

# IM & AD Reconciliation SOP

## NOTICE

The information contained in this document is not to be used for any purpose other than the purposes for which this document is furnished by Genpact, nor is this document (in whole or in part) to be reproduced or furnished to third parties or made public without the prior express written permission of Genpact.

## Version Control

Ver. No.	Released On	Type	Owner	Approver	Next review
1.0	22 <sup>nd</sup> May, 2014	Initial version	Asad Ali	Santosh Sri Hari	31 <sup>st</sup> Dec 2014
1.0	31 <sup>st</sup> Dec 2015	Review	Asad Ali	Santosh Sri Hari	30 <sup>th</sup> May 2015
1.0	01 <sup>st</sup> June 2015	Review	Asad Ali	Santosh Sri Hari	31 <sup>st</sup> Dec 2015
1.0	02 <sup>nd</sup> Jan 2016	Review	Asad Ali	Santosh Sri Hari	11 <sup>th</sup> Jun 2016
2.1	11 <sup>th</sup> Jun 2016	Updated	Asad Ali	Santosh Sri Hari	31 <sup>st</sup> Dec 2016
2.2	1 <sup>st</sup> Jan 2017	Updated	Asad Ali	Santosh Sri Hari	31 <sup>st</sup> Dec 2017
2.3	1 <sup>st</sup> Jan 2018	Updated	Vivekanandan PSV	Chandrashekhar Babu L	31 <sup>st</sup> Dec 2018
2.4	1 <sup>st</sup> Jan 2019	Updated	Vivekanandan PSV	Chandrashekhar Babu L	31 <sup>st</sup> Dec 2019
2.5	1 <sup>st</sup> Jan 2020	Updated	Vivekanandan PSV	Chandrashekhar Babu L	31 <sup>st</sup> Dec 2020
2.6	6 <sup>th</sup> Dec 2020	Procedure Updated	Vivekanandan PSV	Amresh Biswas	31 <sup>st</sup> Dec 2020
2.7	1 <sup>st</sup> Jan 2021	Review	Vivekanandan PSV	Amresh Biswas	31 <sup>st</sup> Dec 2021

**Viewership**

IM-SSO team, SMG-Wintel Team

**Table of Contents**

NOTICE .....	1
Version Control .....	1
Viewership .....	2
Abbreviation .....	3
Purpose.....	3
Scope .....	3
Stake Holders .....	3
Definition.....	3
Operating Procedure .....	4
Post - Reconciliation Report Activities.....	11
Metric / Acceptable Limits .....	12
Defect Definition .....	12
Incident Handling Process .....	12
Escalation Matrix .....	12
Exceptions .....	12
Ownership and Responsibilities.....	12
Compliance .....	12
Enforcement.....	12
Changes to Policy .....	12
Frequency of Review .....	12

**Abbreviation**

NA

**Purpose**

- ✓ To rule out the inconsistencies that may exist on AD resources when compared with the IDs present in IDM.
- ✓ To assure that IDs which are present on AD, comply with the defined regulatory policy at Genpact.
- ✓ For any IDs which are ruled out as “Unmatched”, which means the IDs are present in AD but not in IDM, must be supported with the confirmation to retain or else deleted from the resource.

**Scope**

The scope of this document is to identify and delete/Disable unused, orphan accounts, or ex-employee access accounts

**Stake Holders**

The information presented in this document is for Genpact & IM-SSO Team.

