FUJ00232848

Document Title:	REFINEMENT OF ACCESS RIGHTS TO ORACLE DATABASES
Document Reference:	ARC/SOL/PSD/4429
CP/CWO Reference:	CP2831
Abstract:	Design document covering Oracle database audit enhancements for support user activities.
Document Status:	APPROVED
Author & Dept:	Gareth Seemungal
External Distribution:	(Specify those individuals outside of the Post Office Account who require approved version only. For POA Document Management to distribute following approval)
Information Classification:	See section 0.9

Approval Authorities:

Name	Role	
Torstein Godeseth	Chief Architect	See Dimensions for record
		See Dimensions for record

FUJ00232848

0 Document Control

0.1 Table of Contents

FUJ00232848

FUJ00232848

0.2 Document History

Only integer versions are authorised for development.

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change CWO, CP, CCN or PEAK Reference
0.1	2022-03-10	Initial Version	CP2831
0.2	2022-03-16	Specifically removed BRDB from scope. Added SELECT as an option for auditing. Added HousekeepOrafiles.sh	
0.3	2022-03-29	Updates due to review comments	
1.0	2022-03-31	Approved	

0.3 Review Details

Review Comments by:	29th March 2022
Review Comments to:	Gareth.seemungal@ GRO + POA Document Management

Mandatory Review	
Role	**Name**
Host Architecture	Pete Jobson*
Service Architecture Manager	Alex Kemp
Security Architect	Dave Haywood
Network Architect	Ravi Saini
Fujitsu Requirements Management	Steve Evans; Phil Moss
Architect	Jon Hulme*
SSC Manager	Adam Woodley; sscdm@ GRO
UK PODG Bridge Team Lead	Susan Brindley
Network Operations Manager	Chris Harrison
Service Architect	Phil Boardman*
Senior Service Delivery Manager	Steve Bansal
Management Consultant & CISO	Steven Browell*

Optional Review	
Role	**Name**
CTO	Simon Wilson
Host Bridge Team Lead	Gyan Patel
Data Centre Development Manager	Ajit Mohapatro
Project Management	Abi Loveday
Host Team	Akshyakumar Nahak
Host Team	Mandakini Nayak
Chief Architect	Torstein Godeseth
Test Delivery Manager	Joan Duhaney; Mark Ascott; Trevor Leahy
Information Security Manager	Geoff Baker

FUJ00232848

POA UK Application Delivery Lead	Tariq Arain
Head of Post Office Account Application Transformational Service Centre	Graham Allen
Lead Hosting Architect	Ed Ashford
System Management Group	John Bradley
Oracle DBA	Stuart Johnston
Oracle DBA	Niall McKeefry
Solution Design Architect, Crypto, Web Svcs	Stuart Honey
Security Operations Team	CSPOA.Security GRO
Release Management and Operational Change Manager	Matt Swain
Chief Architect	Torstein Godeseth
Business Continuity	Sidharth Kumar
Network Operations Manager	Chris Harrison
Systems Management, Integration & SCM Manager	Jerry Acton
Infrastructure Operations Manager	Andrew Hemingway
Solution Design / Development	Pavan Vejendla

(*) = Reviewers that returned comments

Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	**Name**

0.4 Associated Documents (Internal & External)

References should normally refer to the latest approved version in Dimensions; only refer to a specific version if necessary.

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 *(DO NOT REMOVE)*	See note above	See note above	POA Generic Document Template	Dimensions
PGM/DCM/ION/0001 *(DO NOT REMOVE)*			POA Document Reviewers/Approvers Role Matrix	Dimensions
SVM/SEC/POL/0003			POA Information Security Policy	Dimensions
SVM/SEC/POL/0005			Community Information Security Policy (CISP) for Horizon	Dimensions
ARC/SEC/ARC/0003			Technical Security Architecture	Dimensions
SVM/SEC/MAN/0003			Information Security Management System (ISMS) Manual	Dimensions
DES/GEN/TEM/2227			Information Technology Health Check (ITHC) Template	Dimensions
DES/APP/HLD/0020			Branch Database High Level Design	Dimensions
DES/APP/HLD/0023			Branch Support Database High Level Design	Dimensions

0.5 Abbreviations

FUJ00232848

Abbreviation	Definition
APOP	Automated Pay Out Pay
BRDB	Branch Database
BRSS	Branch Support Database
DRS	Data Reconciliation Service
NPS	Network Persistence Service
RDDS	Reference Data Distribution Service
RDMC	Reference Data Management Centre
SSC	Software Support Centre
TES	Transaction Enquiry Service

0.6 Glossary

Term	Definition
Alphabetical order please	

0.7 Changes Expected

Changes

0.8 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, while every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.9 Information Classification

The author has assessed the information in this document for risk of disclosure and has assigned an information classification of FUJITSU RESTRICTED(COMMERCIAL IN CONFIDENCE).

