



Accelerate your Database Activity Monitoring readiness to comply with Reserve Bank of India (RBI) Guidelines

June 2020 | Version 20.01
Copyright © 2020, Oracle and/or its affiliates

PURPOSE

This technical white-paper provides an overview of Database Activity Monitoring requirements for compliance with the RBI Guidelines on Cyber Security. The white-paper is intended to help you accelerate your readiness to RBI compliance for Database Activity Monitoring requirements by leveraging Oracle Database's native auditing feature, and Oracle Audit Vault and Database Firewall (AVDF) product.

INTENDED AUDIENCE

Intended audience would include key stakeholders like CIOs, CISOs, Executive Directors, business unit heads, heads of internal audit, operational risk, compliance and fraud management from all of the financial institutions regulated by RBI in Indian sub-continent. If you are responsible for designing, implementing, maintaining, or operating security controls for database systems, this paper is intended for you to help accelerate compliance with RBI guidelines on Database Activity Monitoring requirements.

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.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

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.

LEGAL DISCLAIMER

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.

TABLE OF CONTENTS

Purpose	1
Intended Audience	1
Disclaimer	1
Legal Disclaimer	1
Table of Contents	2
Introduction	3
RBI CIRCULARS	3
EXECUTIVE SUMMARY	4
1. RBI Guidelines for Database Auditing	7
1.1. Sensitive Data Access	7
1.2. Access Control	10
1.3. Privileged User Access	12
1.4. Application Activity	13
1.5. Inactive User Accounts	16
1.6. Specific Components	17
2. RBI Guidelines for Ensuring Audit Integrity	18
Recommendations:	19
3. RBI Guidelines for Continuous Surveillance	21
Recommendations:	24
4. RBI Guidelines for Monitoring Network Traffic	33
4.1. Network Segmentation	33
4.2. Deployment Topology	35
4.3. Firewall Policy	37
Conclusion	45
Appendix	45
Application Activity Auditing Sample	45

INTRODUCTION

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.

The **Reserve Bank of India** issued guidance in April 2011 for banks to mitigate the risks of use of information technology in banking operations. RBI Guidelines are the result of the Working Group's recommendations on information security, electronic banking, technology risk management and cyber fraud. The Working Group was formed under the chairmanship of G. Gopalakrishna, the executive director of RBI in April 2010.

RBI's initial guidance on cyber security was issued in 2011, and additional circulars have been issued over the years, as listed below. Database Activity Monitoring is one of the key requirements for RBI compliance. This paper examines Oracle Database security capabilities that can be used to help comply with RBI Guidelines for Database Activity Monitoring.

RBI CIRCULARS

RBI Circular dated April 29, 2011 on "RBI Circular: Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds- Implementation of recommendations"

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=6366&Mode=0>

Guideline Reference (**Ref 1**): <http://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf>

In a June 2, 2016 notification, RBI released a circular on the "Cyber Security Framework for Banks", as an extension of the circular of April 29, 2011. The circular says that scheduled commercial banks (private, foreign and nationalized banks listed in the schedule of RBI Act, 1934) must proactively create or modify their policies, procedures and technologies based on new security developments and concerns.

RBI Circular dated June 2, 2016 on "Cyber Security Framework in Banks"

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0>

Guideline Reference (**Ref 2**):

<https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF>

RBI developed new norms to scale up the cyber-security and resilience framework at the urban cooperative banks (UCBs) with its circular dated October 19, 2018.

RBI Circular dated October 19, 2018 on "Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs)"

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11397&Mode=0>

RBI recommended a basic cyber security framework to be implemented by all the UCBs (**Ref 3**):

http://rbidocs.rbi.org.in/rdocs/content/pdfs/63NT19102018_A1.pdf

On December 31, 2019, RBI released the below circular on a comprehensive Cyber Security Framework for UCBs:

RBI Circular dated December 31, 2019 on "Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach"

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11772&Mode=0>

Guideline Reference (**Ref 4**):

<https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOT1129BB26DEA3F5C54198BF24774E1222E61A.PDF>

EXECUTIVE SUMMARY

As the banking and financial sector industry in India prepares for RBI compliance on cyber security regulations, Database Activity Monitoring (DAM) is one of the key requirements. RBI mandates a Security Operations Centre (SOC) be set up at the earliest to ensure continuous surveillance. Banks need to ensure the protection of various personal and sensitive information collected from consumers and preserve its Confidentiality, Integrity and Availability regardless of whether the data is stored (or in transit) within the bank, with customers, or with third party vendors. RBI recommends that banks address network and database security comprehensively.

