is 1 working day for processing a request on LAM service, 2 working days for manual provisioning of individual requests and 5 working days for manual provisioning of bulk requests. However, based on the criticality of an application, the TAT for closure of requests within the application may be documented separately as part of the application operations SOP. In the absence of this documentation, the generic TAT will be applicable.

In LAM, the logical access administration team members have access to the approved requests of the applications mapped to the team and performs the logical access management activity in these native applications. On completion of the activity, the team ensures the closure of the request in LAM.

Optionally, LAM has the feature to automate, through a functionality termed “LAM service”, the following logical management activities in the native application:

- Creation of access based on various roles in the application
- Modification of existing access based on various roles in the application
- Deletion of existing access in the application

LAM service is an interface built between LAM application and the native application, for automatically performing activities like user ID creation, modification and deletion, without any manual intervention based on approved LAM requests. LAM service is scheduled to run daily at periodic intervals. For native applications using the LAM service functionality, the maker checker control need not be performed.

D) Password communication -

All critical applications (Tier 1 and Tier 2 and SOX identified) in the Bank should be authenticated through Active Directory. For applications where it is technically challenging/not feasible to authenticate through AD, an exception approval with rationale needs to be obtained from respective business and technology heads.

In case of create ID / reset password activities, on completion of the activity by the Logical Access Administration team, the user ID and password of the application needs to be communicated in a secure manner to the user. The password requirements for access in the native applications need to adhere to the Bank's password policy documented in the ISSP, which should be implemented in the respective native application in case of applications not authenticated through Active Directory (AD).

In case of applications authenticated by AD (Active Directory), the password used for accessing the application is same as the user's AD password. In case of Non-AD authenticated applications, the first time password is communicated in a secure manner following which the system enforces/advises a password change on initial logon.

On the closure of request by the Logical Access administration team, automatically generated e-mail is sent to requester/user, containing a link to view the ID and the password. The LAM application validates the authenticity of the user accessing this link with the user's session ID in the request. On successful validation, the application ID and password is viewable to the user. The password communication link authorizes the user for only one time view. If the user attempts to view the password link again, the LAM system prevents the user from doing so with a message displayed to the user - "ID/Password has been viewed once or has been compromised". For the requests logged for another user, the password communication is sent to both the requestor and the user; however only the user will be authorized to view the ID and password through the link.

The password communication is sent along with a disclaimer whose format is as follows: "Passwords sharing is strictly prohibited. Please note that any non-compliance in this regard will be considered as a breach of security control devised by the Bank. The Password policy for ICICI Bank is available on the URL given below, for your reference - <URL of the password policy>"

E) Access de-provisioning -

Delete requests could be generated for de-provisioning of access in native applications in the following scenarios –

- Change in user's access requirements
- User's transfer
- Resignation
- Termination of service

The delete request form for user's access in the respective applications needs to be submitted by either the user or on behalf of the user by the user's reporting authority. On approval as per the ACM document, the Logical Access Management administration team will de-provision the access of the user in the native application.

The user access de-provisioning is done through logical deletion of user IDs in the native applications.

The LAM application has built-in controls to mitigate risks emerging due to the delay in de-provisioning of access rights of users in native applications who have resigned / have been transferred to a different department. The LAM application interfaces with the Human Resources Management System (HRMS), through a scheduler running daily, for fetching the list of users who have been transferred or who have resigned.

The LAM application fetches the list of resigned employees from Human Resources Management System (HRMS) based on the following criteria -

- If the resignation application status is 'Approved'
- If last working date (LWD) has been approved by the reporting manager

The reporting authority may initiate the disabling of access by submitting a delete request for the user or by advising the user to self-initiate the delete request.

However, if the disabling of access is not initiated, the LAM application, on the user's last working day will automatically generate the delete requests for de-provisioning the access rights of the user in the respective native application.

Such automatically generated delete requests for resigned employees for an application would get rejected if at the time of approval/rejection of the request if, the resigned employee has inventories/ service requests/ cases still assigned to him/her. The employee’s reporting manager would be responsible for reassignment / closure of those cases and raising the deletion requests for the resigned employee.

If a deletion request of a resigned employee has been generated manually but has not been approved by his/her RA, then post his LWD, an automated deletion request will be generated for deletion of employee’s access, notwithstanding the existing manual request.

The LAM application fetches the list of transferred employees from the HRMS based on the following criteria:

- The status of the Transfer application is 'Approved'
- Recommended Transfer Date in present department has been approved by the reporting manager.

The Recommending Authority is sent a list of applications that the transferred user has access to through a system generated mail in LAM. The transferred user's existing access to the native applications may be retained or deleted based on the following:

- In LAM, if the Recommending Authority selects 'Continue', it would trigger an e-mail intimation to the Level 2 approver (Reporting Authority in the department to which the user has been s transferred to). The Level 2 approver may approve or reject the user's access.

In LAM, if the Recommending Authority selects 'Disable', it would trigger the generation of auto delete requests for revoking the user's access in various native applications.

However, if such action is not initiated by both the Recommending Authority and the Level 2 approver, LAM will automatically generate delete requests for de-provisioning the access rights of the transferred employee in respective native applications on the recommended Transfer Date.