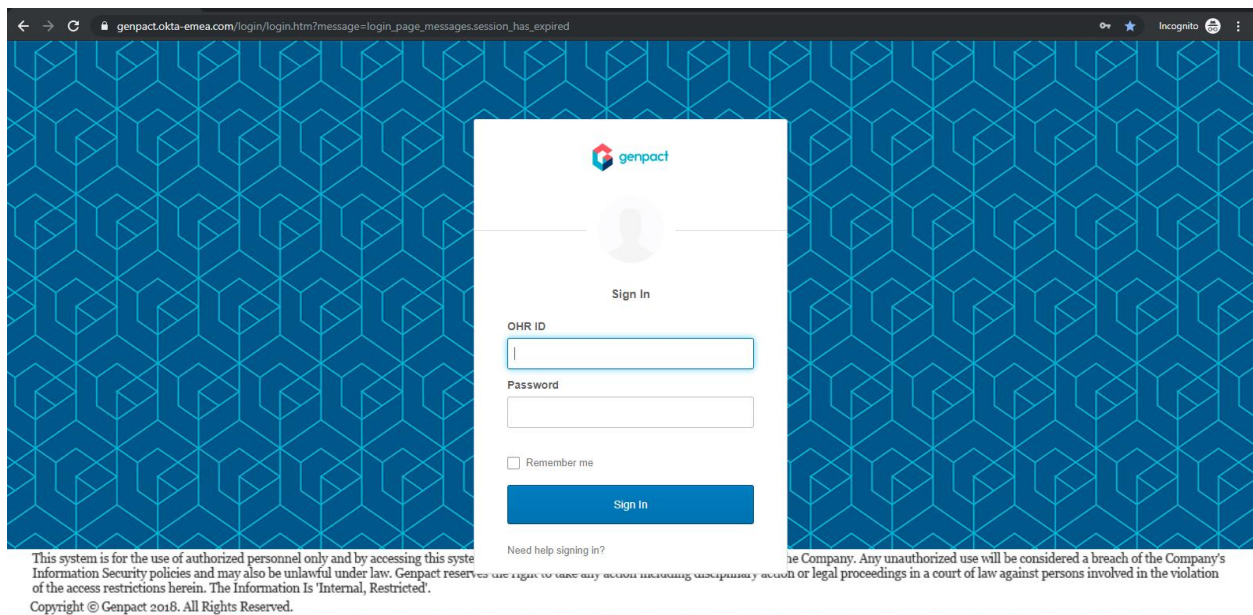
**Definition**

This is in-lieu of the process of reconciliation of Employee Accounts in Genpact. Importance of the process is to prevent the misuse of Access Accounts in Genpact Environment. The Goal is to maintain compliance of all Genpact Employees created Accounts in Identity Management and in AD Resource.

## Operating Procedure

**IM & AD Resource Reconciliation process steps are:-**

**Step:1** Enter the Okta URL (<https://genpact.okta-emea.com/>) in the browser (IE is recommended)



**2. Log in with OHR ID & Password in Okta.**

← → genpact.okta-emea.com/login/login.htm?message=login\_page\_messages.session\_has\_expired Incognito