Database Activity Monitoring is crucial for compliance with the RBI Guidelines on Cyber Security. Some of the key references in RBI Guidelines that highlights the DAM requirements are mentioned.

RBI Guidelines	Source	DAM Requirements highlighted
<i>The fundamental attributes supporting data quality should include accuracy, integrity, consistency, completeness, validity, timeliness, accessibility, usability and auditability.</i>	Ref 1, Page 10	Auditability of data for ensuring data quality.
Accountability and auditability: <i>An organization's security policy can be properly enforced only if accountability is maintained, i.e., security can be maintained only if subjects are held accountable for their actions. Effective accountability relies upon the capability to prove a subject's identity and track their activities. Accountability is established by linking a human to the activities of an online identity through the security services and mechanisms of auditing, authorization, authentication, and identification.</i>	Ref 1, Page 11	Auditability of user activities to ensure accountability.
<i>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.</i>	Ref 1, Page 29, Item 15.i	Ensuring data integrity and consistency.
<i>Digital evidence is similar to any other form of legal proof - it needs to withstand challenges to its integrity, its handling must be carefully tracked and documented, and it must be suitably authenticated by concerned personnel as per legal requirements</i>	Ref 1, Page 16, Item 1.5	Audit data as a form of digital evidence.
<i>Achieving robust security (security assurance) is not a onetime activity. ... It is a continuous process that requires regular assessment of the security health of the organization and proactive steps to detect and fix any vulnerability. Every bank should have in place quick and reliable access to expertise for tracking suspicious behavior, monitoring users and performing forensics.</i>	Ref 1, Page 136, Item 8.2.(d)	Monitoring of user behavior for suspicious activities and forensics.
<i>Hence, it is mandated that a SOC (Security Operations Centre) be set up at the earliest, if not yet been done. It is also essential that this Centre ensures continuous surveillance</i>	Ref 2, Page 2, Item 6	Ability to provide continuous surveillance.
Comprehensively address network and database security: <i>Recent incidents have highlighted the need to thoroughly review network security in every bank. ... 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.</i>	Ref 2, Page 3, Item 9	Comprehensive need for database auditing and network monitoring.
Cyber Crisis Management Plan: <i>CCMP should address the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment. Banks need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond / recover / contain the fall out. Banks are expected to be</i>	Ref 2, Page 4, Item 12	Prompt detection of intrusions and response is needed.

