

Control
Version-11.0
9NT1316-ORACLE FCUBSV.UM 11.0.0.0.0.0
[January] [2010]
Oracle Part Number E51712-01



Document Control

Author: Documentation Team	Group: UBPG	
Created on: October 01, 2008	Revision No: Final	
Updated by: Documentation Team	Reviewed by: Development/Testing teams	Approved by: Software Quality Assurance Team
Updated on: January 04, 2010	Reviewed on: January 04, 2010	Approved on: January 04, 2010

Table of Contents

1. OVERVIEW.....	1-1
1.1 INTRODUCTION.....	1-1
1.1.1 Audience.....	1-1
1.1.2 Organization of the document.....	1-1
1.1.3 Glossary of Icons.....	1-1
2. MAINTENANCE OF CONTROLS.....	2-1
2.1 INTRODUCTION.....	2-1
2.1.1 Oracle FLEXCUBE Level.....	2-1
2.1.2 Server (Operating System) Level.....	2-1
2.1.3 Client (workstation) Level.....	2-1
2.1.4 Data Center Controls.....	2-1
2.1.5 Back-up Controls.....	2-2
2.1.6 Software Controls.....	2-2
2.1.7 Fault in Main System.....	2-3
2.1.8 Natural Calamities.....	2-3
3. ORACLE FLEXCUBE CONTROLS.....	3-1
3.1 INTRODUCTION.....	3-1
3.1.1 Audit Trail Report.....	3-1
3.1.2 Security Violation Report.....	3-1
3.1.3 Clear User Profile.....	3-3
3.1.4 Change User Password.....	3-3
3.1.5 List of Logged-in Users.....	3-3
3.1.6 Change Time Level.....	3-3
3.1.7 Server security controls.....	3-3
4. REVIEW PROCEDURE.....	4-1
4.1 INTRODUCTION.....	4-1
4.1.1 Daily Review Procedure.....	4-1
4.1.2 Weekly Review Procedure.....	4-2
4.1.3 Monthly Review Procedure.....	4-3
4.1.4 Quarterly Review Procedure.....	4-3
4.1.5 Annual Review Procedure.....	4-8

1. Overview

1.1 Introduction

This manual describes the recommended control procedure in the day-to-day operation of Oracle FLEXCUBE. The manual also describes in detail, the security and audit- related features of Oracle FLEXCUBE.

1.1.1 Audience

This manual is a guide for the Control personnel. It describes their functions in detail.









1.1.2 Organization of the document











The chapters on Maintenance of Controls and Oracle FLEXCUBE Controls are organized as follows:

- The chapter on Maintenance of Controls deals with the allocation of tasks and functions to groups and individuals in the bank.
- The chapter on Oracle FLEXCUBE Controls describes Oracle FLEXCUBE -based controls
- The third chapter describes Server Security Controls
- The chapter on Review Procedure describes the various reviews to be conducted by the Control Department. The sections of this chapter have been organized according to the frequency of the review procedure i.e., daily, weekly, monthly, quarterly and annual.

1.1.3 Glossary of Icons

This User Manual may refer to all or some of the following icons:

Icons	Function
	New
	Copy
	Save
	Delete
	Unlock
	Print
	Close
	Re-open

	Reverse
	Template
	Roll-over
	Hold
	Authorize
	Liquidate
	Exit
	Sign-off
	Help
	Add
	Delete

Refer the Procedures User Manual for further details about the icons.

2. Maintenance of Controls

2.1 Introduction

This chapter describes the functions and responsibilities of users at the application (Oracle FLEXCUBE) level. It also describes the procedure for maintenance of controls within the organization.

The Data Center Manager is responsible for all the activities of the Data Center.

The various users who access Oracle FLEXCUBE at the following levels are mentioned below:

2.1.1 Oracle FLEXCUBE Level

The Security Officer is designated by the Data Center Manager. He is responsible for the review and investigation of all Protocol and Security Reports.

The System Administrator/Oracle DBA is responsible for the overall Security management of Oracle FLEXCUBE. The Librarian is responsible for maintenance of disks, tapes, operational programs, software and documentation associated with all systems. The Repair Personnel are responsible for hardware repair.

2.1.2 Server (Operating System) Level

Access to Oracle FLEXCUBE should be only through the client. No user needs to have the direct access to Unix server. Control software to be installed in the Server.