genpact

Sign In

OHR ID

Password

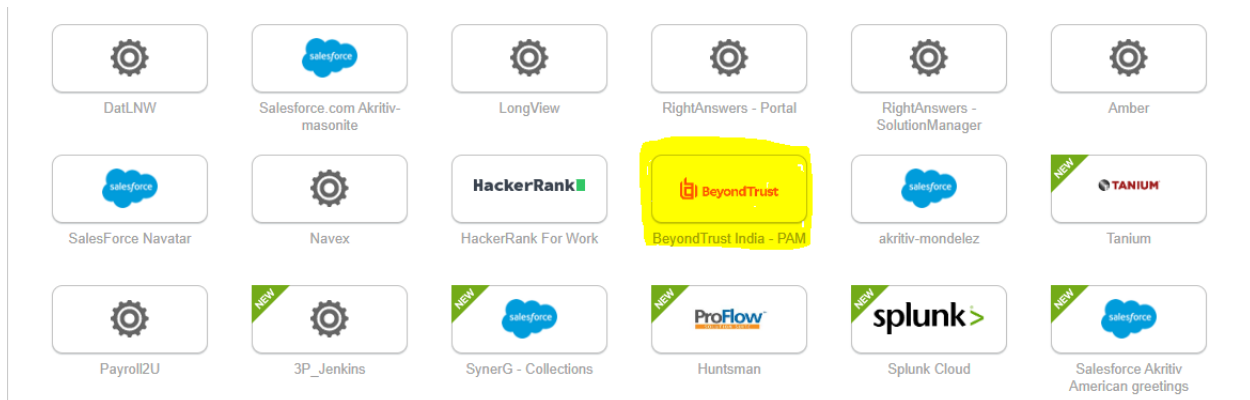
☐ Remember me

Sign In

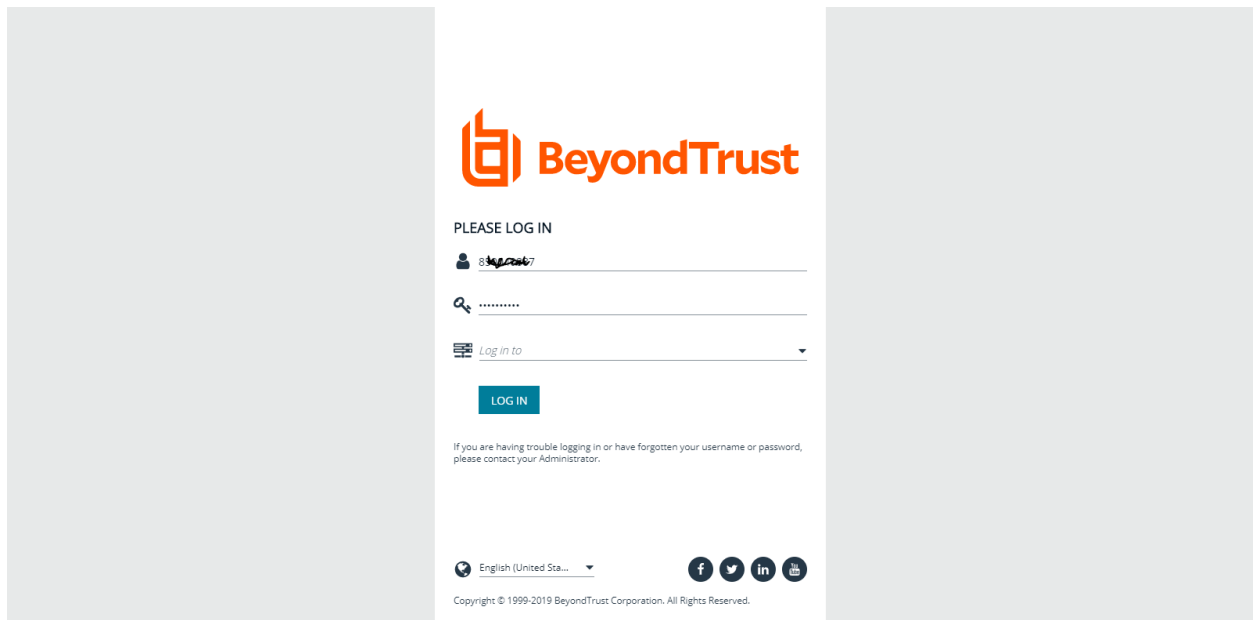
Need help signing in?

This system is for the use of authorized personnel only and by accessing this system you agree to the terms of the Information Security policies and may also be unlawful under law. Genpact reserves the right to take any action including disciplinary action or legal proceedings in a court of law against persons involved in the violation of the access restrictions herein. The Information Is 'Internal, Restricted'. Copyright © Genpact 2018. All Rights Reserved.