For absconding users and for resigned/transferred non-employee users, the reporting manager is responsible for ensuring that the delete requests are submitted for disabling the access in native applications.

TAT defined for the closure of requests is 1 working day for processing a request on LAM service, 2 working days for manual de-provisioning of individual requests and 5 working days for manual de-provisioning of bulk requests. However, based on the criticality of an application, the TAT for closure of requests within the application may be documented separately as part of the application operations SOP. In the absence of this documentation, the generic TAT will be applicable.

F) Monitoring of access privileges of separated/transferred employees:

In order to mitigate the risks arising from the probable misuse of access rights by separated or transferred employees in cases where there is a delay in deletion of their IDs, a process to review usage of access rights granted to employees to ascertain that there are no cases of misuse of such privileges has been implemented. Any cases of misuse of access by separated employees would be flagged off to the Human Resources Management Group (HRMG) for necessary action.

The detailed process of monitoring is enumerated below:

i). Monitoring access rights of employees to applications after their separation from the Bank

At the end of every quarter, a monitoring process would be initiated as under:

a. A list of employees whose resignations/terminations were recorded in the HRMS system during the previous quarter would be generated.

b. Details of application ID deletion requests (including the date & timestamp of deletion of IDs in each application) for the aforementioned list of separated employees would be generated from LAM.

c. Only applications classified as financially sensitive (i.e. all applications classified as SOX-critical) would be considered for this review.

d. All cases where the deletion of IDs in the applications has been done in a timely manner would be excluded from the scope of this monitoring. This would include:

i. LAM requests, which have been successfully actioned (i.e. IDs deleted) on or before 9:00 a.m. on the day following the last working date of the employee, as recorded in HRMS.

ii. Applications, which are integrated with active directory (AD) and wherein the AD access rights of the employee have been successfully revoked on or before 9:00 a.m. on the day following the last working date of the employee, as recorded in HRMS.

iii. Applications where the access is not provisioned/de-provisioned through LAM and instead the access is linked to HRMS. For such applications, the recording of the separation of the employee in HRMS automatically ensures revocation of access to such applications.

e. For residual cases, transaction logs for the period elapsed since the last working date of the employee would be generated. Scrutiny of transaction logs would ascertain if IDs of separated employees have been used to access the application after the last working date of the employee.

f. A list of all such employees, along with the transaction logs evidencing such access would be forwarded to the Human Resources Management Group (HRMG) for necessary action.

Controls for managing logical accesses of separated employees

In order to mitigate potential risks arising out of non-revocation of access rights of separated employees, an automated process is configured to trigger automated delete requests in LAMS based on the last working date (LWD) in Human Resource Management System (HRMS). However, delays in revocation of access rights occur due to lags in updating the LWD of the employee in HRMS on account of unprecedented causes like absconding employees, termination, retirement or death of an employee where the LWD cannot be envisaged in advance.

The following control measures help in minimizing the risks arising out of delayed revocation of access rights for separated employees:

- For voluntary employee resignations, HRMS would be updated at least one day prior to the LWD by building systemic restrictions that prevents modification/approval of cases where LWD is same or before the current date. This would ensure that the access revocation is triggered by LAM (basis the trigger from HRMS) on the LWD of the employee. Subsequently, HRMS would send a trigger to AD on the LWD, between 3:00 PM to 6:00 PM for deleting the employee ID from the domain. The TAT followed by the DPC team would be 2 working days to ensure effective deletion of user accesses in applications that are not integrated with LAM service on the LWD.

- Since the aforementioned control is not feasible for exceptional cases of separation like termination, death or disappearance of an employee, a capability would be built in HRMS to capture the category of separation (either Normal Separation or Abrupt Separation) while passing the entry in the system. The systemic control of preventing modification of the LWD of the employee in voluntary resignation cases would be relaxed to an extent of 21 days in such instances to allow HRMG officials to make retrospective updates in HRMS as per the existing practice.

- An audit trail capturing the details of employee under separation, date of uploading the entry, category of separation selected, and reason for selecting the category, the maker and the approver of the entry would be maintained in HRMS for audit purposes.

Notwithstanding the implementation of the aforementioned control, the activity of monitoring of access rights of separated employees is carried out on a quarterly basis.

ii). Monitoring of access rights of employees transferred within the Bank

At the end of every month, a monitoring process would be initiated as under:

a. A list of all employees whose transfers (within the Bank) are recorded in Human Resources Management System (HRMS) during the previous month is generated from HRMS.

b. The list is analyzed to identify if any delays have occurred in updating the "Transfer Effective Date" in HRMS or if there is any mismatch between the employee's actual date of transfer and the "Transfer Effective Date" as updated in the HRMS. The logical access of transferred employees in cases where such lags are observed is scrutinized further to ensure that there are no cases of misuse of access privileges on account of delay in updating the transfer date.

c. Transaction logs for the time period elapsed since the transfer effective date of the employee are generated to identify if the transactions posted by the employee are authorized.

d. In case unauthorized transactions are found, the logs evidencing such transactions would be taken up for necessary action.

