**Highly Privileged Accounts (HPA) Review**

**Standard Operating Procedure (SOP)**

**Process Flow**

Initiate Reviews

Resolve Defects

Collect Data

Report / Documentation

1. PMO to upload all HPA accounts into OIA

2. Initiate entitlement reviews (authorized owner reviews) to review access appropriateness

1. IM Owner removes/alters HP access of any defect / discrepancy identified during review

2. Extract Highly privilege user list and send to Access Management PMO team.

1. Review active user list to ensure all defects are resolved

2. Document test plans and report

1

2

4

5

1. IM team to extract all active accounts in the application/infrastructure.
2. Review the account list to identify all highly privileged accounts.
3. Identify the appropriate “Authorized Approver”\* for every active highly privileged account.
4. Send the entire users list to the Access Management PMO team.

Defects Rollout

1. PMO to download report from OIA

2. Roll out report to IM Owners highlighting defects

3

\*Authorized Approver (AA): Functional Owner, IM Owner, Module Owner, GE Manager/Sponsor, etc.

Note: IM Owners are responsible to understand and identify the most appropriate “Authorized Approvers” to validate/approve the HP accounts

IM Owner responsibility

AM PMO team responsibility

* **Applications:**
* Any account (personal or non-personal) with:
  + - System Administrator privileges, including but not limited to the following:
* Ability to create/modify/delete users or set/change passwords
* Modify or promote code (production environment)
* Override of application controls that the business relies on
* Change configurable parameters
* the ability to change master data (i.e. customers, vendors, products, prices…) that impact business functions and/or global definitions
* Any additional accounts identified by the application owner and/or functional owner that are considered privileged.
* **Databases:**
* Any account (personal or non-personal) that:
* has database administrative functions (ex: role = DBA… may also include management or monitoring accounts)
* can alter schemas (ex: schema ancillary accounts)
* manages users (ex: can create, modify, delete users; alter privileges or passwords, etc.)
* **OS / Domains:**
* Any account (personal or non-personal) that has privileges to do the following:
* Create, delete, and/or modify users within the system
* Modify permissions for users within the system
* Administrative-level access or other unrestricted access to modify system level settings

**Example:** For **\*nix**, this may include but is not limited to the following:

* Root UID
* Root GID
* PowerBroker group (ex: group 9999)
* ldap sudo role which allows user to sudo to root
* Legacy systems, suroot permission

**Example**: For **Windows**, this may include but is not limited to the following:

* Any member, including members of sub-groups, of the Local Administrators group on the windows server
* Any member, including members of sub-groups, of the Administrators group in each of the domains.

**HPA Review Purpose:**

## Review of users with Highly-privileged account (HPA) access to an IT asset. Review of accounts is performed by authorized approver as determined by the asset owner to determine whether HPA access is required for business purposes. Any access identified as unauthorized is revoked.

**HPA Definition (As per Corporate Standard):**

The account has the ability to make changes to the application that would result in inaccurate or a misrepresentation of data within the application. This includes but is not limited to:

* Ability to change master data (i.e. customers, vendors, products, prices…) that impact business functions and/or global definitions
* System Administrators (e.g. access to all data, access to default/management accounts)
* Creation/modification/deletion of users (may be application specific)
* Override of application controls that the business relies on
* Change configurable parameters in production
* Management accounts - Accounts that comes with the product and are used to manage the application (e.g. administrator, SAP\*)
* Monitoring accounts - Accounts used to monitor the application (normally comes with product installation)
* Any additional accounts identified by the asset owner that are considered privileged
* All non-personal highly privileged accounts

**Process:**

Phase 1 – Active User List Collection:

* PMO works with Application team to obtain the Active User list of all in-scope applications every Quarter.
* A kick off meeting is held for all the Asset owners who are new to the review - to let them know the review process, share proposed timelines, and discuss on the evidences required to initiate the review process.
* Workflows are designed in Support Central for this activity that comprises the process steps in detail for each stage and is initially kicked off to start the review. AM PMO send the workflows to the Asset Owners and identified delegates to submit back with Fresh active user list extracted along with screenshot evidences.
* Application team to extract all highly privileged role based active user list along with screenshot evidences from the Application/Server/Database with appropriate authorized owner information.

Phase 2 – Account certification through OIA

* PMO to upload all HPA accounts in OIA (Access Certifier Tool) and initiate Data Owner review (authorized owner review).
* Authorized owner to review privileged user for access appropriateness and submit responses through the Access Certifier Tool.

Phase 3 – Defect Remediation

* PMO to download report from OIA and roll-out to Application team.
* Asset Owner removes/alters HP access of any defect / discrepancy identified during review and submits complete role based active users list along with screen shot evidences from the Application/Server/Database.
* PMO to validate all identified defects are removed with the Fresh User list and screenshot evidences.
* PMO to document/report test plan.