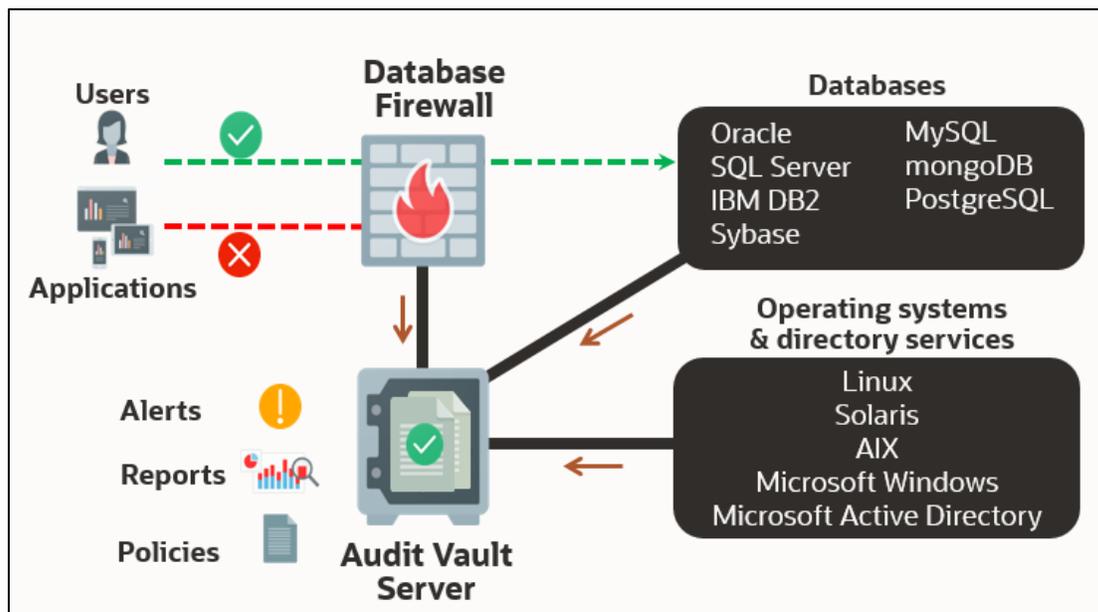
<p>well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks.</p>		<p>Detect cyber-intrusions by alerting on anomalies in database access patterns.</p>
<p>Constant and Continuous monitoring of the environment using appropriate and cost effective technology tools, clearly defined policies and procedures based on best practices and monitored by technically competent and capable manpower is the urgent need for the Industry.</p> <p>Take into account proactive approaches rather than reactive approaches and have to also address possible unknown attacks. For example, zero day attacks and attacks for which signatures are not available have to be kept in mind</p> <p>Cyber SoC has to take into account proactive monitoring and management capabilities with sophisticated tools for detection, quick response and backed by data and tools for sound analytics.</p> <p>Incident investigation, forensics and deep packet analysis need to be in place</p> <p>Analytics with good dash board, showing the Geo-location of the IP's</p>	<p>Ref 2, Page 18, Item 3,Item 4.2, Item 4.4</p>	<p>Enable constant and continuous proactive monitoring.</p>
<p>Audit Logs: Capture the audit logs pertaining to user actions in a system. Such arrangements should facilitate forensic auditing, if need be. An alert mechanism should be set to monitor any change in the log settings.</p>	<p>Ref 4, Page 6 , Item 10.1,Item10.2</p>	<p>Comprehensive audit logs to support forensic investigation.</p> <p>An alert mechanism to detect changes to audit settings.</p>
<p>Technology framework designed and implemented to ensure proactive monitoring capabilities</p> <p>Identification of the location for the sensors to collect the logs that are required to carry out the analysis and investigation</p> <p>Security analytics engine which can process the logs within reasonable time frame and come out with possible recommendations</p> <p>Deep packet inspection approaches</p> <p>Technology for improving effectiveness and efficiency (tracking of metrics, analytics, scorecards, dashboards, etc.)</p>	<p>Ref 2, Page 20, Item 5</p>	<p>To processes audit logs from a variety of database and operating system platforms, normalizing the data elements and making them ready for timely analysis and reporting.</p>
<p>For accountability purposes, a bank should ensure that users and IT assets are uniquely identified and their actions are auditable.</p>	<p>Ref 1, Page 20, Item 5.(viii)</p>	<p>To be able to audit database users and their actions.</p>
<p>Cyber Security Operations Centre should have the capacity to monitor various logs / incidents in real time / near real time.</p>	<p>Ref 2, Page 7, Item c</p>	<p>Need real time/ near real time monitoring of logs for analysis and detection.</p>
<p>Establish and implement a Security Operations Centre for centralised and coordinated monitoring and management of security related incidents.</p>	<p>Ref 2, Page 16, Item 19.6.b</p>	<p>Centralized and coordinated monitoring required.</p>
<p>Have support/ arrangement for network forensics/forensic investigation/DDOS mitigation services on stand-by</p>	<p>Ref 2, Page 17, Item 22.1</p>	<p>Network forensics capability.</p>

Core DAM requirements of RBI can be broadly classified into four categories. This paper details the RBI requirements for each category, followed subsequently by Oracle Database security recommendations for each of this category to help comply with RBI Guidelines.