1. Controls for managing logical accesses of transferred employees

To mitigate the risk arising out of non-revocation of access rights for transferred employees, an automated process to de-provision access rights for transferred employees has been implemented. Based on the transfer effective date received from the Human Resources Management System (HRMS), the Logical Access Management System (LAMS) triggers deletion requests for revocation of access rights of a transferred employee.

However, delays in revocation of access rights of transferred employees occur due to the lags in updating transfer effective date in HRMS. To address this lag, a systemic restriction has been built in HRMS that prevents modification or approval of transfers 2 days prior (T-2) to transfer effective date (T). Further, on approval of transfer requests, HRMS would send the trigger by T-1 day to initiate the access revocation. In case of branch banking group, access provisioning as per the RBAC matrix would be initiated on the transfer effective date (T).

The details of the process are enumerated below:

- On change of designation / location / department of a Branch Banking employee (for employees in other groups, triggers would be sent on change in department only), HRMS would send the trigger to LAMS on T-1 where T is the "transfer effective date"

to generate automated delete ID requests to be processed either manually by Data Processing Centre (DPC) or through automated LAM Service as the case may be, within the defined Turn Around Time (TAT). It is proposed that the TAT followed by the DPC team would be 2 working days to revoke all application access rights. Open access applications would continue to be available to all employees without any necessitating any approvals.

- Automated requests for creation of IDs for newly provisioned access rights would be generated by LAMS as per matrix defined in Role Based Access Control (RBAC) module for Branch banking. Such requests would be generated through a scheduler, post successful deletion of user id in respective applications. These requests would be deemed to be auto-approved and processed either manually by Data Processing Centre or through automated LAM Service as the case may be, so as to ensure that the new access is provisioned on "T for all applications which are covered under the purview of LAM Service.

- Access to other applications (not covered in RBAC matrix) if any, would be provisioned by the user through a LAM request, which would necessitate requisite approvals as laid out in the Access Control Matrix of the application for which access request is requisitioned.

Cases in which employees are temporarily assigned to other departments / locations / designations, would not be treated as "Transfers" as employees return to their original assignment after completion of the temporary assignment.

For user access revocation (and subsequent user access re-provisioning, in case of Branch Banking department) for temporary assignments auto initiated through LAM, the systemic restriction of updating the transfer effective date on T-2 was not deemed practical to achieve on account of the fact that temporary assignments are decided by the HRMG in consultation with the respective business groups, only a day in advance prior to the commencement of an assignment depending on variable factors like unplanned absence, availability of employees, business requirements, emergency etc.

In order to have a tighter control for user access management for employees on temporary assignments, the existing scheduler that sends data from HRMS to LAM for triggering automated delete requests would be run twice, once at the beginning of the day (as is done presently) and again at the end of day. If any temporary assignments are updated in HRMS prior to the transfer effective date (T), the access revocation and access re-provisioning would be carried out on T. If temporary assignments are updated in HRMS on T, then LAM would be able to trigger user access revocation and re-provisioning on the same date by virtue of the scheduler that would run at the end of day. The only exception to the above would be the LAM requests handled manually by the DPC team.

Notwithstanding the implementation of the aforementioned controls, the activity of monitoring of access rights of transferred employees would continue to be carried out on a quarterly basis.

In order to prioritize the deletion of user IDs for separation/transfer cases and to be able to adhere to the TAT defined in those cases, a control is being built in LAM to differentiate between deletion requests generated/raised for separation and transfer cases from the other type of deletion requests.

Additionally, to expedite cases where IDs could not get deleted due to failure of schedulers, an automated failure report would be built so that the LAM DPC team could check these failures and re-initiate any cases of failed deletions.

G) Blocking employee IDs during absence/leaves

As an information security measure, the access rights of employees on certain categories of leave are disabled on the day of commencement of leave. These rights are restored on the day the employee resumes office on the conclusion of his leave.

To facilitate maintaining uniform rules of access control across all banking applications, the blocking of access rights has been built at the active directory (AD) level. The blocking of access to applications has been implemented for employees falling in the below two categories:

A) Employees who are entitled to mandatory leaves, as identified by the Human Resource Management Group (HRMG), and
B) Employees who have applied for leaves for a continuous period of 14 calendar days or more

An employee whose ID is disabled would be restricted the following:

- Logins to their desktop/laptop
- Access to any AD authenticated application
- Access to mobile based bank applications
- Access to VPN
- Access to Email

Each day, a list of employee IDs satisfying the aforementioned criteria would be generated from HRMS and sent to AD before the commencement of operations. AD would disable such employee IDs from logging on to the ICICI Bank domain, thereby restricting the employee from accessing the Microsoft Exchange server and performing business activities/operations of any manner.

Re-enabling blocked IDs

Employee IDs disabled on account of an employee being on leave would be enabled by AD automatically on the day following the last day of leave in HRMS. For such employees, a trigger would be sent from HRMS to AD for re-enabling employee IDs every day before the commencement of operations. In case an employee resumes office earlier than the expected end date of leave due to business reasons, the employee ID may be explicitly enabled by raising a service request through I-Helpdesk.

In addition to the aforementioned control, a process has been implemented for treasury applications for deactivation of user IDs during long or unauthorized leave.

