ORACLE

Oracle Database and the Reserve Bank of India Security Guidelines

A practical approach to meeting RBI requirements with the Oracle Database

June 2020 | Version 20.01

PURPOSE

This technical white-paper provides an overview of securing an Oracle Database, including a discussion of features, options, and complimentary products. It is intended to help you evaluate options for reducing security risk and improving regulatory compliance for your Oracle Databases.

INTENDED AUDIENCE

If you are responsible for designing, implementing, maintaining, or operating security controls for an Oracle Database this paper is intended for you.

DISCLAIMER

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

The purpose of this document is to help organizations understand how Oracle Database Security technology can be utilized to help comply with certain Reserve Bank of India requirements. Some of the Oracle Database Security technologies may or may not be relevant based upon an organization's specific environment. Oracle always recommends testing security solutions within your specific environment to ensure that performance, availability and integrity are maintained.

The information in this document may not be construed or used as legal advice about the content, interpretation or application of any law, regulation or regulatory guideline. Customers and prospective customers must seek their own legal counsel to understand the applicability of any law or regulation on their processing of personal data, including through the use of any vendor's products or services.

EXECUTIVE SUMMARY

The breadth of RBI's guidance can be daunting, but from a database security standpoint that guidance can be summed up in a few core principles:

1. Know your databases including patch levels and configuration. Be aware of which databases contain sensitive data
2. Encrypt sensitive data at rest and in motion
3. Control access to sensitive data, enforcing least privilege to restrict access to only what is needed to carry out an individuals job function
4. Monitor access to data, securing the audit trail to prevent tampering or destruction

Security capabilities of Oracle Database can be used to help comply with RBI guidance.

TABLE OF CONTENTS

Purpose	1
Intended Audience	1
Disclaimer	1
Executive Summary	1
Table of Contents	2
Background	3
Mapping RBI Guidelines to Database Controls	3
Conclusion	10
References	10

BACKGROUND

The Reserve Bank of India (RBI) exercises supervision and control over banks and non-banking finance companies in India. This includes a mandate to encourage data security practices that protect citizen's privacy, minimize the opportunity for fraud, and improve the integrity of financial transactions. RBI paved the way for a secure banking system in 2011 with the release of the reports and recommendations of the Working Group on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds and the subsequent *Guidelines on Information security, Electronic banking, Technology risk management and cyber* frauds (reference 1) which required Financial Services institutions to establish a board-approved information security policy that considers information security at all stages of an information assets lifecycle. Guidelines from the working group recommendation also included requirements for controlling and auditing access to data. These guidelines increased the level of detail around RBI recommendations for securing data.

In 2016, RBI released the *Cyber Security Framework in Banks* (reference 2). The 2016 guidelines require banks to take appropriate steps in preserving the confidentiality, integrity, and availability of financial data and stress the urgency. To assist banks in complying with the guidelines, a list of baseline controls is included in annex 1. These guidelines augment those from the original 2011 working group and the combination of the two documents form the basis of current RBI policy regarding securing financial data. RBI guidance was extended to Urban Cooperative Banks (UCB) in 2018 (reference 3), with a control framework very similar to earlier guidance in the 2011 and 2016 guidelines. The UCB guidance was updated in 2019, with RBI separating UCBs into four distinct categories with different reporting requirements (ref 4).

While all four documents are important to understand RBI's comprehensive guidance, most specific technical guidance is found in references 1 and 2.

Oracle Database is used throughout the global financial services industry, by every major financial institution. Security has been a core capability of the database since its creation, and over time Oracle Database has evolved a comprehensive set of security capabilities that allow it to meet virtually any compliance target. The RBI guidelines are no exception. Here are some of the database-relevant guidelines along with the corresponding database security capability that can help you meet the requirement.

MAPPING RBI GUIDELINES TO DATABASE CONTROLS

Oracle Database has hundreds of features, options, and supporting products. Below you will find the RBI guidelines relevant to Oracle Database, along with the suggested database capability to help you meet the guidelines. In the Source column, I list the relevant document, annex, and paragraph number. A key with links to the reference documents may be found at the end of this section.