2.1.3 Client (workstation) Level

Control software (client-version) to be installed in the Client-Source server. The access to the client machines should be protected with POWER-ON password. The screen-saver password feature of the WINDOWS should also be enabled.

2.1.4 Data Center Controls

You should ensure that the following steps are taken to maintain safety and security in the Data Center:

- There should be a strict control on the people authorized to access the Data Center. A list of the authorized personnel should be put up at the entrance. If possible, a flipcard system can be installed to control entry into the Data Center.
- A log book should be maintained at the entrance to the Data Center. This book should contain the following information on all the people who enter the Data Center:
 - The name of the person
 - The date and time of entry
 - The purpose of entry

- When unauthorized people enter the data center, they should be accompanied by authorized personnel. They should write all the required information in the log book.
- Inflammable material and excessive stationery should not be kept in the Data Center.

2.1.5 Back-up Controls

Back-ups should be taken regularly. This will minimize downtime if there is an emergency. Access to the application areas should not be at the operating system level. On-line archival of redologs should be set up from the date of going live. It is recommended that:

- Backup of all database related files viz., data files, control files, redologs, archived files, init.ora, config.ora etc should be taken at the end of the day.
- The tape can be recycled every week by having day-specific tapes.
- On-line backup of archived redo-log files onto a media to achieve to the point recovery in case of crash, shutdown etc.(recycled every day)
- Complete export of database and softbase should be done atleast once in a week and this can be stored off-site (media can be recycled in odd and even numbers).
- Complete backup of the Oracle directory (excluding the database related files) to be taken once in a month. This media can be recycled bimonthly.
- When the database is huge, incremental exports and on-line tablespace backups are recommended.

The above strategy may be improvised by the Oracle DBA, depending on the local needs. The backup operations are to be logged and tapes to be archived in fireproof storages.

2.1.6 Software Controls

It should be ensured that the latest version of Oracle FLEXCUBE and other recommended third party software exist on the main system.

You should ensure that the off-site area contains a full set of the following:

- The latest version of the application software (Oracle FLEXCUBE - both Client & Server components) and the recommended third party software) and operating system software.
- The export of the database backup of Oracle directory separately on a regular basis to save from reinstallation of Oracle in case of contingencies.
- The documentation of the application software and operating system software.
- The manuals explaining the installation procedure of Oracle FLEXCUBE and other software.
- The manuals explaining the control and system security procedure.
- Oracle DBA and Installation manuals.

A comprehensive fault reporting, fixing, re-testing and reconciliation procedure would be provided in future. POIROT can be used for the purpose of reporting problems.

2.1.6.1 Contingency Planning

It should be ensured that downtime is at a minimum, in the event of an emergency. Good planning is necessary for quick revival of the system. Two types of problems could cause an interruption in data processing activities, as follows:

2.1.7 Fault in Main System

It should be ensured that the following steps are taken, to minimize downtime if there is a fault in the main system:

- The configuration of the back-up machine for both the hardware and the operating system should be similar to that of the main machine.
- The organization of the disk and user profiles in the back-up machine should be similar to that of the main machine.
- When there is a fault in the main system, the database should be restored on the backup machine. These can be obtained from the library. Data processing operations can be carried out on the back-up machine.
- The hardware vendor should be informed about the fault. The system should be brought back into action as soon as possible.
- On rectification of the fault, the data processing operations should be shifted back to the main system. This should be done at the beginning of the next logical day.
- A detailed analysis should be made of the hardware fault and take preventive action to avoid similar problems in the future.
- The problems could be related to ORACLE - Rollback segments to be increased, maximum extents reached for a tablespace etc. Database reorganisation and other related DBA activities to be done by the ORACLE DBA at regular frequencies.

2.1.8 Natural Calamities

It should be ensured that the following steps are taken, to minimize downtime if there is a natural calamity:

- A machine with a configuration that is similar to that of the main system should be maintained at an off-site area. This machine may be acquired on a contractual basis.
- The operating system should be installed in the off-site machine.
- User profiles should be created for the off-site system, similar to those of the main system.

In the event of a natural calamity, the off-site system should be used. The latest database work area, queues area and softbase should be obtained from the library and restored.