1. [RBI Guidelines for Database Auditing](#)
2. [RBI Guidelines for Ensuring Audit Integrity](#)
3. [RBI Guidelines for Continuous Surveillance](#)
4. [RBI Guidelines for Monitoring Network Traffic](#)

Oracle Database security recommendations for activity monitoring and auditing include the use of database auditing (a core feature of the Oracle Database), along with Oracle Audit Vault and Database Firewall (a separately licensed product). Together, these provide a comprehensive DAM solution that help address the RBI activity monitoring requirements. Oracle Audit Vault and Database Firewall (AVDF) collects audit data from many different types of systems, monitors and analyzes network SQL traffic to databases, and takes appropriate action before the SQL reaches the database. AVDF combines native database audit logs with captured network SQL traffic and stores it in a centralized, secure warehouse for analysis and reporting. AVDF includes host-based agents for collecting audit data from multiple targets, data retention options, reporting and analysis tools, alert generation and integration with SIEM tools, an audit dashboard, and a comprehensive set of customizable reports for security and compliance. Delivered as a soft appliance, a single Audit Vault Server consolidates database audit logs and network-based database activity events from multiple databases.

AVDF Architecture diagram:



AVDF combines two complementary data streams to deliver a complete DAM solution.

- a) Native database auditing that provides a complete view of database activity along with full execution context irrespective of whether the statement was executed directly, through dynamic SQL, or through stored procedures.
- b) Network-based monitoring that is independent of the database type and requires no modification to the databases. Network-based monitoring uses the Database Firewall component of AVDF, compatible with multiple heterogeneous database systems simultaneously.

RBI Guidelines on cyber security recommend a Database Activity Monitoring solution that combines native database auditing with network-based monitoring. The rest of the paper details requirements in each of the RBI Guidelines categories, followed by recommendations involving Oracle Database auditing feature and AVDF.

1. RBI GUIDELINES FOR DATABASE AUDITING

Database auditing is an important component of Database Activity Monitoring. Database auditing involves creating and enabling database policies to track the use of database objects and users. When auditing is enabled, database activities on specified objects and users produce an audit trail of these operations. Each generates an audit record that includes what database operation was performed, the database objects involved, who performed the operation, time of execution, and the SQL statement itself.

RBI guidelines recommend tracking who did what to which piece of data, capturing when and how it was changed, and preserving the evidence for forensic investigation. Database auditing is important because there are many threats to the security of your data, including external agents trying to compromise your security and access your company data, and internal agents within your organization. The most typical security threat comes from a disgruntled or malevolent current or ex-employee who has access to the database. Auditing is crucial to find an unauthorized access emanating from an authorized user.

As auditing occurs post-activity, it does not do anything to prohibit access. Auditing helps ensure data integrity by facilitating the timely detection of security breaches, thereby mitigating risks quickly. An audited system is a deterrent against users tampering with data because it helps to identify infiltrators.

Oracle Database provides the industry's most comprehensive auditing capability, enabling the capture of detailed information. Oracle Database provides predefined audit policies that cover commonly used security-relevant audit requirements such as logon failures, database configuration parameter changes, user account and privilege management, etc. Additionally, one can create custom audit policies specific to the user, database object, privilege, role or action that needs to be audited. Build selective and effective audit policies by adding various conditions including SYS_CONTEXT and Application Context values, enabling the capture of audit information from applications.

The requirements from RBI for database auditing fall into the following categories. Subsequent sections highlight the requirements and recommendations:

- 1.1. [Sensitive Data Access](#)
- 1.2. [Access Control](#)
- 1.3. [Privileged User Access](#)
- 1.4. [Application Activity](#)
- 1.5. [Inactive User Accounts](#)
- 1.6. [Specific Components](#)

1.1. Sensitive Data Access

RBI Guidelines recommend implementing Information Security Management System (ISMS) best practices for their critical functions/processes. Adherence to ISMS Standards like ISO 27001 and ISO 27002 emphasizes the need to classify information assets (applicable to data in the database) as sensitive /critical, and establish security measures commensurate with the sensitivity and criticality of the data.

RBI Guidelines	Source	Audit Implication
<p><i>Banks need to establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g. public, confidential, or top secret) of enterprise data. This scheme should include details of data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements (criticality and sensitivity).</i></p> <p><i>... Banks also need to define and implement procedures to ensure integrity and consistency of data stored in electronic form.</i></p>	Ref 1, Page 8, item 1.j	Sensitive data classification.