**HPA Activities**

* **Scope Finalization**:
* Based on our previous quarter review we finalize the scope once we receive the scope file from the client
* Check for the Asset owner and additional contact details
* Check for the activeness of the asset
* Check whether the application was marked as out of scope or NO HPA users, if so then we are excluding that application from the review.
* **Upload Sheet Creation**:
* Once the scope is finalized we upload the list of application with all other data into the support central to kick off the review.
* Requester SSO should be the PMO assigned person to that application
* Asset Id to Asset type get the information from the scope file.
* Audit year should be Quarter + Year (Ex: Q1 2017)
* Access Management Team contacts - SSO separated by comma and space – who ever needs access to the workflow their SSO should be given here
* Due Date – Review due date common to all type of reviews.
* Baseline Annual(\*), HPA(\*), IT SOD - Quarterly(\*), CBI - Quarterly(\*), HPA ERP – which ever review is applicable in that particular column give it as Yes or else No
* Applicable Review – need to mention the type of reviews applicable for the Asset (Ex: HPA, CBI)

Attached is the sample upload data



Attached is the document showing how to upload the data sheet to the support central workflow



**Collection of Data**

* **Score Card preparation:**
* Based on the scope file we prepare the score card which includes:
* **Application Information** - Application Name, Asset owner details, category, type etc..,
* **ACTIVE USER LIST COLLECTION** – gives the information about the workflow status and user list and initial documentation.
* **OIA KICK OFF** – for the application for which AUL is complete we create the master sheet and kick off the review through OIA – this gives the information about the accounts count and the number of applications for which OIA kickoff is complete.
* **DEFECT REMEDIATION** – After the OIA review is complete, based on the BI report we create the review report and for which applications defect is present we send that application for defects removal to the asset owner. – This gives the information about for which application the defects are rolled out , remediated and the final documentation status.

Attached is the sample score card



**User List check list**

* Once we receive the user list from the application team through workflow we need to review the user list
* There should be a user list and screen shot evidence in the required format
* **User List :**
* Application or Asset Name
* User SSO – valid 9 digit SSO ID
* User ID/Account Name – this is optional
* HPA Role – The HPA role that particular account owns.
* Authorized Owner – 9 digit SSO (manager, IM owner, who can authorize the User) – The User SSO and authorize owner SSO cannot be same.
* **Screen shot evidence:**
* Application Name or the production instance from where the list is extracted.

**Initialization of the review**

* **Master Sheet preparation**
  + This is one of the most important step in the review. Once the user list collection is complete, we need to consolidate the data for all the application. Master sheet consist of all the information that is provided by the application team and necessary details required to perform the OIA review.
  + The following are the columns which is required to be present in the master sheet.(Kindly use the same format since we are using an automated tool to generate the csv files, these names should be same as below).
* Category: To which category the particular application belongs.eg.: SoX, FISMA..
* AccountType: SSO or Non-SSO
* OIAFileName: This is the resource type which we have given while creating the resource in OIA.
* OIAReferenceName: This is application name and it should be same as in OIA
* SSO: User SSO(9 digit)
* User Person Type: This is obtained from bulk.
* AccountName: NT id if present or else please user the user SSO
* RoleName: HPA Role
* HPA: Y
* RoleDescription(Optional): Role description if given or else please give the HPA role
* AuthorizedOwner: 9 digit SSO
* AuthorizedOwner Person Type: took it from Bulk
* Account status: Active or Inactive
* accountCreateDate: blank.
* **Check list for Master Sheet:**
* There should not be any blanks in the above mentioned columns.
* User SSO and authorized owner SSO should not be same.
* Concatenate user SSO with role there should not be any duplicates.
* Concatenate account id with role there should not be any duplicates.
* One role should have only one authorized approver, if there are more then concatenate role with user SSO and make the role unique.
* Same account id should not be there more different user SSO, please change the account id to user SSO.
* If account type is officer please exclude those accounts from the review.
* If authorize owner is officer then need to check that it is all properly delegated.
* If authorize owner is inactive then please contact the application team and get the present authorized owner information.

Please refer below is the tool used to review the role based master sheet.