3. Oracle FLEXCUBE Controls

3.1 Introduction

This chapter describes the various programs available within Oracle FLEXCUBE, to help in the maintenance of security. The Oracle FLEXCUBE Security Management System offers an exhaustive security environment. Access to the system is possible only if the user logs in with a valid ID and the correct password. The activities of the users can be reviewed by the Security Officer in the Event Log and the Violation Log reports.

The functions in the Oracle FLEXCUBE Security Management System are:

3.1.1 Audit Trail Report

A detailed Audit Trail is maintained by the system on all the activities performed by the user from the moment of login. This audit trail lists all the functions invoked by the user, along with the date and time. The program reports the activities, beginning with the last one. It can be displayed or printed. The records can be optionally purged once a printout is taken. This program should be allotted only to the Security Officer.

Refer Annexure A for a sample of the Protocol Report.

3.1.2 Security Violation Report

This program can be used to display or print the Violation Report. The report gives details of exceptional activities performed by a user during the day. The difference between the Violation Report and the Audit Trail is that the former gives details of all the activities performed by the users during the day, and the latter gives details of exceptional activities, for e.g. forced password change, unsuccessful logins, Auto Sign off, User already logged in, etc. The details given include:

- Time
- The name of the operator
- The name of the function
- The ID of the terminal
- A message giving the reason for the login

The system gives the Security reports a numerical sequence. The Security Report includes the following messages:

3.1.2.1 Password Change messages

Message	Explanation
Forced Password, Change	There is a forced change in the password if it is not altered at the time specified by the system, for example, a user password should be changed when it is a month old. If it is not done, the system will force the user to change the password.
Change of Password	The password has been changed using the Password Change Menu Option.

3.1.2.2 Sign-on messages

Message	Explanation
User Already Logged In	The user has already logged into the system and is attempting a login through a different terminal.
Duplicate Terminal ID	If two clients have the same terminal ID set- up. This prevents improper copying the INI files on the client.
Time Level Restriction	If the User who is attempting to log in has a time level lower than that of the branch.
Sign-on Bad Name	An incorrect ID is entered.
Sign-on Bad Password	An incorrect password is entered.
Sign-on Profile Disabled	There have been three consecutive Bad Password attempts.
Profile Already Disabled	Login is attempted on a disabled profile.

3.1.2.3 Display/Print user profile

This function provides an on-line display / print of user profiles and their access rights. The information includes:

- The type (customer / staff)
- The status of the profile - enabled or disabled or on-hold
- The time of the last login
- The date of the last password /status change
- The number of invalid login attempts
- The language code / home branch of the user

3.1.3 Clear User Profile

A user ID can get locked into the system due to various reasons like an improper logout or a system failure. The Clear User Profile function can be run by another user to reset the status of the user who got locked in. This program should be used carefully and conditionally.

3.1.4 Change User Password

Users can use this function to change their passwords. A user password should contain a minimum of six characters and a maximum of twelve characters (both parameterizable). It should be different from the current and two previous passwords. The program will prompt the user to confirm the new password when the user will have to sign-on again with the new password.

3.1.5 List of Logged-in Users

The user can run this program to see which users are in use within Oracle FLEXCUBE at the time the program is being run. The information includes:

- The ID of the terminal
- The ID of the user
- The login time

3.1.6 Change Time Level

Time levels have to be set for both the system and the users. Ten time levels are available, 0 to 9. Restricted Access can be used to set the Users time level. The Change Time Level function can be used to do the same for the branch. A user will be allowed to sign-on to the system only if his/her time level is equal to or higher than the system time level. This concept is useful because timings for system access for a user can be manipulated by increasing the system time level. For e.g., the End of Day operators could be allotted a time level of 1, and the users could be allotted a time level of 0. If the application time-level is set at 1 during End of Day operations, only the End of Day operators will have access to the application. The other users will be denied access.

3.1.7 Server security controls

Control over ORACLE user passwords - SYSTEM/SYS /SCHEMA_ID etc.

Audit trail to be set on for SYSTEM/SQLDBA/SQLPLUS logins.

Use of roles for giving only SELECT privileges for all users using SQLPLUS.

Protecting SQLDBA., SYSTEM , SYS with passwords under dual control

4. Review Procedure

4.1 Introduction

You are recommended to carry out reviews on a regular basis. This will ensure that the standards of the organization are being met and will bring to light any discrepancy in the operation of Oracle FLEXCUBE. The following sections describe the various reviews to be carried out - daily, weekly, quarterly and annual.