This paper is a summary of the RBI Guidelines and corresponding database capabilities. In many cases, a requirement will appear in multiple different references – since all of the guidelines listed as references are still active, we've listed each source. Because Oracle Database is so widely used by financial institutions, Oracle also provides a more in-depth look at the activity monitoring requirements outlined below, with specific recommendations on configuring the suggested controls to meet the requirements of the guidelines. That detailed paper is available upon request.

Key to the four references listed in the Source column:

1. Guidelines on Information security, Electronic banking, Technology risk management and cyber frauds
2. Cyber Security Framework in Banks
3. Basic Cyber Security Controls for Primary (Urban) Cooperative Banks (UCBs)
4. Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach

Note: Page numbers listed are based upon the PDF page number, not the page numbers shown in the actual document

RBI Guideline	Source	Oracle Database Control
Audit of logging and monitoring of access to IT assets by all users	Ref 1, page 20, item (vi)(h)	Oracle Database has the capability to audit all user access to the system. Oracle Audit Vault and Database Firewall centralizes database audit information into a secure repository for analysis, reporting, and alerting
Regular reviews of user access by information asset owners to ensure appropriate access is maintained	Ref 1, page 20, item (vi)(i)	Oracle Audit Vault and Database Firewall retrieves user account and entitlement information for the Oracle Database, and produces reports which data owners can review and attest to
Applying the four-eyes principle to very critical/sensitive IT assets	Ref 1, page 20, item (vi)(j)	Oracle Database Vault command rules can be used to enforce the four-eyes requirement for sensitive database commands
Instituting strong controls over remote access by privileged users	Ref 1, page 20, item (xiii)(b)	Oracle Database Vault can restrict the ability to connect from remote network access in accordance with bank policies. Oracle Database can audit access from remote networks. Oracle Audit Vault and Database Firewall can alert when remote network access is detected in the database audit trail
Personnel with elevated system access privileges should be closely supervised with all their systems activities logged as they have the inside knowledge and the resources to circumvent systems controls and security procedures.	Ref 1, page 20, item xiii	Oracle Database can audit privileged user activity. Oracle Audit Vault and Database Firewall collects audit data and stores it in a secure repository for analysis and reporting.
Maintaining audit logging of system activities performed by privileged users	Ref 1, page 21, item (xiii)(e)	Oracle Database can audit system activities performed by privileged users. Oracle Audit Vault and Database Firewall collects information on privileged user activity and supports reporting, analysis, and alerting on that activity
Ensuring that privileged users do not have access to systems logs in which their activities are being captured	Ref 1, page 21, item (xiii)(f)	Oracle Audit Vault and Database Firewall extracts audit logs from the database and operating system, and centrally stores that information in a secure repository which can be separated from the database and system administrators.
Conducting regular audit or management review of the logs	Ref 1, page 21, item (xiii)(g)	Oracle Audit Vault enables periodic review of audit data, and allows for reviewers to attest to their completion of the review

RBI Guideline	Source	Oracle Database Control
Applications must not allow unauthorized entries to be updated in the database	Ref 1, page 25, item 15	Oracle Database Vault can block unauthorized updates to data, including from compromised privileged users. Oracle Database can audit attempts to perform unauthorized access, even if that attempt is blocked by Oracle Database Vault. Oracle Audit Vault and Database Firewall can collect and store this audit information for analysis, reporting, and alerting
All application systems need to have audit trails along with policy/procedure of log monitoring for such systems including the clear allocation of responsibility in this regard. Every application affecting critical/sensitive information, for example, impacting financial, customer, control, regulatory and legal aspects, must provide for detailed audit trails/ logging capability with details like transaction id, date, time, originator id, authorizer id, actions undertaken by a given user id, etc. Other details like logging the IP address of the client machine, terminal identity or location may also be considered.	Ref 1, page 25, item 5	Oracle Database provides comprehensive auditing capabilities. Oracle Audit Vault and Database Firewall centralizes that audit information in a secure repository for reporting and analysis
Applications must also provide for, inter-alia, logging unsuccessful logon attempts, access to sensitive options in the application, e.g., master record changes, granting of access rights, use of system utilities, changes in system configuration, etc.	Ref 1, page 25, item 6	Oracle Database audits unsuccessful logins, granting of access rights, and changes to database configuration
The audit trails need to be stored as per a defined period as per any internal/regulatory/statutory requirements and it should be ensured that they are not tampered with.	Ref 1, page 25, item 7	Oracle Audit Vault and Database Firewall stores audit information in a tamper-resistant repository that is separate from the source that generates the audit data. Retention of audit data within the Audit Vault is controlled by retention periods assigned per database, allowing a single Audit Vault to satisfy multiple retention period requirements.
The development, test and production environments need to be properly segregated.	Ref 1, page 25, item 9 Ref 2, page 10, item 6.5	Oracle Data Masking and Subsetting and Oracle Data Safe both remove sensitive data from non-production copies of databases.
Access to application should be based on the principle of least privilege and “need to know” commensurate with the job responsibilities. Adequate segregation of duties needs to be enforced	Ref 1, page 25, item10	Oracle Database Vault controls privileged user access, separating database administration from access to sensitive data and enabling close control of administrator and developer ability to directly update the database.