G) Deactivation of user IDs during long leave or unauthorized leave

Process to deactivate the user access to certain treasury related applications on account of planned / unplanned leave has been established. The list of applications would be as decided as necessary from time to time..

As an information security measure, the Active Directory (AD) IDs of employees (Up to N-2 grade) will be deactivated who are on continuous approved long leave for >= 30 days (calendar days) in the below mentioned categories of leave. The deactivation would be done from the leave start date or the date on which the leave is approved, whichever is later:

- Maternity Leave
- Child Care Leave
- Adoption leave
- Sick Leave
- Fertility Leave
- Study Leave
- Long Leave
- Leave without Pay

In addition, Active Directory(AD)IDs of Employees in Grades of CMII and below ,who have not signed in the muster for a continuous period of 15 (calendar) or more days and there is no approved leave for the same days, will also be blocked.

The ID can be activated post approval from reporting authority by logging a request using i-Helpdesk. Please refer to the detailed steps mentioned below:

- Helpdesk Link : http://10.16.17.197:90, New Service Request –> Type: IT Process Management –> Area: Active Directory Access –> Sub Area: Enable AD ID
- Post logging the call, please ensure that the request is approved by the reporting authority for further action
- Once the request is approved through FCRM, the ID will be enabled automatically within one hour and the call will be closed
- The ID activation request can be logged in Helpdesk "on behalf of the concerned employee" by any other employee

2. Disabling of inactive consultants' IDs

Consultants engaged with the bank are provided access to the Bank's domain by creating an identity through the Non-Employee Enrolment System (NEES) by initiating a NEES request and obtaining two levels of approvals by the ownership manager and an additional approver who is in the grade of AGM or from Leadership team. The validity of the NEES ID (BAN ID) thus created, is until the 'Expected last working date' provided in the NEES request.

As a control measure, NEES restricts the engagement duration of a consultant to a maximum of six months. However, for cases where consultant IDs are valid for 6 months, to mitigate risks arising out of consultants leaving the organization earlier, a control has been implemented to disable BAN IDs that have been inactive for a period of 15 days or more. The detailed steps are enumerated below:

- Access logs generated from Active Directory (AD) would be monitored by the AD team on a daily basis to capture the consultant's last successful log-in in to ICICI Bank network

- A notification e-mail would be triggered to the consultant's reporting manager apprising him/her about the consultant's absence if the consultant's ID is found inactive for a continuous period of 5 days or more
- A scheduler would be executed in AD, at the end of each day, to disable IDs that are inactive beyond 15 days, thereby restricting access of these IDs to the ICICI domain. However, these IDs wouldn't be explicitly deleted from AD.
- NEES would host the information on the number of consultants in disabled state based on data received from AD on a daily basis
- For BAN IDs that are inactive beyond 30 days, deletion requests would be triggered from AD to NEES
- Subsequently, NEES would initiate access revocation through LAM for the BAN IDs that have been deleted due to such inactivity.

To restore access rights of IDs that are disabled on account of inactivity, a Service Request (SR) would be raised in i-Helpdesk and approved by an employee of the bank, not below the grade of Manager. On closure of the SR, all accesses to the BAN IDs would be restored and would remain valid until the "Expected last working date" of the consultant as requisitioned through NEES.

In addition to the aforementioned control, the monitoring of access rights of consultants carried out on a quarterly basis would be carried out.

H) Reconciliation (only for applications having user management being routed through LAM)

Since the approved requests are captured in LAM application and the actual user management activity is done on the native application, there exists the inherent risk of mismatch of the active user list in LAM system and the native application.

To mitigate the above risk, a control in the form of quarterly reconciliation of active user lists from LAM application and each of the native application is implemented. The reconciliation of active user list ensures their synchronization with each other. The mismatches generated out of the reconciliation activity are be corrected and brought in sync by deleting the mismatch IDs. Also a RCA is mandatory to be performed whenever a discrepancy is identified in the RECON process.

The quarterly reconciliation activity has to be undertaken before the quarterly user access review, to establish the completeness and correctness of the active user-list consider for the user review. The Logical Access administration team ensures that the reconciliation of active user list for their respective native applications are completed and also ensure the closure of all the delete requests generated due to reconciliation process prior to the start of user access review process.

In addition to this, a list of separated users (both employees and consultants) should be obtained from HRMS and NEES and a reconciliation should be carried out between the IDs in Active Directory, LAM and the native application to ensure that IDs of separated users have been deleted in LAM, AD and the native application.

I) Quarterly User Access Review

The user's access in various applications need to be reviewed by the user's reporting manager or by the users' reporting manager's manager, in the absence of the immediate reporting manager, on a periodic basis. The period defined for the user access review is quarterly. As part of the review, the Reporting Manager should confirm on the accesses existing for the user in various applications within 15 days of the initiation of user review process.

The reporting authorities are communicated the list of all their reportees with their active access roles in each of the application.

For the user's access, wherein the reporting authority confirms as "Retain", the access will continue in the application.

For the user's access, wherein the reporting authority confirms as "Delete", the delete request is initiated for disabling the access in the application.

For the users of designation levels "N-2 and above", where "N" is the grade of the MD&CEO, the frequency of the user access review undertaken would also be quarterly.