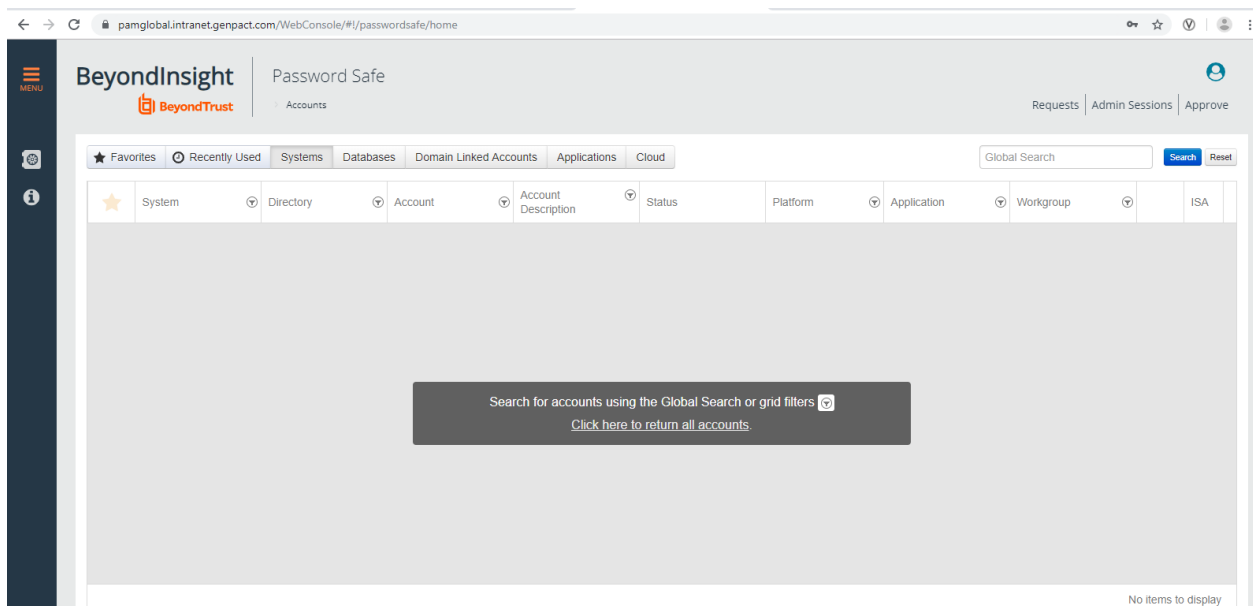
3. After successful login to Okta, add BeyondTrust India app from Genpact Apps and click on the tile as shown below



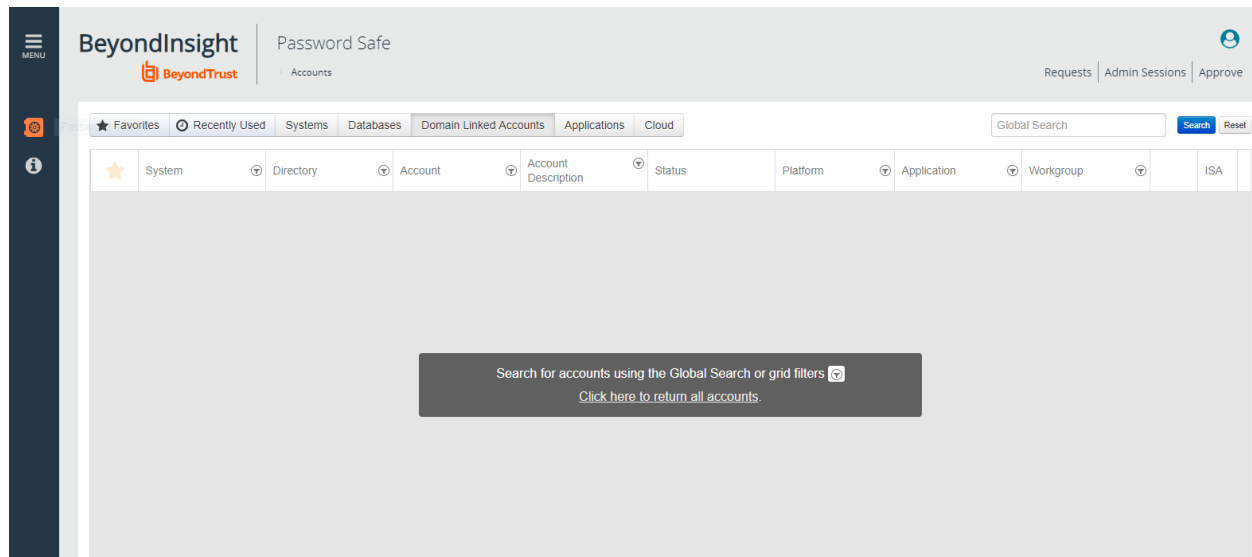
4. Upon clicking on the BeyondTrust India, user will be redirected to PAM (BeyondTrust) web portal:



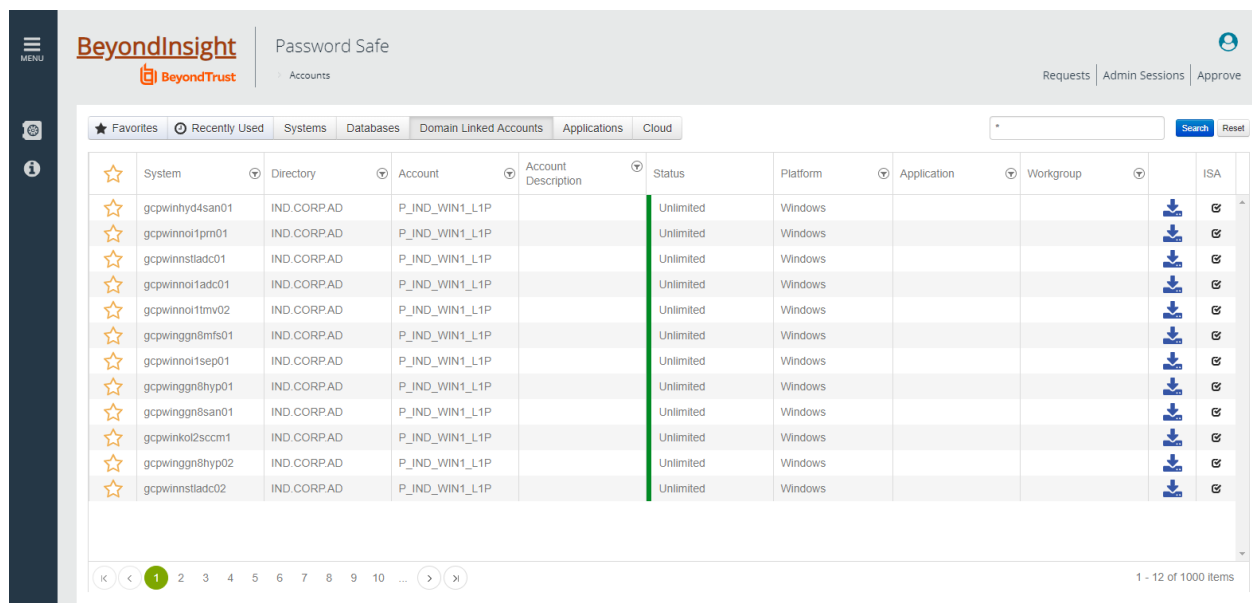
6. After successful logging in to BT, Favorites tab will be displayed by default and user would be able to access other required tabs.



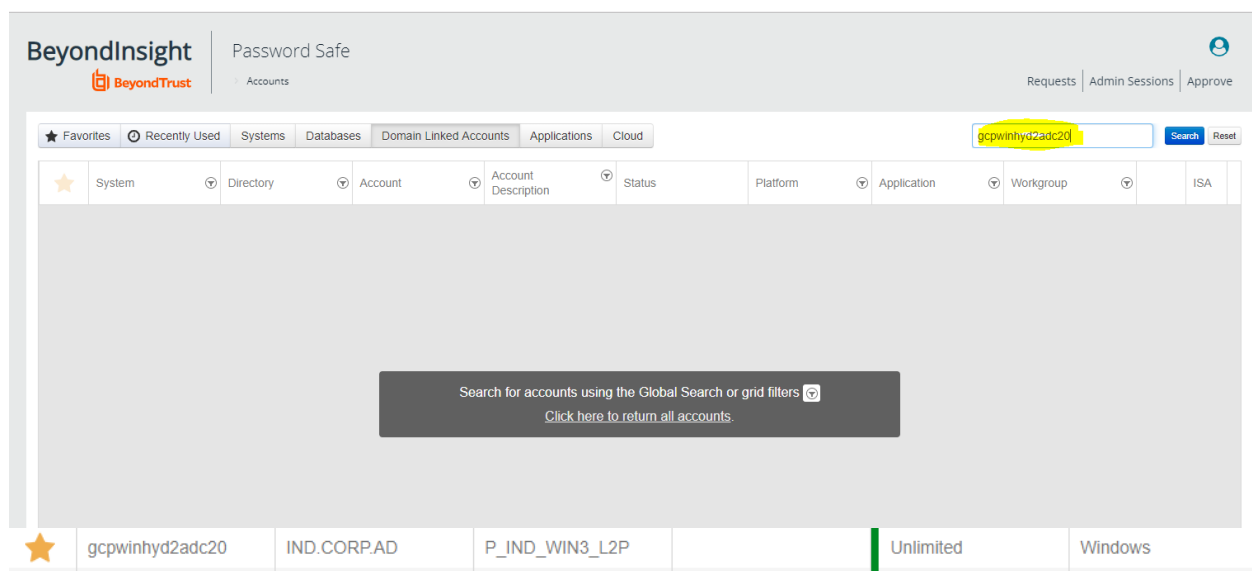
6. Click on Domain Linked Accounts as devices like Windows, Network which are accessed using domain credentials will be shown here