RBI Guideline	Source	Oracle Database Control
Direct back-end updates to database should not be allowed except during exigencies with genuine business need and after due authorization as per relevant policy.	Ref 1, page 26, item 16	Oracle Database Vault can enforce trusted-path access to data, restricting the use of application service accounts so they can not be used for ad-hoc access to data
Access to the database prompt must be restricted only to the database administrator.	Ref 1, page 26, item 17	Oracle Database Vault can enforce trusted-path access to data, restricting the use of application service accounts so they can not be used for ad-hoc access to data
Applications should be configured to logout the users after a specific period of inactivity. The application must ensure rollover of incomplete transactions and otherwise ensure integrity of data in case of a log out.	Ref 1, page 26, item 26	Oracle Database Password Profiles control inactive session timeout periods. Profiles are assigned at the user level, so a single database can support different inactive timeouts for different classes of user.
Banks need to define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.	Ref 1, page 29, item 15) i	Oracle Database can apply data block checksums to identify corrupt or maliciously altered data blocks through the DB_BLOCK_CHECKSUM parameter. Checksum can be for all blocks, or for a sampling of blocks.
Highly sensitive and/or critical IT assets would need to have logging enabled to record events and monitored at a level proportional to the level of risk.	Ref 1, page 32, item v	Oracle Database auditing allows for different levels of auditing for different database objects and users, allowing the amount of logging to be adjusted proportional to the risk.
Users, like system administrators, with elevated access privileges should be subjected to a greater level of monitoring in light of the heightened risks involved.	Ref 1, page 32, item vi	Oracle Database auditing allows auditing of end user activity, including the ability to differentiate between appliation service accounts and user-intitated sessions
The integrity of the monitoring logs and processes should be safeguarded through appropriate access controls and segregation of duties	Ref 1, page 32, item vii	Oracle Database auditing stores audit records in a schema that is protected from update and delete operations, only allowing purging of the audit trail under narrowly defined conditions. Oracle Audit Vault and Database Firewall extends this protection by moving the database audit trail into a secure repository that is protected from access by database administrators

RBI Guideline	Source	Oracle Database Control
Banks should frequently review all system accounts and disable any account that cannot be associated with a business process and business owner. Reports that may be generated from systems and reviewed frequently may include, among others, a list of locked out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire.	Ref 1, page 32, item viii	Oracle Audit Vault and Database Firewall reports on database accounts and their assigned privileges. Reports on unused/dormant and locked account are also included. Both Database Security Assessment Tool and Oracle Data Safe will identify accounts with expired passwords and passwords that never expire.
Banks should regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.	Ref 1, page 32, item x	Oracle Database Password Profiles control inactive session timeout periods. Profiles are assigned at the user level, so a single database can support different inactive timeouts for different classes of user.
Banks should monitor account usage to determine dormant accounts that have not been used for a given period, say 15 days, notifying the user or user's manager of the dormancy. After a longer period, say 30 days, the account may be disabled.	Ref 1, page 32, item xi	Oracle Audit Vault and Database Firewall reports on database accounts, including dormant or inactive accounts.
On a periodic basis, say monthly or quarterly basis, banks should require that managers match active employees and contractors with each account belonging to their managed staff. Security/system administrators should then disable accounts that are not assigned to active employees or contractors.	Ref 1, page 32, item xii	Oracle Audit Vault and Database Firewall reports on database accounts, including assigned system and object privileges. Reports are available for managed attestation by data owners and managers.
Banks should monitor attempts to access deactivated accounts through audit logging.	Ref 1, page 32, item xiii	Oracle Database can audit attempts to login as a locked account
Banks should validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries. If systems cannot generate logs in a standardized format, banks need to deploy log normalization tools to convert logs into a standardized format.	Ref 1, page 32, item xiv	Oracle Database audit records include timestamp, source address, database and OS user names, and other information useful in analyzing transactions
System administrators and information security personnel should consider devising profiles of common events from given systems, so that they can tune detection to focus on unusual activity, reducing false positives, more rapidly identify anomalies, and prevent overwhelming the analysts with insignificant alerts.	Ref 1, page 32, item xv	Oracle Audit Vault and Database Firewall performs network-based monitoring of database activity. The Database Firewall profiles are tuned to white-list normal activity, and to block/record/alert on deviations from normal activity patterns