[**URL:http://libraries.ge.com/download?fileid=866876791101&entity\_id=64384259101&sid=101**](http://libraries.ge.com/download?fileid=866876791101&entity_id=64384259101&sid=101)

* **CSV file generation 1**
  + Manually:
* Accounts File: This file contains the user information. Please copy and paste the below mentioned columns from the master sheet. There is no change in the information.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Category | Accounts Type | ServiceNow CI | OIA reference name | SSO | Account Name | Role Name | HPA | accountType | accountCreateDate |

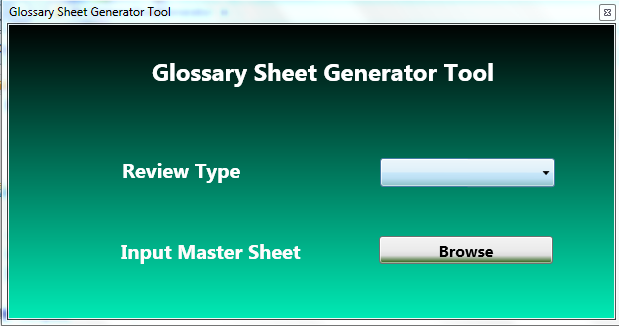
* Glossary File: This file contains the information about the authorize owner. The common value between these two files is HPA role. Based on the roles the mapping is done in OIA.

Copy the role and authorized information for each of the application and remove duplicates. Then fill the remaining information in the file.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Category | ServiceNow CI | OIA reference name | Role | Role Name | Owner | classification | Role Definition | comments |

* + Automated Tool:

Glossary file Generation: [**http://libraries.ge.com/download?fileid=824875843101&entity\_id=64384259101&sid=101**](http://libraries.ge.com/download?fileid=824875843101&entity_id=64384259101&sid=101)

****

The above tool is used to get the accounts and glossary files. Select the review type as GE Aviation-HPA. The Input master file should be saved as “GE Aviation-HPA” and upload the master file. The output file will be saved in the same location.

* **CSV file generation 2**

Once the account and glossary files are ready. We need to convert it to .csv files with different application names.

* + **Manually:**

Download Import Template from ACT tool and save as .csv file and fill all the mandatory fields from the respective accounts and glossary

* + **Automated Tool:**

**CSV generator Tool:** [**http://libraries.ge.com/download?fileid=824877873101&entity\_id=64384259101&sid=101**](http://libraries.ge.com/download?fileid=824877873101&entity_id=64384259101&sid=101)



The above tool is used to get the csv files for each of the applications separately. We can the same output file which we obtained from Glossary file generator or the files created manually. Select the review type as GE Aviation-HPA. The Input file should be saved as “GE Aviation-HPA” and upload the file. The output excels will be saved in the same location along with the summary sheet**.**

* **OIA KICK OFF :**
  + Upload the account and glossary files with respect to the application names.
  + OIA Score card:
* Once we upload the files we will receive and automated email to the custom DL which we have given while creating the resource.
* Please take the success and terminated count.
* Take the OIA count from the tool.
* The OIA count and success count should be same then only we can proceed with the review.
* Once we kick off the data owner review through OIA, please download the Workflow History Report and match the subtract (OIA accounts CSV file # - Term#) with WF count. If there is any mismatch then please find out for which accounts the review is not initiated, raise RITM ticket and recreate the cert6ification for the missed accounts.
* Please refer to the below documents to upload the csv files and to create the certification:

Resource Creation in OIA:



Creating Certification:



Download BI Report:



**Defects Remediation**

* **Defects Roll Out:**
* Once the OIA review is complete and all the certifications are expired we need to roll out the defects to the application owner and get them remediated.
* **Review Report:**

This report contains all information about the accounts similar to the master sheet along with the reviewer response.

* Download the BI report.
* Concatenate OIA Reference name (application name)+User SSO+HPA Role in the review report and in BI report.
* Apply “Vlook up” for this column and get the reviewer response.
* Get the account status from the idm Bulk data.
* If any certified accounts are inactive please change it to the INACTIVE and ask the application owner to remove those accounts.

Please find attached below is the sample Defect Remediation Review Report:



* **Resolve Defects:**
* Roll out the defects report along with the counts to the application owner using the workflow and get the updated user list along with the screen shot evidence.
* Review the list and check that all the defects are removed and save the document as final user list.



**Report / Documentation**

* **Test Plan:**

This document contains all information on the review.

* List of scoped applications
* Summary on the accounts count
* Summary on the certified and defects counts
* Initial and final user list documents
* Review Report and Defects report
* Email approvals(Any)

Attached is the sample test plan:

****

**Access Reviews Execution Method**

Report &  
Document

Defect Remediation

Activities

Collect Data

Initiate Reviews

Defects Rollout

Access   
Appropriateness   
Reviews

Document   
Test results

Highly Privileged   
Accounts (HPA)   
Reviews (Quarterly)

Remove appropriate  
 access for defects  
 identified

Download   
Certification report   
from OIA & roll out

Authorized Owners   
to review HPA &   
Certify thru OIA

Upload HPA in   
OIA & trigger   
Certifications

ALL active HPA   
with authorized   
owner info

PMO Team

IM Owner Responsibility