4.1.1 Daily Review Procedure

This section describes the reviews to be carried out on a daily basis.

- Review of Violation Logs
- Review of Audit Report

4.1.1.1 Review of Violation Log

The Security Log and the Violation Log should be made Mandatory EOD reports. This would force the execution and printing of these reports. The reports should be reviewed by the Security Officer to ensure that there is no break in the sequential numbering. Any deviation should be reported to the Data Center Manager and the Head of Operations. The Data Center personnel should keep track of the serial number of this report to ensure that there was no purge of the log done during the day.

In case there are unusual messages in the Security report, the Security Officer should take the following steps:

Message	Action to be taken
Bad Password	If this message appears repetitively, you should enter the USER ID in the Standard Oracle FLEXCUBE Form and send it to the head of the concerned department.
Profile Disabled Already Disabled User Already Logged In	You should indicate the USER ID in the Standard Oracle FLEXCUBE Form and send it to the head of the concerned department.
Bad Control Password	You should approach the Password Administrator/s (Control Clerk) and enquire if this was an input error.
New Control Password	You should verify that the change was made by a Password Administrator/s (Control Clerks). You should check the Key and Combination record to verify that the new Password has been sealed in an envelope. These envelopes should be kept in the bank and off-site.

4.1.1.2 Review of Audit Report

Records of login and logout messages should be printed through a dot matrix printer maintained for the purpose. You should review the records to ensure the following:

- There is no break in the sequence of numbers
- The Data Center Manager has reviewed the log.
- When the log shows entries by non- Oracle FLEXCUBE users (Repair, System Administrator, etc.), there is reconciliation with the terminal session records.
- If there has been an entry through the SUPERVISOR ID, there is justification for it.

If there are any irregularities in the records, the Head of Operations should be informed.

4.1.2 Weekly Review Procedure

Specify the following details.

4.1.2.1 Review of Protocol

On a weekly basis, the protocol reports (violation / audit reports) that have been generated by the staff of the Data Center every day, with the print and delete option should be reviewed. The reports will give the protocol list with details of the functions accessed, along with the name of the operator and the terminal ID.

On a daily basis, the Data Center Manager should check the list for the following:

Functions terminated with NO END

Programs should end normally. If a program has ended abnormally due to a software or hardware error, power failure, forced logout, etc., the message NO END will appear against the concerned ID on the Protocol report.

EOD Programs

The Data Center Manager should ensure that all EOD programs have been run. The use of programs like Clear User Profile etc. should be justified.

Sequential Deletion Number

The Security report contains a sequence number. It should be verified that the number on the report is consistent with the last report's sequence number (last seq. no + 1).



On a weekly basis, you should verify that the Data Center Manager has reviewed the Protocol report every day, covering the above aspects.

4.1.3 Monthly Review Procedure

This section describes the reviews to be carried out on a monthly basis:

- Review of Software Changes.
- Review of Access Rights.
- Review of space-management in the ORACLE database.
- Review of response time.

4.1.3.1 Review of Software Changes

The source programs need to be controlled to ensure that modifications are made only after due approval and review.

The Librarian is the custodian of programs and back-up data. Program maintenance and reconciliation are the responsibility of the librarian.

All modifications should be approved by the head of the bank or by senior people designated for the task. Oracle FLEXCUBE Development and Modification (MDM) forms should be filled in, serially numbered and signed by the appropriate people - the User, Programmer, Data Center Manager and Librarian., Database Administrator.

4.1.3.2 Review of Access Rights

It is advisable to check the access rights of users in the system. This would ensure that no one is able to access a system function that should not have been available to him/her. Any access rights given at the user level and not at the role level need to be explained.

4.1.4 Quarterly Review Procedure

This section describes the quarterly reviews to be carried out by you:

- Review of Software Fault Reports
- Review of Hardware Maintenance
- Review of the Database Parameters like SGA, Rollback Segments, no. of datafiles etc
- Review of Data Center Procedure
- Review of Library Procedure
- Review of Password and Key and Combination Records

4.1.4.1 Review of Software Fault Reports

When there is a fault in the software, the user is required to fill in a Software Fault Report (SFR) through the software POIROT. The details to be included are:

- The Terminal & User ID
- The function being run when the fault occurred
- The type of error
- The message that appeared on the terminal screen

The Data Center Manager should indicate on the SFR, the nature of action taken.