7. Click on Click here to return all accounts to view all the available servers & devices mapped with various managed accounts



8. Particular devices&servers can be searched using Search field given in top-right area. \* will indicate all devices:(gcpwinhyd2adc20)



**Step: 1**– Fetching AD dump from the root DC [119.43.85.23].

a) Batch file **AD\_DUMP\_DWNLDR.bat** is prepared and placed at

**C:\AD\_DUMP\_CORP**

on the respective servers which fetches and prepares the CORP AD dump containing all OHRs present in AD.

119.43.85.23- C:\AD\_DUMP\_CORP

I

**Step 2**:- bring that .csv file on your local machine and remove the first column, named as “**DN**”. Now the .csv file should contain only one column “**sAMAccountName**” and save.

**Step 3**:- Remove first row from the file, which has the value “sAMAccountName”, and save.

**Step 4**:- Now sort and remove the **duplicate values** and remove last line from the file if it is blank, from the .csv file prepared in previous step and save.

**Step 5**:- Initiate a putty session on **58.2.47.194** (gcpsinggn3idm02) through PAM and go to **/export/home/JAVA\_Prog/IMSSO\_Utils/ReconCode** and upload the .csv file prepared in **Step 4**.



Account: P\_IND\_LIN2\_L2P on iamdashboard

Reason: AD Recon

Ticket System: (None)

Ticket Number:

Retrieve Password Open SSH Session Cancel

Record Session ☒

By creating file through “vi 20191205\_CORPDUMP” and paste the data on the file.

**Step 6:-** After uploading the .csv, open **reconexportOJDBC.inf** as shown below and import the path.

```

root@GCPLINGN3IDM02:/export/home/JAVA_Prog/IMSSO_Utils
[root@GCPLINGN3IDM02 IMSSO_Utils]#
[root@GCPLINGN3IDM02 IMSSO_Utils]#
[root@GCPLINGN3IDM02 IMSSO_Utils]# pwd
/export/home/JAVA_Prog/IMSSO_Utils
[root@GCPLINGN3IDM02 IMSSO_Utils]# more reconexportOJDBC.inf
export CLASSPATH=./export/home/JAVA_Prog/IMSSO_Utils/ojdbc6.jar
export PATH=/usr/sbin:/usr/bin:/usr/local/bin:/usr/local/sbin:/export/home/JAVA_Prog/IMSSO_Utils/ojdbc6.jar
[root@GCPLINGN3IDM02 IMSSO_Utils]#
[root@GCPLINGN3IDM02 IMSSO_Utils]#
[root@GCPLINGN3IDM02 IMSSO_Utils]#
[root@GCPLINGN3IDM02 IMSSO_Utils]#
[root@GCPLINGN3IDM02 IMSSO_Utils]#
[root@GCPLINGN3IDM02 IMSSO_Utils]#
[root@GCPLINGN3IDM02 IMSSO_Utils]#