<p>Maintain an up-to-date inventory of Assets, including business data/information including customer data/information, indicating their business criticality. ..</p> <p>Classify data/information based on information classification/sensitivity criteria of the bank</p> <p>Appropriately manage and provide protection within and outside organisation borders/network taking into consideration how the data/information are stored, transmitted, processed, accessed and put to use within/outside the bank's network, and level of risk they are exposed to depending on the sensitivity of the data/information.</p>	<p>Ref 2, Page 7, item 1.1, item 1.2, item 1.3</p>	
<p>Standards like ISO27001 and ISO 27002 are explicit in requiring a risk assessment to be carried out before any controls are selected and implemented and are equally explicit that the selection of every control must be justified by a risk assessment.</p>	<p>Ref 1, Page 16, item 2.2, item 2.3</p>	<p>Auditing and monitoring of data to be commensurate with its sensitivity /risk.</p>
<p>Data Leak Prevention Strategy: Develop and implement a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information.</p>	<p>Ref 4, Page 6, item 9.1</p>	
<p>Information assets have varying degrees of sensitivity and criticality in meeting business objectives. By assigning classes or levels of sensitivity and criticality to information resources and establishing specific security rules/requirements for each class, it is possible to define the level of access controls that should be applied to each information asset.</p>	<p>Ref 1, Page 17, item 3</p>	<p>Auditing of user access to sensitive data.</p>
<p>There should be controls on updating key 'static' business information like customer master files, parameter changes, etc.</p>	<p>Ref 1, Page 25, item 11.11</p>	<p>Track customer data changes in applications.</p>
<p>More sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration</p>	<p>Ref 1, Page 30, item 15.v</p>	<p>Tracking production data changes.</p>
<p>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.</p>	<p>Ref 1, Page 32, item 17.v</p>	<p>Security monitoring in proportion to the risk.</p>
<p>Banks should be proactive to identify and specify the minimum security baselines to be adhered to by the service providers to ensure confidentiality and security of data. This is particularly applicable where third party service providers have access to personally identifiable information and critical customer data.</p> <p>Discuss and agree on the instances where customer data shall be accessed and the user groups who will have access to the same. Access to a Bank's data should be strictly on a need to know basis</p>	<p>Ref 1, Page 83, item 2.v</p>	<p>Monitoring PII data/critical customer data access when outsourced.</p>

Recommendations:

Databases frequently contain sensitive data – data whose access should be controlled and monitored. Examples of sensitive data might include financial results, credit card numbers, email addresses, and personal data that describes an employee or customer.

There are a few ways to identify and categorize sensitive data in the Oracle Database. One of them is with Oracle Database Security Assessment Tool (DBSAT). DBSAT provides various reports of sensitive data summary from the scan of database metadata. A sample screenshot from DBSAT report showing sensitive columns is given below.

Schema Name	Table Name	Column Name	Column Comment	Sensitive Category	Sensitive Type	Risk Level
HCM_USER	EMPLOYEES	EMAIL	This is the email address.	IDENTIFICATION INFO – PUBLIC IDS	EMAIL ADDRESS	High Risk
HCM_USER	EMPLOYEES	EMPLOYEE_ID	This is the unique employee identifier.	JOB INFO – EMPLOYEE DATA	EMPLOYEE ID NUMBER	High Risk
HCM_USER	EMPLOYEES	FIRST_NAME	--	IDENTIFICATION INFO – PUBLIC IDS	FIRST NAME	High Risk
HCM_USER	EMPLOYEES	HIRE_DATE	--	JOB INFO – ORG DATA	HIRE DATE	Low Risk
HCM_USER	EMPLOYEES	JOB_ID	--	JOB INFO – EMPLOYEE DATA	JOB CODE	High Risk
HCM_USER	EMPLOYEES	LAST_NAME	--	IDENTIFICATION INFO – PUBLIC IDS	LAST NAME	High Risk
HCM_USER	EMPLOYEES	PHONE_NUMBER	--	IDENTIFICATION INFO – PUBLIC IDS	PHONE NUMBER	High Risk
HCM_USER	EMPLOYEES	SALARY	This is the employees salary – treat as sensitive.	JOB INFO – COMPENSATION DATA	INCOME	High Risk

Oracle Database Auditing Controls:

Once you identify sensitive data, create **object action audit policies** on access to the specific sensitive objects. The audit can include both DDL and DML statements used on the object. To learn more about object action auditing, refer to ‘**Auditing Object Actions**’ in the **Oracle Database Security Guide**.