FUJ00232848

1 Scope

This document is produced under CP2831.

This document provides a view of the changes necessary to satisfy the auditability and traceability requirements around support user access and activities when connected to HNG-X Oracle databases. These changes attempt to bring a common approach to auditing across the various Oracle databases.

Support users include the SSC as well as Unix and DBA users.

1.1 Purpose of Document

This document intends to specify the changes necessary to both the HNG-X Oracle databases and supporting scripts that create new support users.

1.2 Target Audience for this Document

This document is intended to be read by

- Host Development
- Host Architecture
- 3rd Line Support (SSC)
- 1st Line Support (Unix & DBAs)
- Test
- Service

FUJ00232848

2 Security and Data Privacy

2.1 Check List

Table 2, below, lists the security related areas that have been considered in this design / solution. Refer to the sections below for impact / assessment details.

Area	Relevant (Y/N)?
Assets	
New (Devices etc)	N
Changed (Devices etc)	N
Data Classification	N
Risks	
Risks documented across all areas	Y
Confidentiality	
Protection of information	N
Integrity	
IT Security Health Check (ITSHC) required	N
Anti-Virus / Anti-Malware protection required	N
Protection from (un)intentional change	N
Risks documented	Y
Availability	
Access available to systems / users	Y
Denial Of Service (DoS)	N
Resilience	N
Performance / Sizing	Y
Supportability / Service Life	N
Updates / Patching	N
Monitoring	N
Legal / Contractual / Compliance	
Change of commercial terms – Contractually Controlled Document (CCD) / Contract Reference Document (CRD) / Contract Terms (CT)	N
Change to Operational Level Agreements (OLA) with other parts of Fujitsu	N
Change to OLA with 3rd parties – Non disclosure etc	N
Does this change affect people, technology, physical locations, procedures or 3rd Parties in the scope of: • ISO 27001 • Link • Payment Card Industry Data Security Standards (PCI DSS) • Data Protection Act (DPA) • POA contracts • Fujitsu Intellectual Property Rights (IPR)	 N N N N N N

Table 2 Security – Checklist

2.2 Security Profile

FUJ00232848

2.1.1 Risks

Number	Risk	Owner	Probability	Impact	Action
R001	Support staff lose ability to carry out authorised data changes due to flawed implementation	Fujitsu	Low	High	Prove solution within each environment, ensuring LST signoff remains as a gate prior to Live implementation. Ensure Unix and SSC are involved or at least consulted during testing of the solution.
R002	Support staff activities produce large amounts of audit, resulting in the audit tablespace filling up. This would stop support staff from logging in.	Fujitsu	Low	High	The Operational DBAs must ensure the audit tablespaces are never below an agreed freespace level (currently alerts are configured to appear at <= 10% free space)

Table 4 Security – Risks

FUJ00232848

3 Overview of Changes

This section provides a high level summary of

- the changes that will be common across all impacted databases
- the changes specific to each database

3.1 Common

The following databases fall under this category

1. APOP
2. BRSS
3. DRS
4. NPS
5. RDDS
6. RDMC
7. TES

3.1.1 Enable Database Audit & Extended Audit

Each database should have extended audit enabled. We should assume this change will require database instance restarts.

3.1.2 Roles

The following section identifies various roles which are created or removed (as directed) within each database. Where the role already exists then the role should be aligned with the design specified within this document. Each role's privileges are defined within the solution detailed design section (4 Solution Design).

- SSC_RW created
- SSC created
- APP_SUP removed
- CFM_DBA removed
- APPSUP removed

3.1.3 User Maintenance Script "create_db_user.sh"

Script create_db_user.sh should be altered to automatically grant the SSC role as default and the SSC_RW role as not default to newly created 3rd Line Support users.

In addition, the script shall include directives to force the new user's activities to be audited including logon, DML activities on database tables and execution of any stored procedures.

Note this script is delivered to Belfast Oracle servers via the UNIX_SUPPORT_UTILS_V2 design part.

3.1.4 Oracle Housekeeping Script "HousekeepOrafiles.sh"

Update this Oracle file housekeeping script to move audit files produced under oracle directory "audit_file_dest" to the application's audit directory.

FUJ00232848

3.1.5 Existing Support User Realignment

3.1.5.1 Existing Support Users

Existing database support users will have their update/insert/delete SQL statements, executed procedures and their logins audited by default.