The SFRs should be forwarded to you for regular reviews. You should verify that timely action has been taken. If you find recurring problems you should report them to the Head of Operations.

4.1.4.2 Review of Hardware Maintenance

The Data Center should have a Branch Data Center Manual that covers hardware problems and their solutions.

When a hardware fault is encountered the user should fill in a Hardware Fault Report (HFR) and send it to the Data Center Manager. The Data Center Manager should indicate in the report, the nature of action taken.

On a quarterly basis, the Hardware Fault Reports should be sent for review. It should be verified that:

- Hardware Fault Reports have been prepared when faults have been encountered.
- The HFRs include all details of the fault.
- The maintenance work has been documented. When External Repair Personnel have been summoned, ensure that they have signed in the log, indicating the nature of work carried out by them.
- A record has been maintained for equipment downtime.
- A record has been maintained for preventive measures taken on disk drives and CPUs.
- The Branch Data Center Manual is followed for hardware maintenance.
- Hardware is serviced regularly. Any unserviceable equipment should be replaced.
- The Maintenance Contracts are current.

4.1.4.3 Handling of Spare Parts

Spare parts should be maintained very carefully. Additional control is necessary. You should verify that there is an accurate inventory of all items. You should ensure that the spare parts are maintained in a secure location and that only authorized people enter the area. Records should be maintained for usage of spare parts. The information recorded should cover:

- The type of spare part
- The name of the person receiving the spare part
- The need for the spare part

On a quarterly basis, review these records to ensure that everything is in order. After the review is completed send a memorandum to the Data Center Manager. If there are discrepancies, they should be mentioned in the memorandum. A copy of this memorandum is to be sent to the Head of Operations.

4.1.4.4 Review of the Data Center Procedure

You are recommended to carry out quarterly reviews on the safety, security and fire prevention measures. You should ensure that:

- There is a list of people who are authorized to enter the Data Center and a log is being maintained for people who enter it.
- Authorization for access to the Data Center is strictly controlled.
- A list of important addresses and phone numbers is put up in a prominent place. The list should include:
 - The Data Center Manager
 - Shift Supervisors
 - Operators
 - Programmers
 - Head of the Control Department
 - Personnel holding access to SA and REPAIR functions
 - Technical Support staff
 - The Police department
 - The Fire department
 - The nearest hospital
 - The electricity company
- Non-bank personnel who access the Data Center are always accompanied by authorized personnel.
- The librarian, operators and programmers are independent of each other.
- The staff in the Data Center is trained in its duties and in the Security systems of the organization.
- The Data Center temperature is maintained between 18 and 26 degrees Centigrade and the humidity between 20 and 60%.
- Inflammable material and excessive stationery are not kept in the Data Center.
- The air conditioning system is well maintained.
- The fire alarm system in the Data Center is tested regularly.
- The fire extinguishers are easily accessible and are inspected regularly.

- The Data Center staff is not permitted to eat, drink or smoke in the Data Center.
- All Maintenance contracts are current. Maintenance contracts should be held for:
 - Fire prevention equipment
 - Fire detection equipment
 - Air-conditioning systems
- End of Day and End of Month logs are updated regularly in the Data Center.
- The staff at the Data Center does not have any input or authorization password, other than Dates file.

4.1.4.5 Review of Library procedure

The Librarian is responsible for:

- Disks
- Tapes
- Operational programs
- Software
- Documentation associated with all systems
- Material related to data processing, e.g., magnetic media, spare parts, etc.

There are three kinds of libraries:

- Data Center Library
- In-house Library
- Off-site Library

It should be ensured that the library procedure is systematically followed. The procedure is given below:

- The required forms should be filled out and signed regularly.
- The inventory of magnetic media should be updated by the Librarian on a monthly basis.
- A Historical Information Form should be maintained for every disk and tape. It should cover all details of the tape, including its movements- in and out, of libraries.
- Disks and tapes, etc., should be stored in locked metallic cabinets.
- The off-site library should be under dual custody.
- There should be a reconciliation of media stock in the various libraries with the records of the librarian. Any discrepancies should be notified to the Head of Operations.
- Program change documentation should be maintained in the libraries of the bank and off-site.
- Tapes and Disks should be labelled according to the norms of the organization.