RBI Guideline	Source	Oracle Database Control
Banks needs to ensure that audit trails exist for IT assets satisfying the banks business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution. This could include, as applicable, various areas like transaction with financial consequences, the opening, modifications or closing of customer accounts, modifications in sensitive master data, accessing or copying of sensitive data/information; and granting, modification or revocation of systems access rights or privileges for accessing sensitive IT assets.	Ref 1, page 36, item 21) i	Oracle Database auditing is flexible and extensible, contributing to and regulatory and legal compliance and supporting forensic investigation
Audit trails should be secured to ensure the integrity of the information captured, including the preservation of evidence. Retention of audit trails should be in line with business, regulatory and legal requirements	Ref 1, page 36, item 21) ii	Oracle Audit Vault and Database Firewall protects audit trails with a combination of encryption and strong access controls. Retention of audit trails is configured on a per-database basis to allow for varying business requirements
Recent incidents have highlighted the need to thoroughly review network security in every bank. In addition, it has been observed that many times connections to networks/databases are allowed for a specified period of time to facilitate some business or operational requirement. However, the same do not get closed due to oversight making the network/database vulnerable to cyber-attacks. It is essential that unauthorized access to networks and databases is not allowed and wherever permitted, these are through well-defined processes which are invariably followed. Responsibility over such networks and databases should be clearly elucidated and should invariably rest with the officials of the bank.	Ref 2, page 3, item 9	Oracle Database supports a wide variety of access control mechanisms that can be tuned to block unauthorized access at the session, data object, and command level
Classify data/information based on information classification/ sensitivity criteria of the bank	Ref 2, page 7, item 1.2 Ref 3, page 1, item 1.2	Transparent Sensitive Data Protection (TSDP) – TSDB allows grouping columns in different tables together into arbitrary classification types. All columns of a given type may be governed by policies requiring encryption and auditing
Continuously monitor the release of patches by various vendors / OEMs, advisories issued by CERT-in and other similar agencies and expeditiously apply the security patches as per the patch management policy of the bank	Ref 2, page 8, item 2.3	Oracle Critical Patch Updates (CPUs)- Oracle customers may subscribe to receive notifications of security patches, including CVSS scoring for risks addressed.
Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints	Ref 2, page 9, item 4.7	Oracle Audit Vault and Database Firewall profiles normal activity and can alert on or block unusual activity.