In LAM, the user access review activity is initiated at the beginning of the last month of each quarter and is scheduled for a period of 15 days. Through LAM system, an intimation mail is sent to all the reporting managers at periodic intervals during the 15 days schedule period.

During this user access review period, the LAM system auto generates approved delete requests for the user access confirmed for delete by their reporting authorities. In LAM, the user access generated in applications due to create / modify requests submitted during the user access review period will not be considered in the current quarter. The review of all such user access will be undertaken as part of the next quarterly review.

At the end of the scheduled user access review period, the LAM system auto generates the delete requests for non-confirmed access in applications

The Logical Access administration team should ensure the closure of all the delete requests generated due to user access review. The closure of the delete requests should be completed within each quarter for which the user review was undertaken.

TAT as defined earlier in the PAC note for user management activities like creation/modification/deletion would not be applicable for the requests generated post the user review period.

J) User management for access via internet

For native application having user provisioning/de-provisioning for Internet users (like ICICI Partners, Agents, Merchants etc.), formal requests have to be raised for all activities. The entities involved in the process will be:

- Relationship Manager (RM)- Employee of ICICI Bank
- Agency Admin – The approving authority from the Agency
- Agents – The users/employees from the Agency

All agencies will be assigned a unique agency code which needs to be provided by agents while raising a request for an application.

i) Access requests and approvals -

An access request could be raised for the following activities:

- Creation of access based on various roles in the application
- Modification of existing access based on various roles in the application
- Deletion of existing access in the application
- Unlock of locked/deactivated access in the application
- Reset Password
- Role Delete

The users from agents including agency Admins can raise a request for activities like Creation, Modification, Deletion, Unlock, Role Delete and Reset of a particular application through LAM application. First level approver would be respective Relationship Manager from ICICI Bank.

Additionally, create and modify requests would require a role-based approval by a second level authorized approver as defined in the approved ACM document.

For other requests like delete ID/ unlock ID/ Role Delete / reset password, it is mandated to have one level of approval from relationship manager from ICICI. For applications requiring additional levels of approval for these activities approvers need to be defined as per the levels in the ACM document and capture the same as part of the request.

ii) Registration of Agency:

The relationship manager from ICICI Bank for a concerned agency has to raise a SR in iHelpdesk in the following path for getting the agency registered in LAM.

Path in iHelpdesk
Master Maintenance -> LAM -> Agency Registration-LAM

Upon approval by the reporting authority of the Agency's relationship manager, the LAM administration team will check whether the agency is already present in LAM and will create the agency in LAM if it doesn't exist. At the time of agency mapping there are options to map the Relationship manager who will be associated with the Agency and who will act as the first level approver. The applications that needs to be made visible to the Agency via the LAM Internet module can be specifically chosen. Finally, as a security measure maximum no. of registrations can be set as a parameter wherein LAM will restrict the no. of registrations from a particular agency if it increases beyond the set parameter. The agency registration form on submission is sent for on line approval to the relationship manager from ICICI bank.

iii) Registration of Admin:
Once the Agency registration is successfully approved by the RM, the Admin of the agency gets a system generated mail communication from LAM about a unique Agency Code, a temporary user ID and temporary password. The agency Admin accesses the temporary

access page and enters the details provided on mail. On successful entry the Agency Admin is directed to the Self Registration page and registers himself/herself by choosing a LAM Login ID of his/her choice and a password. Along with this there are 3 challenge questions asked for checking authenticity of the user in case of Forgot Password request. On submission, the self-registration approval is sent online to the RM. Once approved by the RM, the agency Admin will be able to login to LAM application from the internet site (https://lam.icicibank.com) to lodge request for any application.

iv) Registration of Agent:

Once the Agency Admin registers, the agents (users of the agency) can self-register themselves in LAM. The Admin shares the unique Agency Code with the agents which is the initial parameter for self-registration. Apart from choosing a unique LAM login ID and password, there are 3 challenge questions asked for checking authenticity of the user in case of Forgot Password request. On submission, the registration approval is sent online first to the agency admin and after agency admin's approval, the request would be forwarded to the RM. Once RM approves the request, the Agent(s) will be able to login to LAM from internet site to raise a request for any application.

v) Forgot Password:

The admin/agent clicks on the Forgot password option available on the LAM login page. The system will prompt to enter the LAM login ID and answers to 3 challenge questions which the user had answered at the time of self-registration. On successful submission, the system will prompt to enter New Password with which he can login to LAM.

vi) User Access Review:

The user access review for these external users will follow the same process as that of internal users. The only difference being that these user IDs will be validated by the concerned Relationship Manager from ICICI bank for a respective agency.

K) User management for RBAC functionality:

Role based access is a feature in user provisioning process which allows the end user to raise a single request to get authorized access to pre-defined set of applications.

RBAC request can be raised for SELF or for another Employee

Access to various systems and roles within each system depends on the corporate role. Corporate role of the end users for whom the request is raised is decided on the basis of the following parameters in Global address list (GAL)

- Company
- Department
- Group
- Main Group
- Designation

Configuration of corporate role wise application list and roles within each system requires approval from a member of the leadership team of the functional group for which the functionality is to be enabled.