Enforce the object action audit policies on following users:

Application service accounts: These are database users used by an application to perform a defined set of standardized business functions

Human actors: These are database users granted access to the database to generate reports, perform ad-hoc queries or otherwise interact with data.

For **application service accounts**, focus on trusted path when designing your audit policy. By trusted application path, we mean the collection of session attributes that help define access to sensitive data that is expected and within policy. For example, activity that originates from a known set of IP addresses, using a pre-approved program running as a designated operating system user. Sensitive data access through the trusted path presents a lower level of risk, and therefore needs a lower level of auditing, or may not need to be audited at all. Sensitive data access by an application service account outside of the trusted path indicates the account is being used for something other than application access, and therefore presents a higher level of risk and therefore a higher level of audit is required. Consider auditing all activity on the sensitive data by the accounts that is not within the trusted path. Consider adding the conditions for excluding the trusted path in the audit policy configuration to audit only the abnormal access by application service accounts. Using the Oracle Database conditional auditing features, construct the audit policies to capture object access that is outside of the trusted path of the application.

For **human actors** authorized to interact directly with sensitive data, a higher level of auditing is almost always appropriate. RBI Guidelines mandate direct access to the database must be restricted only to the database administrator and emphasizes that direct back-end updates to database should not be allowed except during exigencies, with a clear business need and after due authorization. If the version of your Oracle Database supports the ability to audit only the top-level SQL activities, consider auditing all top-level statements by these users, including accounts with administrative privileges, and accounts that have been granted the DBA roles.

RBI Guidelines mandate tracking access to personally identifiable information and critical customer data. Consider creating Fine-Grained Auditing (FGA) policies in the Oracle Database to audit sensitive personally identifiable information (PII) data stored in specific columns. Using FGA parameters like `audit_condition` and `audit_column`, audit behavior can be fine-tuned to target specific sensitive columns in the table and for specific conditions (for example, auditing SQL statements against the salary column only in cases where the salary amount is greater than 100,000 INR). Consider enforcing audit policies for specific users with `audit_condition` based on factors like session user from `SYS_CONTEXT` to ensure that only specific users will be audited. This will be effective for enforcing the policy for third party service providers as emphasized in RBI Guidelines. Consider configuring alerts that take effect when a user (or an intruder) violates the policy by extending the FGA

policy to send out emails when such a condition happens. Additionally, consider leveraging alerting feature in Audit Vault and Database Firewall, which allows alerts to be created and emailed, and can be integrated with a SIEM product. Refer to **'Auditing Specific Activities with Fine-Grained Auditing'** in the **Oracle Database Security Guide** for FGA configuration details.

Implementing Continuous Monitoring Controls:

To monitor continuously and detect suspicious transactions/behaviors in an effective way, leverage the following features of the Oracle Audit Vault and Database Firewall (AVDF):

1. Monitor activity on sensitive data access using **'Activity on Sensitive Data'** data privacy report, as detailed in the section [Establish Proactive Security Monitoring Practices, including Sensitive Data Access](#).
2. Define alerts on DML activity on sensitive data access events. Use alert conditions with appropriate data access audit events (INSERT, UPDATE, and DELETE) and TARGET_OBJECT to reflect the sensitive tables in the schema. Refer to [Define Alerts that are Actionable and Granular](#).
3. Monitor activity on sensitive data by privileged users by using the report **'Activity on Sensitive Data by Privileged Users'** data privacy report.

1.2. Access Control

RBI Guidelines require banks adhere to the access control principles of “least privilege”, and “need to know” commensurate with the job responsibilities, and adequate “segregation of duties”. Some of the activities that need to be closely monitored and tracked are listed below.