RBI Guideline	Source	Oracle Database Control
periodically evaluate critical device (such as firewall, network switches, security devices, etc.) configurations and patch levels for all systems	Ref 2, page 9, item 5.2	Oracle Database Security Assessment Tool and Oracle Data Safe both evaluate database configuration and report on variations from best practices.
Provide secure access to the bank's assets/services from within/outside bank's network by protecting data/information at rest	Ref 2, page 11, item 8.1	Transparent Data Encryption encrypts data at rest within the database.
Implement centralised authentication and authorisation system or accessing and administering applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties.	Ref 2, page 11, item 8.4	Enterprise User Security and Centrally Managed Users provide centralised authentication and authorisation for Oracle Database. Authentication may be via password, Kerberos, PKI certificate, of multi-factor through RADIUS Oracle Database supports password complexity, minimum length requirements, expiration and more. Oracle Database Vault enforces separation of duties, including restricting database administrator access to sensitive data.
Implement appropriate (e.g. centralised) systems and controls to allow, manage, log and monitor privileged/superuser/administrative access to critical systems	Ref 2, page 11, item 8.5 Ref 3, page 3, item 7.4	Oracle Audit Vault and Database Firewall provides centralised logging and monitoring of privileged, super user, and administrative access to the database.
Implement controls to minimize invalid logon counts, deactivate dormant accounts	Ref 2, page 11, item 8.6	Oracle Audit Vault and Database Firewall provides reporting on dormant user accounts and failed login attempts.
Monitor any abnormal change in pattern of logon.	Ref 2, page 11, item 8.7	Oracle Audit Vault and Database Firewall detects, alerts, and blocks abnormal login patterns.
Develop a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information.	Ref 2, page 14, item 15.1	Oracle Database Security Assessment Tool, Oracle Data Masking and Subsetting, and Oracle Data Safe each provide sensitive data discovery capabilities. Oracle Audit Vault and Database Firewall detects access to sensitive data.
Manage and analyse audit logs in a systematic manner so as to detect, understand or recover from an attack.	Ref 2, page 14, item 16.1	Oracle Audit Vault and Database Firewall collects and securely stores audit logs for analysis. Because the audit logs are transferred to a secure repository, they can be used to help understand what happened in the event of an attack.

RBI Guideline	Source	Oracle Database Control
Implement and periodically validate settings for capturing of appropriate logs/audit trails of each device, system software and application software, ensuring that logs include minimum information to uniquely identify the log for example by including a date, timestamp, source addresses, destination addresses.	Ref 2, page 14, item 17.1 Ref 4, page 8, item 6.3	Oracle Audit Vault and Database Firewall captures audit logs for each database server, including database and operating system security logs. The system is extensible and can also capture audit trails for most applications using the custom collector framework.
Periodically conduct vulnerability assessment and penetration testing exercises for all the critical systems,	Ref 2, page 14, item 18.1	Oracle Database Security Assessment Tool and Oracle Data Safe both provide security assessment functionality that can be used to help assess a system's vulnerability, augmenting a penetration testing regime with early detection and remediation of known vulnerabilities
Capture the audit logs pertaining to user actions in a system. Such arrangements should facilitate forensic auditing, if need be.	Ref 4, page 6, item 10.1	Audit Vault and Database Firewall captures audit logs and stores them in a secure repository for analysis and reporting
An alert mechanism should be set to monitor any change in the log settings.	Ref 4, page 6, item 10.2	Audit Vault and Database Firewall can report and alert on changes to audit settings
Provide secure access to the UCB's assets/services from within/outside UCB's network by protecting data/information at rest (e.g. using encryption, if supported by the device) and in-transit (e.g. using technologies such as VPN or other standard secure protocols, etc.)	Ref 4, Page 6, item 6.1	Oracle Database offers both Native Network Encryption and industry standard Transport Layer Security (TLS) 1.2 to protect data in-transit. Oracle Transparent Database Encryption encrypts data at rest, including in database backups, clones, and exports.
Manage and analyse audit logs in a systematic manner so as to detect, respond, understand or recover from an attack.	Ref 4, page 8, item 6.2	Audit Vault and Database Fireall provides capbilities to manage and analyse audit logs

CONCLUSION

The Reserve Bank of India guidelines provide a comprehensive framework for financial institution security. Oracle Database's security capabilities play an important part in complying with those guidelines.

REFERENCES

1. Guidelines on Information security, Electronic banking, Technology risk management and cyber frauds http://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf
2. Cyber Security Framework in Banks https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF
3. Basic Cyber Security Controls for Primary (Urban) Cooperative Banks (UCBs) http://rbidocs.rbi.org.in/rdocs/content/pdfs/63NT19102018_A1.pdf
4. Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI129BB26DEA3F5C54198BF24774E1222E61A.PDF

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Database Security and Regulatory Compliance
June, 2020
Russ Lowenthal, Database Security Product Management