- Back-ups of all data should be maintained in the off-site library.
- There should be an updated copy of the Librarian s records in the off-site back-up.
- The libraries should be fire-proof and secure.
- The librarian should be well- trained. There should be another person equipped to replace the librarian in case the necessity arises.
- The librarian should keep accurate records of all disks and tapes given to the Data Center personnel.
- The off-site library should have copies of:
 - Oracle FLEXCUBE manuals
 - Local Procedure manuals
 - Technical manuals
 - Program Change Documentation
 - Contingency plans

4.1.4.6 Review of Password and Key and Combination Records

It should be ensured that the following steps are meticulously followed:

- When a user profile is deleted, added or modified, an approved Password Maintenance Request (PMR) form should be forwarded to the Password Administrators (PAs). The PAs should ensure that the PMR is approved by the Head of Operations. There should be no overwriting or alteration on the form. The PAs should sign the form and file it.
- When the PAs receive a PMR they should refer to the PMR files and ensure that it is not a duplication.
- The passwords for PAs, SA and Repair personnel should be maintained in sealed envelopes and kept in the bank and off-site.
- If a password is issued to an alternate holder for a specific purpose, it should be changed when the purpose is achieved. The altered password should be sealed in an envelope and maintained in the bank and off-site.
- Every change in the sealed envelopes should be reflected in the Key and Combination Record.
- Employees who go on leave should ensure that their profiles are disabled.
- Employees who are related to each other should not hold conflict of interests functions in Oracle FLEXCUBE, e.g., Maker and Checker, etc.
- Allocation of programs should be based on functional responsibilities (especially to the staff of the Control Department and the Data Center).

4.1.4.7 Review of Database Administration

Database Administration is one of the most important activities of the Data Center personnel. Since the Database Administrator (DBA) has access to all the tables and other objects in the database, it should be ensured that the use of SQLPLUS under SYS and SYSTEM user is minimised and whenever used, an explanation is provided. An audit option could be included if required for all actions of the SYS and SYSTEM user. It is the DBA's responsibility to ensure that the system resources (for ex. SGA, Rollback segments) are in tune with the size of the database. The DBA also would have to add additional datafiles as the database increases in size. In case of distributed databases, it is DBA who should ensure that the DBLINKS (database links) are maintained between all the instances.

4.1.5 Annual Review Procedure

When the software is being installed, the Data Center should ensure that the back-up and contingency plans are adequate, reflecting current technology. The Risk Analysis should be incorporated in the Data Center Manual with particular reference to Computer Hardware and other automation-related equipment (including telecommunication).

The following functions should be carried out annually:

- Ensure that there is a plan that adheres to the standards of the bank.
- Ensure that the Line Management has reviewed the Risk Analysis on a quarterly basis, and has updated or modified it accordingly.
- Review and retain a copy of the report that documents testing of the Contingency Plan. If you have not been involved in the plan itself, a sample review of the report should be made.
- Review the Insurance policy to ensure that the hardware is adequately covered and that it is current. If additional hardware or spare-parts have been procured during the year, ensure that a revised insurance policy has been obtained.
- Review the Maintenance Contract Agreement for hardware servicing, to ensure that it is current and the service is satisfactory.



Control
[January] [2010]
Version 11.0

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
[www.oracle.com/ financial_services/](http://www.oracle.com/financial_services/)

Copyright © [2010] Oracle Financial Services Software Limited. All rights reserved.

No part of this work may be reproduced, stored in a retrieval system, adopted or transmitted in any form or by any means, electronic, mechanical, photographic, graphic, optic recording or otherwise, translated in any language or computer language, without the prior written permission of Oracle Financial Services Software Limited.

Due care has been taken to make this document and accompanying software package as accurate as possible. However, Oracle Financial Services Software Limited makes no representation or warranties with respect to the contents hereof and shall not be responsible for any loss or damage caused to the user by the direct or indirect use of this document and the accompanying Software System. Furthermore, Oracle Financial Services Software Limited reserves the right to alter, modify or otherwise change in any manner the content hereof, without obligation of Oracle Financial Services Software Limited to notify any person of such revision or changes.

All company and product names are trademarks of the respective companies with which they are associated.