```

**Step 7:-** Now execute the ADReconer.java as shown below;

```
58.247.189 - PuTTY
bash-3.2# java ADReconer:
```

**Step 8:-** After executing the above mentioned java, system will prompt you to mention the path to the .csv file that was uploaded in previous steps. You may either mention the name of the file (if the file is present on the same path else mention the full path).

```
58.247.189 - PuTTY

Enter path to the list of OHRs fetched from AD 20160929_CORPDUMP.csv

Connected at 182.94.106.169 with OIM DB Repository.

Total OHRs Present in AD : 102896
Total OHRs Present in OIM : 102283
Total OHRs Deleted in OIM : 14680
Total MATCHED : 99682
Total UN-MATCHED : 66
Total NON_IDM_OHR : 3148
Total DIFF_OIM_and_AD : 2601
AD Recon Completed Successfully.
Refer output files for further action.

Time Taken : 28.4 min

You have new mail in /var/mail/root
bash-3.2#
```

**Step 9:-** Once the report is prepared then all the files will be shared with OIM L3 and the list of “**Total\_Unmatched IDs**” will be verified sharing the same with Wintel Team.

**Step 10:-** Once verified by OIM L3, “**Total\_Unmatched IDs**” will be shared with Wintel Team. The team further takes the necessary action, depending upon the approvals received.

Total No of User Ids in IM	Total No of User IDs in AD	Total No of User Ids difference	Total No of User ids deleted from AD	Total No of User ids Retained in AD	Provide approvals for retained IDs

## **Post - Reconciliation Report Activities**

Post completion of the IM-AD recon, 6 files are generated containing the OHRs. Below are the detailed information about these files.

- 1. Total OHRs Present in AD** - This is the count of OHRs present in AD as per the backup of that particular day on which this activity is initiated.
- 2. Total OHRs Present in OIM** - This is the count of OHRs present in OIM irrespective of their status on the date of Recon execution.
- 3. Total Unmatched IDs** - Total Valid OHRs [created via IDM], which are not present in IDM but present in AD. These are the IDs for which the Ex-employee has been received but could not be deleted by the sync.
- 4. Total Matched IDs** - Total valid OHRs [created via IDM], which are present in IDM as well as in AD.
- 5. Total Non-IDM IDs** - Total OHRs which are not created via Identity but do exists on AD.
- 6. Total IDM-AD Difference**- This is the count of OHRs which are present in IDM but have no reference on AD
- 7. Total IDs deleted from IDM** - This is the count of OHRs which have been deleted from IDM. Employees who have left the organization.

Wintel team would share the mail confirmation regarding the same, whether the IDs have been retained or removed from AD as well.

## **Metric / Acceptable Limits**

- IMSSO team releases the list of verified, “Un-matched” IDs and share the same with AD Team within the first week of every month.
- The TaT for the confirmation of any action taken [Disable/Deleted/Approved] from the AD team, should reach to IM-SSO team on or before **25<sup>th</sup> of the same month**.
- In case the closure does not reach to IM-SSO team by the 25<sup>th</sup> of the same month, the team will send **3 reminders till the end of the month**.
- Even after reminders, if no closure received then IMSSO will consider all the “Un-matched IDs” approved and will initiate the recon for the next month, followed by the same follow up and closure process.

## **Defect Definition**

Non adherence to the process will be considered as defect definition.

## **Incident Handling Process**

For all incidents, team will follow the incident handling process (Helpmate System) (Wherever Applicable)

## **Escalation Matrix**

All escalation will follow-up the laid down ITIL escalation matrix.

## **Exceptions**

None

## **Ownership and Responsibilities**

Management informed that the reconciliation will not be marked completed without the approvals from the relevant stakeholders. Instead of follow-up emails, team will escalate/call the ‘Domain Leads’ to ensure a response is obtained from each of the stakeholders. Process/SOP document will be updated to reflect the same.

## **Compliance**

It is the responsibility of the IMSSO team to adhere to this policy and ensure compliance with the standards setup in this policy.

## **Enforcement**

Management informed that the reconciliation will not be marked completed without the approvals from the relevant stakeholders. Instead of follow-up emails, team will escalate/call the ‘Domain Leads’ to ensure a response is obtained from each of the stakeholders. Process/SOP document will be updated to reflect the same.

## **Frequency of Review**

The policy document needs to be review by the functional leader at least once in a year.