SecOps will ensure that the User Access Database and JML forms are updated to reflect these new role clarifications.

3.1.5.2 Existing 3rd Line Support Users

Users identified as being SSC (also 3rd Line Support) within the databases (at the time of this solution's deployment) will have the following actions applied (in addition to those identified in 3.1.4.1)

Action	Action
Grant SSC role	Grant the SSC role to each user. This role shall be a default role (i.e. enabled at logon)
Grant SSC_RW role	Grant the SSC_RW role to each user. This role shall not be a default role and must be set when the support user requires escalated read/write privileges within the relevant database

3.1.6 Ensure SYS Auditing is Enabled

Ensure database parameter audit_sys_operations is set to TRUE if not already enabled.

3.1.7 Database Table Sizing Considerations

The current live databases currently have ample space for additional audit logging information. The sizing information here is from 2022-03-11.

DB	Tablespace	Used MB	Free MB	Total MB	Pct. Free
APOP	APOP_AUDIT	353	3,647	4,000	91
BRSS	BRSS_AUDIT	3,572	2,428	6,000	40
DRS	DRS_AUDIT	149	2,851	3,000	95
NPS	NPS_AUDIT	51	3,949	4,000	99
RDDS	RDDS_AUDIT	122	1,878	2,000	94
RDMC	RDMC_AUDIT	185	1,815	2,000	91
TES	TES_AUDIT	297	3,703	4,000	93

Design Note for Test: *testing within LST should confirm whether the additional audit logging overhead might result in a much larger impact on storage requirements than currently anticipated.*

FUJ00232848

3.2 Specific Database Requirements

The details around the solution can be found in Section 4 Solution Design.

3.2.1 APOP

3.2.1.1 Roles

The following role shall be removed

- APPSUP

The following roles shall have SELECT privileges granted for the required schemeta

- SSC
- SSC_RW

The following role shall have UPDATE, INSERT, DELETE privileges granted for the required schemeta

- SSC_RW

3.2.2 BRSS

3.2.2.1 Roles

The following role shall be removed

- APPSUP

The following roles shall have SELECT privileges granted for the required schemeta

- SSC
- SSC_RW

The following role shall have UPDATE, INSERT, DELETE privileges granted for the required schemeta

- SSC_RW

3.2.3 DRS

3.2.3.1 Roles

The following role shall be removed

- APPSUP

The following roles shall have SELECT privileges granted for the required schemeta

- SSC
- SSC_RW

The following role shall have UPDATE, INSERT, DELETE privileges granted for the required schemeta

- SSC_RW

FUJ00232848

3.2.4 NPS

3.2.4.1 Roles

The following role shall be removed

- APPSUP

The following roles shall have SELECT privileges granted for the required schemeta

- SSC
- SSC_RW

The following role shall have UPDATE, INSERT, DELETE privileges granted for the required schemeta

- SSC_RW

3.2.5 RDDS

3.2.5.1 Roles

The following role shall be removed

- APPSUP

The following roles shall have SELECT privileges granted for the required schemeta

- SSC
- SSC_RW

The following role shall have UPDATE, INSERT, DELETE privileges granted for the required schemeta

- SSC_RW

3.2.6 RDMC

3.2.6.1 Roles

The following role shall be removed

- APPSUP

The following roles shall have SELECT privileges granted for the required schemeta

- SSC
- SSC_RW

The following role shall have UPDATE, INSERT, DELETE privileges granted for the required schemeta

- SSC_RW

FUJ00232848

3.1.7 TES

3.1.1.1 Roles

The following role shall be removed

- APPSUP

The following roles shall have SELECT privileges granted for the required schemeta

- SSC
- SSC_RW

The following role shall have UPDATE, INSERT, DELETE privileges granted for the required schemeta

- SSC_RW

FUJ00232848

4 Solution Design

This section provides a high level summary of

- the changes that will be common across all impacted databases
- the changes specific to each database

4.1 Common

The following databases fall under this category

- APOP
- BRSS
- DRS
- NPS
- RDDS
- RDMC
- TES

4.1.1 Enable Database Audit & Extended Audit

Enable Extended Audit via the following command

```
alter system set audit_trail='DB','EXTENDED' scope=spfile;
```

Database instances may require a restart to ensure the change is applied.

4.1.2 Roles

The following roles altered as follows. Note some roles may already be present or may not exist, therefore implementation should accommodate this. It is expected that the installation patches should be explicit in reporting pre-existence or non-existence at installation time.