RBI Guideline	Source	Audit and Access Control Implications
<i>Identification of any unauthorised changes</i>	Ref 1, Page 16, item 1.4	Security control for unauthorized changes.
<p><i>Internal sabotage, clandestine espionage or furtive attacks by trusted employees, contractors and vendors are among the most serious potential risks that a bank faces. Current and past employees, contractors, vendors and those who have an intimate knowledge of the inner workings of the bank’s systems, operations and internal controls have a significant advantage over external attackers....</i></p> <p><i>Hence, access to information assets needs to be authorised by a bank only where a valid business need exists and only for the specific time period that the access is required.</i></p> <p><i>The examples where increased authentication strength may be required, given the risks involved include : administration or other privileged access to sensitive or critical IT assets, remote access through public networks to sensitive assets and activities carrying higher risk like third-party fund transfers, etc.</i></p>	Ref 1, Page 19, item 5.(i) , item 5.(ii), item 5.(v)	Ability to track internal and external user activities, including privileged access to sensitive assets.
<p><i>Conducting a risk assessment and granting access rights based on the same. For example, contractors and temporary staff would have higher inherent risks. Implementation of role-based access control policies designed to ensure effective segregation of duties.....Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment .. Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes ..Periodic reconciliation of user ids in a system and actual users required to have access and deletion of unnecessary ids,</i></p>	Ref 1, Page 20, item 5. (vi).b,c,e,f,g,h,k , item 5. (viii)	Ability to track changes to user accounts and privilege grants to spot changes and identify candidate accounts for removal.

<p><i>if any ... Audit of logging and monitoring of access to IT assets by all users... Considering de-activating user ids of users of critical applications who are on prolonged leave</i></p> <p><i>For accountability purposes, a bank should ensure that users and IT assets are uniquely identified and their actions are auditable.</i></p>		
<p>Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged...</p> <p><i>Granting privileged access on a “need-to-have” or “need-to-do” basis</i></p> <p><i>Instituting strong controls over remote access by privileged users</i></p> <p>Maintaining audit logging of system activities performed by privileged users</p> <p><i>Disallowing vendors and contractors from gaining privileged access to systems without close supervision and monitoring</i></p>	Ref 1, Page 20, item 5.(xiii)	Capture activity information of privileged users.
<p>Access should be based on the principle of least privilege and “need to know” commensurate with the job responsibilities.</p> <p><i>Adequate segregation of duties needs to be enforced.</i></p>	Ref 1, Page 25, item 11.c.10	Application access control.
<p><i>Banks use third-party service providers in a variety of different capacities. It can be an Internet service provider (ISP), application or managed service provider (ASP/MSP) or business service provider (BSP). These providers may often perform important functions for the bank and usually may require access to confidential information, applications and systems.</i></p>	Ref 1, Page 38, item 23.i	Unauthorized access by third-party service providers.
<p><i>Network access by system engineers should be monitored and reviewed closely to detect unauthorized access to the network.</i></p> <p><i>Another important security improvement is the ability to identify users at every step of their activity.</i></p>	Ref 1, Page 46, item 24.viii.r,s	Unauthorized access over network.
<p><i>Disallow administrative rights on end-user workstations/PCs/laptops and provide access rights on a need to know basis and for specific duration when it is required following an established process.</i></p> <p><i>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.) following the principle of least privileges and separation of duties.</i></p>	Ref 2, Page 11, item 8.3 ,item 8.4	User access control.

Recommendations:

Oracle Database Auditing Controls:

When a database user is granted database privileges that exceed the requirements of their job function, those privileges can be potentially abused. Frequently, administrators grant excessive privileges to avoid the risk of application failure due to lack of access privileges. Thus, users may be granted generic or default access privileges that far exceed their specific job requirements, or they may simply accumulate such privileges over time. System privileges can be very powerful, and should be granted only when necessary to roles and trusted users of the database and should be monitored very closely. RBI Guidelines emphasize the need to closely supervise users with elevated system entitlements, ensuring all their activities are logged.

Identify the system privileges that are granted to database users and which are being currently used /not used from the output of the Privilege Analysis. Refer to **‘Performing Privilege Analysis to Find Privilege Use’** in the **Oracle Database Security guide** for more details on configuration of Privilege Analysis.

Consider creating an audit policy to track all top-level activities by users who are granted roles that contain used /unused system privileges, which can be obtained from Privilege Analysis. Audit policies are enforced for users who have been granted the specified role directly or indirectly.

RBI Guidelines recommend monitoring administrator or other privileged access to sensitive or critical IT assets. Consider auditing object actions, instead of auditing the privilege use, of administrative users such as SYS. Refer to [Sensitive Data Access](#), where it is detailed.

