# Access Review – HPA Procedure for Asset Owners

**Purpose:**  Certify all HPA owners are authorized to access in-scope applications.

**Scope:**  Accounts with System level administrative access, account creation, management access or administrator accounts (access to databases, can change master data). [Detailed definitions](#_HPA_Definitions)

**Procedure:**

AUL - Extract a list of all in-scope accounts

Notification - You will receive an email from the Access Review Workflow.

Extract the requested, in-scope user list and paste your data into the [**User list extraction template**](http://libraries.ge.com/download?fileid=865796254101&entity_id=66080671101&sid=101)

Or create a procedure for extracting a real-time HPA active user list in same format as the template:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **App Name** As recorded in ServiceNow | **Account ID**  SSO/NT/ non-SSO that identifies the account in the system | **User SSO** for shared accounts – all user SSOs  for non-personal accounts – the owner SSO | **Role** Associated with the account | **Role Description (OPTIONAL)** Role to be approved by the authorized owner | **Authorized Approver (SSO only)** Person familiar with the privileges granted with the role and authorized to certify access appropriateness |
| CTD | a21249t | 210007129 | SYSADMIN | GE Engine System Admin | 210058316 |
| CTD | nite7it | 501699379 | SYSADMIN | GE Engine System Admin | 210007129 |
| CTD | nite7it | 501699379 | EASYSADMIN | Engine Alliance System Admin | 210007129 |

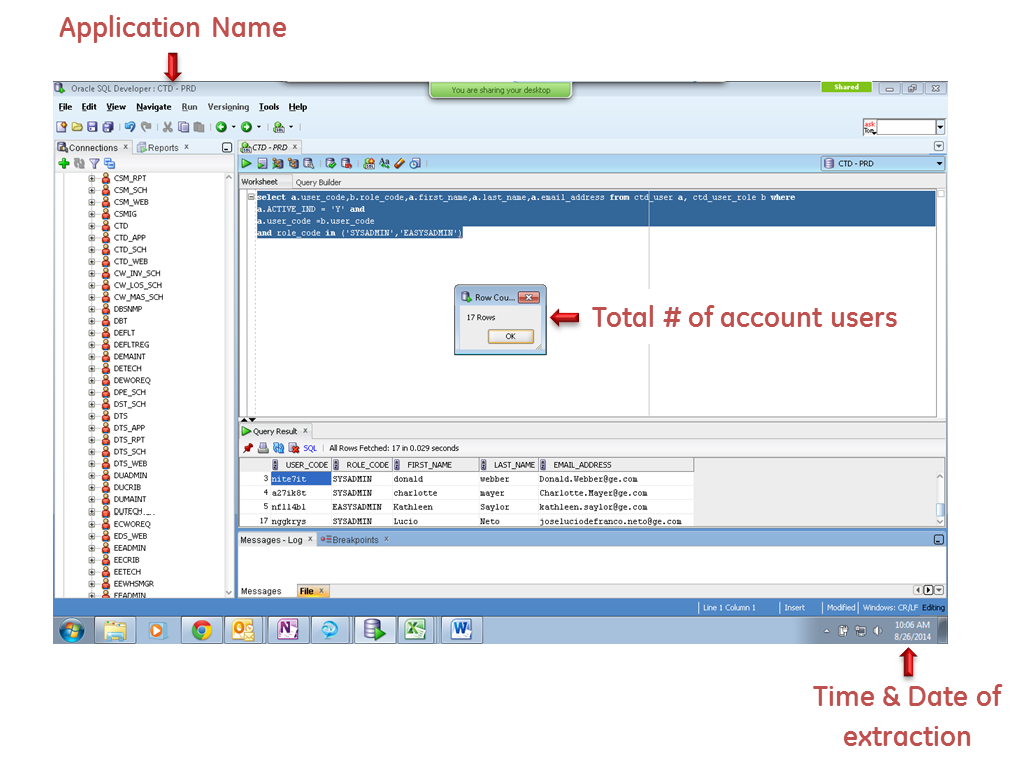
Identify an appropriate Authorized Approver for each account

An appropriate Authorized Approver can be a Functional Owner, IM Owner, Module Owner, GE Manager/Sponsor, etc

Capture screen shots to document your extraction procedure

Include in screen shots:

* Application Name
* Number of records
* Time and date



Defect Remediation – Submit your defect-free HPA active user list

Notification - You will receive a notification email from the Access Review Workflow

**When the Access Review workflow is returned to you, a Defect Review Report will be attached** identifying the accounts that have not been approved by the Authorized Approver.

Follow the instructions indicated in the Defect Report to disable unauthorized accounts:

* Inactive
* Revoked
* No Response from Manager
* OIA Review not Performed

**After remediating all defects**, generate a revised HPA active user list. Attach the revised list and resubmit the Access Review Workflow.

## HPA Definitions

**Application HPAs**

**HPAs** have an elevated level of access:

* Can perform System-level administrative functions:
  + Can override application controls,
  + Can modify or promote code
  + Can change configurable parameters in production,
  + Can manage/monitor the application
* Account creation or management privileges or password management privileges.
* Account administration - can change master data

**Database HPAs**

**HPAs** have an elevated level of access:

* Can perform System-level administrative functions
* Can manage/monitor accounts/privileges/passwords
* Can alter schemas

**OS / Domain HPAs**

**HPAs** have an elevated level of access:

* Can perform System-level administrative functions
* Can create, modify, delete users
* Can modify permissions
* Can modify systems