Role	Action	Description
SSC_RW	Create	SSC Read Write role that grants users the following privileges (note these capabilities should be COMBINED with the database specific requirements defined in 4.2) 1. grant select any dictionary
SSC	Create	SSC Read only role that grants users the following privileges (note these capabilities should be COMBINED with the database specific requirements defined in 4.2) 1. grant select any dictionary
APP_SUP	Remove	Where this role exists, please remove from the database
CFM_DBA	Remove	Where this role exists, please remove from the database
APPSUP	Remove	Where this role exists, please remove from the database

FUJ00232848

4.1.3 User Maintenance Script "create_db_user.sh"

Script create_db_user.sh shall be altered to automatically grant the SSC role as default and the SSC_RW role as not default to newly created 3rd Line Support users.

Remove the functionality that provides the ability to grant the APPSUP role.

In addition, the script shall include directives to force the new user's activities to be audited including logon, DML activities on database tables and execution of any stored procedures.

The user should also be granted the ability to logon and create tables/procedures/sequences/triggers within their own schema.

```
AUDIT ALL BY <user> BY ACCESS;
AUDIT SELECT TABLE, UPDATE TABLE, INSERT TABLE, DELETE TABLE BY <user> BY ACCESS;
AUDIT EXECUTE PROCEDURE BY <user> BY ACCESS;
GRANT RESOURCE TO <user>;
GRANT CONNECT TO <user>;
```

Note this script has been delivered to Belfast Oracle servers via the UNIX_SUPPORT_UTILS_V2 design part in the past.

4.1.4 Oracle Housekeeping Script "HousekeepOrafiles.sh"

Update this script for all platforms to move the audit files in the oracle adump location (defined as the ${ADUMP_DEST} variable in this script) to the following locations, depending on the input database (parameter -d).

Database (-d parameter)	Move Files To
APOP	/bvnw01/apop/support/hostaudit
BRDB	/app/brdb/trans/audit/hostaudit
BRSS	/app/brss/trans/audit/hostaudit
DRS	/bvnw01/drs/trans/drsaudit
NPS	/REPL/npsf/trans/npsaudit
RDDS	/bvnw01/rdds/aud$/output
RDMC	/bvnw01/rdmc/aud$/output
TES	/bvnw01/tes/trans/tesaudit

FUJ00232848

4.1.5 Existing Support User Realignment

4.1.5.1 Existing Support Users

Users identified as being SSC as well as Unix and DBA users within the databases (at the time of this solution's deployment) shall have the following actions applied.

Action	Action
Enable User Audit	AUDIT ALL BY <user> BY ACCESS; AUDIT SELECT TABLE, UPDATE TABLE, INSERT TABLE, DELETE TABLE BY <user> BY ACCESS; AUDIT EXECUTE PROCEDURE BY <user> BY ACCESS; GRANT RESOURCE TO <user>; GRANT CONNECT TO <user>;

4.1.5.1.1 Identifying Support Users

```
select distinct username
from (
   select (select name from v$database) as database,
          grantee as username, granted_role as role
   from   dba_role_privs
)
where username not in ('SYS','SYSTEM')
and (
      (database = 'APOP' and role in ('APPSUP','SSC','DB_MONITOR', 'UNXADM'))
   or (database = 'BRSS' and role in ('DB_MONITOR','SSC','UNXADM','APPSUP'))
   or (database = 'DRS' and role in ('APPSUP','APP_SUP','DB_MONITOR','UNXADM') and username
not in 'OPS$DRS')
   or (database = 'NPS' and role in ('APPSUP','DB_MONITOR','UNXADM'))
   or (database = 'RDDS' and role in ('APPSUP','DB_MONITOR','UNXADM','CFM_DBA','MONITOR'))
   or (database = 'RDMC' and role in  ('APPSUP','DB_MONITOR','UNXADM','CFM_DBA','MONITOR'))
   or (database = 'TES' and role in ('APPSUP','DB_MONITOR','UNXADM'))
);
```

Design Note for Host: *I would suggest any prospective patch developer should be aware the above identification method only works prior to roles being reorganised as part of this CP.*

FUJ00232848

4.1.5.2 Existing 3rd Line Support Users (SSC)

Users identified as being SSC (also 3rd Line Support) within the databases (at the time of this solution's deployment) shall have the following actions applied

Action	Action
Grant SSC role	Grant the SSC role to each user. This role shall be a default role (i.e. enabled at logon)
Grant SSC_RW role	Grant the SSC_RW role to each user. This role shall not be a default role and must be set when the support user requires escalated read/write privileges within the relevant database