Since the application systems as well as the roles within each systems are preconfigured, end user while raising the request does not have to select the application and role in the request form while raising the request and hence approval from second level approver (role based approver) is not required for RBAC request. Post reporting authority approval, individual LAM request for the predefined systems are generated and are bucketed to the respective user management team or LAM service.

Access requests and approvals:

- To raise RBAC request, requester will have to select RBAC request menu in LAM
- Based on his details in GAL, his corporate role will be decided and will be displayed in the drop-down.
- Requester will select the corporate role from the drop-down and will provide mandatory details
- Requester will select the reporting manager for approval.
- Reporting manager can approve or reject the request. On rejection, the request will be closed.
- On approval, individual request would be created for each application system on the basis of the user's corporate role.

These individual requests will be processed either manually or through LAM service.

Following processes remain same as defined earlier in this PAC note for the RBAC request.

- Access management
- Password communication
- Access de-provisioning
- Reconciliation Quarterly
- User Access Review

Role Based Access Control for newly hired employees in the Bank has been implemented in LAM for Branch banking employees, the Human Resources Management Group (HRMG) and the Self Employed segment. (SEG)

Implementation of provisioning an automated Role Based Access Control (RBAC) for Branch Banking employees:

The following process has been implemented for Branch Banking employees to prevent service issues arising from non-availability of access to applications needed for respective corporate role on account of role changes or quarterly validation not conducted.

- HRMS will send the trigger to LAMS on change of designation / location / department of a Branch Banking employee. (For employees other than Branch Banking group, HRMS will send the trigger based on change in department.) The trigger will be sent on T+1 where T is the date of action. Based on the trigger, automated delete ID requests will be generated by LAMS on T+1 day. Such requests shall not require any approval and will be processed either manually by Data Processing Centre (DPC) or through the automated LAM Service as the case

may be, within defined TAT. Open access applications shall continue to be available to all employees without any approval process.

- Automated create ID requests will be generated by LAMS for applications as per matrix defined in RBAC (Role Based Access Control) module. Such requests shall be generated through a scheduler, post successful deletion of user id in respective applications. These requests shall be deemed to be auto-approved and processed either manually by Data Processing Centre or through automated LAM Service as the case may be, so as to ensure that the new access is provisioned T+1 for all applications which are covered under the purview of LAM Service.

- Access to other applications (not covered in RBAC matrix) if any, shall be provisioned by the user through a manual LAM request, which will require due approvals as laid out in the Access Control Matrix of the respective applications.

As provisioning of this role based access is automated, it is exempted from the quarterly user validation process for accesses covered under RBAC matrix. The LAM system has following features to mitigate the risks of this process:

- Quarterly validation is not exempted if the employee is tagged as absconding / fraudulent or is on long leave. The tagging flag shall be provided by HRMS application.

- The user access is de-provisioned automatically when the employee is separated by way of resignation / retirement / termination (as per current de-provisioning process).

- Entire user access validation for Branch Banking shall be carried out at least once a year (recommended in Quarter 1).

L) Generic ID user management: Request for creation, modification and deletion of Generic IDs in OS and DB is tracked through Logical Access Management system (LAM).

An ID creation request is accepted on submission of all the mandatory details. A De-duplication check is carried out on the basis of Server IP & Generic-ID-Name for OS; for DB, it is based on Application Name, DB name and Generic-ID-Name.

The approval process is as per the workflow defined in LAM application. If a request is rejected, it is closed without action.

Post all approvals, the request is forwarded to the respective team as defined below:

If request pertains to Windows OS, it is forwarded and actioned by NT Admin Team.
If request pertains to UNIX OS, it is forwarded and actioned by Sys Admin team.
If request pertains to Oracle or Sybase DB, it is forwarded and actioned by Sys DBA Team.
If request pertains to SQL DB, it is forwarded and actioned by SQL DBA Team.

Maker-Checker controls exist in the Generic ID management process wherein the same user cannot be maker as well as checker for a request.

Mapping of Generic ID in ARCOS

Generic IDs are mapped and their access is controlled through ARCOS, a Privilege ID Management application. ARCOS logs all actions performed by a user (using a Generic ID) on the OS/DB to establish accountability and non-repudiation. It also includes the password vault, which enables strong password generation and encryption. By vaulting, ARCOS prohibits access to the credentials required for accessing a server outside ARCOS.

Once a Generic ID is mapped in ARCOS by the ARCOS administrator, it changes the password of the Generic ID on the target server and vaults it. A user who wants to access this Generic ID should have access to ARCOS, which is approved as per the user provisioning process in LAM.

There are instances where Generic IDs are not mapped in ARCOS. For such cases, appropriate justification is captured in LAM and is approved by ISG. Generic ID mapping in ARCOS also is governed by hardening policy guidelines. For example, Default IDs created during standard software/application installation are exempted. Such exemptions should be either documented in the OS/DB hardening policy or specifically approved in LAM with justification. Exception requests for generic IDs that are not/cannot be mapped in ARCOS should be approved by all stakeholders including ISG.

A process would be instituted to disable those server IPs in ARCOS that have been deinducted.

User Review

Generic IDs present in LAM should be reviewed and validated by the Generic ID owner's reporting manager or by a manager senior in the hierarchy once in a quarter. The reporting manager has the option to either retain or delete the Generic ID during the review. Basis the option chosen during validation, appropriate actions will be carried out in LAM, ARCOS and the target server either automatically (if the services are integrated) or manually.

Ownership mapping of Generic ID

Generic ID ownership is assigned at the time of ID creation. If the owner changes due to transfer or resignation, the ID should be mapped to another employee within the team.

Generic ID reconciliation process

Generic IDs active on Production, Fallback and DR servers should be reconciled with LAM and ARCOS on a quarterly basis. The base for identifying active servers will be App360; i.e. Generic IDs will be extracted for all target servers based on the IPs/Hostnames registered in App360. If any unreconciled IDs are identified in the reconciliation exercise, appropriate remedial action would be taken.

M) On boarding process for consultants and non-employees

Consultants and non-employees (referred to as 'Consultant' in this section) engaged with the bank are provided access to the bank's domain by creating an identity through Non-Employee Enrolment System (NEES). Any member from the business unit, employee or non-employee that hires a Consultant can initiate the on boarding process of the Consultant by creating a new request through NEES. The request form captures essential data as listed in Annexure II for initiating the on boarding process.

Once the request form is submitted for further approvals, NEES checks for duplicate entries using the primary fields – first name, last name, parent company and date of birth.

The request form is sent for two levels of approval in case there are no duplicates found in the database. The first level of approval is sought from the ownership manager selected in the request form. The ownership manager must be an employee from the bank – this ensures that the ownership of the Consultant's ID rests within the bank. The second level of approval is sought by an employee of the grade "AGM or from Leadership team" picked from the reporting hierarchy of the 1st level approver. If 1st level approver is "AGM or from Leadership team", then 2nd level approval is not required separately. For every approved enrolment, a unique NEES ID is generated.

The generated ID is then sent to the Active Directory (AD) for domain access creation. The TAT for creation of domain access is 1 working day post the final approval is received. The Consultant's ID is updated in AD based on the details provided in the initial request; reporting manager in the Global Address List (GAL) is recorded based on the Reporting Manager selected in NEES request. Subsequent to addition of the new ID into AD, mail box access is configured by the Mail Admin team with a TAT of 1 working day.

The ID created as per the above process shall be valid for the Consultant for a maximum period of 6 months from the date of raising the request. If the Consultant requires to continue association with the bank beyond six months, then a request for modifying the expected last working date can be lodged through NEES before the expiry of the ID for another 6 months. In case the expected last working date of the ID is not extended before the expiry of the ID, then NEES shall initiate a delete request at the end of expiry date.

Password communication

User ID and Password (randomly generated) are communicated securely through NEES in two halves. One half of the password is sent to the requester and other is sent to the ownership manager.

Access to applications

On successful creation of ID for the Consultant, accesses to applications in ICICI Bank domain can be requested as per existing the Logical Application Management process.

Access requests and approvals

1. Requester logs a request to enroll the Consultant for domain access or/and Mail access in Bank post which this request is sent for 2 levels of approval.

2. First level approver is the immediate reporting manager associated with the non-employee.
3. Second level approver will be AGM or from Leadership team in the reporting hierarchy of the 1st level approver.
4. If first level approver is AGM or from Leadership team, second level approval is not required.
5. For Delete request, only one level of approval from reporting manager is sought.
6. On approval by all, domain access and/or mail access (if requested) is granted and password in two halves is communicated to requestor and ownership manager

N) E-NDA feature:

E-NDA is an electronic version of Non-Disclosure Agreement being signed through LAM application and is enabled at Country, Application or at Business group level. (This Business group is identified using the details updated in GAL under Organisation > Group).This feature is a control in LAM for ensuring that the NDA is signed off by the users as per various geography regulatory requirements.

The Confidentiality Undertaking or eNDA is accepted by the employees as an onetime exercise and approved by their manager or as per the frequency defined by the business/various geography's regulatory requirements or subsequently when a new version of the eNDA is introduced, the employees are again required to accept the terms of the eNDA and subsequently their manager needs to approve it.

To ensure that all such employees (who are mandatorily required to sign an E-NDA) have accepted the Confidentiality Undertaking, there exists a control in LAM wherein the user is prevented from raising a LAM request of any system access without having accepted the terms of the E-NDA hosted on LAM under

Request > E-NDA Signing Form.

For certain Business groups in the bank who have already accepted the undertaking before, it has been mandated that the E-NDA undertaking would now be required to be accepted in LAM on an annual basis. Such acceptance procedure should be carried out within any given month of a given financial year on an annual basis. Employees who join these groups (requiring E-NDA to be accepted on an annual basis) any time after initiation of this eNDA validation will be required to accept the undertaking under the E-NDA immediately after joining the group. If acceptance by the user or approval by their manager of the confidentiality undertaking (e-NDA) is pending as at EOD of eNDA validation cycle the respective logins to systems will be deleted automatically and further the users will not be allowed to apply for fresh logins till the confidentiality undertaking (e-NDA) is accepted by the user and approved by their manager.