4.1.5.2.1 Identifying 3rd Line Support Users

```
select distinct username
from (
   select (select name from v$database) as database,
          grantee as username, granted_role as role
   from   dba_role_privs
) users_roles
where username not in ('SYS','SYSTEM')
and (
      (database = 'APOP' and role in ('APPSUP','SSC','DB_MONITOR', 'UNXADM'))
   or (database = 'BRSS' and role in ('DB_MONITOR','SSC','UNXADM','APPSUP'))
   or (database = 'DRS' and role in ('APPSUP','APP_SUP','DB_MONITOR','UNXADM') and username
not in 'OPS$DRS')
   or (database = 'NPS' and role in ('APPSUP','DB_MONITOR','UNXADM'))
   or (database = 'RDDS' and role in ('APPSUP','DB_MONITOR','UNXADM','CFM_DBA','MONITOR'))
   or (database = 'RDMC' and role in  ('APPSUP','DB_MONITOR','UNXADM','CFM_DBA','MONITOR'))
   or (database = 'TES' and role in ('APPSUP','DB_MONITOR','UNXADM'))
)
and not exists (
   select null
   from   dba_role_privs unx
   where  unx.grantee = users_roles.username
   and    unx.granted_role = 'UNXADM'
);
```

Design Note for Host: *I would suggest any prospective patch developer should be aware the above identification method only works prior to roles being reorganised as part of this CP.*

FUJ00232848

4.1.6 Ensure SYS Auditing is Enabled

Ensure database parameter audit_sys_operations is set to TRUE if not already enabled.

FUJ00232848

4.2 Specific Database Requirements

4.2.1 APOP

4.2.1.1 Roles

Carry out the following changes to this specific database

Role	Action	Description
SSC_RW	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant on all tables within schema OPS$APOP 3. Grant UPDATE, DELETE, INSERT on all tables within schema OPS$APOP
SSC	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant SELECT on all tables within schema OPS$APOP

4.2.2 BRSS

4.2.2.1 Roles

Carry out the following changes to this specific database

Role	Action	Description
SSC_RW	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant SELECT on all tables within schemata OPS$BRSS, OPS$BRDB, OPS$OGGADMIN 3. Grant UPDATE, DELETE, INSERT on all tables within schemata OPS$BRSS, OPS$BRDB, OPS$OGGADMIN
SSC	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant SELECT on all tables within schemata OPS$BRSS, OPS$BRDB, OPS$OGGADMIN

FUJ00232848

4.2.3 DRS

4.2.3.1 Roles

Carry out the following changes to this specific database

Role	Action	Description
SSC_RW	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant SELECT on all tables within schema OPS$DRS 3. Grant UPDATE, DELETE, INSERT on all tables within schema OPS$DRS
SSC	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant SELECT on all tables within schema OPS$DRS

4.2.4 NPS

4.2.4.1 Roles

Carry out the following changes to this specific database

Role	Action	Description
SSC_RW	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant SELECT on all tables within schema OPS$NPS 3. Grant UPDATE, DELETE, INSERT on all tables within schema OPS$NPS
SSC	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant SELECT on all tables within schema OPS$NPS

FUJ00232848

4.2.5 RDDS

4.2.5.1 Roles

Carry out the following changes to this specific database

Role	Action	Description
SSC_RW	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant SELECT on all tables within schema OPS$RDDS, RDDS 3. Grant UPDATE, DELETE, INSERT on all tables within schema OPS$RDDS, RDDS
SSC	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant SELECT on all tables within schema OPS$RDDS, RDDS

4.2.6 RDMC

4.2.6.1 Roles

Carry out the following changes to this specific database

Role	Action	Description
SSC_RW	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant SELECT on all tables within schema RDMC 3. Grant UPDATE, DELETE, INSERT on all tables within schema RDMC
SSC	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant SELECT on all tables within schema RDMC

4.2.7 TES

4.2.7.1 Roles

Role	Action	Description
SSC_RW	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant SELECT on all tables within schemata OPSTES, OPSTESREP 3. Grant UPDATE, DELETE, INSERT on all tables within schemata OPSTES, OPSTESREP
SSC	Create	Grant the following privileges: 1. SELECT ANY DICTIONARY 2. Grant SELECT on all tables within schema OPSTES, OPSTESREP

FUJ00232848

4.2.8 Appendix: Application Schemata

The following table identifies which schemata's tables can be SELECTed by the SSC role and SELECTed/UPDATEd/INSERTed/DELETEd by the SSC_RW role

Database	Schema
APOP	OPS$APOP
BRSS	OPS$BRSS
BRSS	OPS$BRDB
BRSS	OPS$OGGADMIN
DRS	OPS$DRS
NPS	OPS$NPS
RDDS	OPS$RDDS
RDDS	RDDS
RDMC	RDMC
TES	OPS$TES
TES	OPS$TESREP