O) Temporary Access

In order to mitigate the risks arising from non-deletion of temporary Access to native applications within TAT, a new feature “Temporary Access” has been introduced in user provisioning process that allows the end user to raise access authorization request for a particular application for a predefined validity period (< 1 month). At the end of the given

validity period, automated delete ID requests will be generated by LAMS for the given temporary access. Such LAM request will be auto approved by the system and will be closed within pre-defined TAT. Temporary Access request can be raised by an employee either for himself or for another employee by clicking on the corresponding radio button on LAM request form.

P) Retention of records

The approved requests and the LAM records will be maintained as per the Record Retention Policy of the Bank.

Q) Roles in LAM application

The following roles are configured in LAM to perform logical access management activities:-

- Requestor – Logical Access Requests are initiated by a requester.
- Approver/s – All requests initiated are approved by approvers as per the ACM document.
- Logical administration team – This team performs the user management activities in the native applications and ensures the closure of the logical access requests raised. The following two roles forms the function of this team
- Maker – performs the activity of providing access in the native application based on the approved request.
- Checker – checks whether the activity performed by maker is as per the approved request and the process.

R. Toxic combination of roles/Segregation of duties

Access controls are the collection of techniques, processes, and mechanism that helps to protect the assets of an organization. User access management is one of the key pillars for ensuring confidentiality & integrity of a product/solution/platform, appropriate implementation of which is largely based on the principles of least privilege and segregation of duties (SOD). The former means that people only get the privilege they need in order to do their job, whereas the latter is a situation where privileges are bifurcated between users so that an individual user does not possess combination of access rights on a system/ combination of systems, which could lead to oversight or malicious activity. "Toxic combinations" of roles or individual privileges are those that indicate combination of access rights to a particular system/combination of systems which can be misused for conducting unauthorised activities.

a. Examples of toxic combination

At an application level, example of toxic combination can be maker/checker (if there are not adequate application level controls), wherein in case any single individual has both the access rights, it can be misused for carrying out unauthorised transactions. The same example can be extended for combination of applications, wherein a specific access in one system along with a combination of a different role in another system, might allow an individual to conduct unauthorized activities. One indicative example would be having access in core banking system along with SWIFT system, wherein an individual can initiate

a transaction from the core banking system and then can also initiate or approve the corresponding payment transaction from SWIFT.

b. Guidelines to prevent toxic combination

- Toxic combinations should never be granted to any individual
- It should be split apart and two separate individuals should have to coordinate action to achieve the concerned task
- Where ever applicable this should operate on a role basis as well as individual access based i.e. this principle should be adhered to when defining the roles in an application and also at the time when granting accesses to individuals

c. Responsibility matrix for prevention of toxic combination

- Identification of toxic combination of roles will be done by the concerned business team of the application; in case a toxic combination exists across two applications, approval needs to be obtained from business teams (Assistant General Manager or from Leadership team) of both applications. The identified pairs of toxic combination of roles would be documented within LAM, but not as a part of the Access Control Matrix (ACM).
- Technology team will build the control in the LAM application that would contain features for identifying and preventing usage of toxic combination
- Respective business teams would be responsible for a periodic review (at least once a year) or at the time of ACM (Access Control Matrix) review for identification of roles in the application that constitute a toxic combination. Additionally, the Internal Audit team will also perform a review of the same for the applications due for audit as per the application risk assessment approach/plan.

S) Each native IT application in the Bank would have its own customized and specific list of roles. However, the list of roles outlined in Annexure III provides a generic and illustrative list of roles (not restricted to) to serve as a reference point for application teams.

II) Validation to be performed, if applicable: As mentioned in the process

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

i-process memo

5.2 Annexures, if applicable:

Sl No.	Annexure
1	Annexure I : Data captured in Consultant's ID creation request
2.	Annexure II : List of indicative roles and privileges in an IT application

Annexure I

Data captured in Consultant's ID creation request:

First Name
Last Name
Date of birth
Date of Joining
Parent company
Designation at parent company
Type of resource
Resource's reference number (if any memo is available, optional)
Expiry date of the reference number
Employee ID at parent company (if available)
sConsultant's category (profile)
Work location country
Work location state
Work location
Access validity start date
Expected last working date
Type of access
Mail access required
Domain of the reporting ownership manager
Reporting manager employee id and name
Ownership manager employee id and name
Department
Cost center
Approving authority

Annexure II

Role (indicative)	Description	Privileges
Transaction maker/creator (financial/non-financial)	For creating financial or non-financial transaction	To create financial or non-financial transaction
Transaction verifier/checker (financial/non-financial)	For verifying financial or non-financial transaction	To verify financial or non-financial transaction
IT administrator	IT team or support team	Unrestricted access to entire application including data, masters, code etc.
Super user	Business team	Unrestricted access to application data
Module/functional lead	Lead of the module	Access to specific module of the application
Application owner/lead	Application owner	Access to entire application including data, masters etc.
Auditors/regulators	For audit and regulator	View access to various data and masters of the application
Module specific modify access	User with modify access for a specific module in an application and not entire application	Modify details in a specific module of an application
View access specific modules	User with view access for a specific module in an application and not entire application	View details in a specific module of an application