Ensure the predefined Oracle audit configuration policy – “ORA_ACCOUNT_MGMT” is enabled in the environment to track database accounts and access modifications attempts. RBI Guidelines recommend monitoring of any modification of database access rights whenever there is a change in role or responsibility, and removal of access rights upon cessation of employment, and other account modifications like user additions and deletions.

RBI Guidelines place special emphasis on monitoring unauthorized access and changes to systems, applications or data, by third-party service providers like an Internet service provider (ISP), application or managed service provider (ASP/MSP) or business service provider (BSP). Consider using role-based access control for these user accounts to make it easy to create policies for such users. For example, one can audit all top-level activities for users granted the role “service_provider” using the **‘by users with granted roles’** clause in audit policy configuration. The role “service_provider” can be used to assign the appropriate privileges for users who are providing the managed services.

Implementing Continuous Monitoring Controls:

To monitor access controls and detect suspicious transactions/behaviors in an effective way, leverage the following features of Oracle Audit Vault and Database Firewall:

1. Track changes to user accounts and their roles/privileges using the entitlement reporting functionality contained within AVDF. Consider using the baseline comparative features within this reporting to highlight only privileges that have changed since the last report was reviewed. Refer to [Establish Proactive Security Monitoring Practices, including Sensitive Data Access](#) for details.
2. Define alerts on account modification audit events (CREATE/ DROP/ ALTER USER, CREATE/ DROP/ ALTER PROFILE). Use alert conditions with TARGET_TYPE (USER, PROFILE).
3. Create a custom report to monitor activity on sensitive data access by users who need to be closely tracked like third-party service providers. Use the **‘Activity on Sensitive Data’** data privacy report as detailed in the section [Establish Proactive Security Monitoring Practices, including Sensitive Data Access](#).

1.3. Privileged User Access

RBI Guidelines requires closely monitoring users with elevated access privileges, including system administrators, database administrators, and security officers, as mentioned below.

RBI Guideline	Source	Audit Implication
<i>System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the banking systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures</i>	Ref 1, Page 20, Item 5.(xiii)	Audit usage of system access entitlements by privileged users.
<i>Users, like system administrators, with elevated access privileges should be subjected to a greater level of monitoring in light of the heightened risks involved.</i>	Ref 1, Page 32, Item 17.(vi)	Monitoring of users with elevated privileges.

<p><i>Direct back-end updates to database should not be allowed except during exigencies, with a clear business need and after due authorization as per the relevant policy.</i></p> <p><i>Access to the database prompt must be restricted only to the database administrator.</i></p>	<p>Ref 1, Page 25, Item 11.c.16,17</p>	<p>Restriction on back-end updates to database administrator and monitoring/auditing of such activities.</p>
<p><i>Implement appropriate (e.g. centralised) systems and controls to allow, manage, log and monitor privileged/superuser/administrative access to critical systems (Servers/OS/DB, applications, network devices etc.).</i></p>	<p>Ref 2, Page 11, Item 8.5</p>	<p>Monitor and log administrative access.</p>

Recommendations:

Oracle Database Auditing Controls:

Users with elevated access privileges in the database like database administrators must be closely monitored and all their actions audited. Top-level statements (direct SQL statements executed) by users with administrative privileges (e.g. SYSDBA, SYSKM) are already audited mandatorily when the database is in the closed or mount state. When the database is open, capture all top-level actions of administrative user accounts with an audit policy configured for this activity. Turn off the audit policy during maintenance operations like upgrade /patching to reduce the audit record volume and re-enable them post the maintenance operations window. Enable the audit policy for user accounts with administrative privileges, and for accounts that have been granted the DBA roles.

All the database administrator activities happening through direct back-end updates to database (which are typically provided only to privileged users) are audited using the audit policy configuration described in the section [Sensitive Data Access](#).

Implementing Continuous Monitoring Controls:

Consider configuring the alerts for the following events in Oracle Audit Vault and Database Firewall for users with administrative privileges, and user accounts that have been granted the DBA roles: CREATE/DROP DATABASE LINK, Object Management Events like CREATE/DROP/ALTER on TABLE, VIEW, INDEX and other important administrative functions as applicable in the environment. Fine-tune the alert conditions with session attributes like Client ID so that authorized direct-access connections are filtered out and the alert is fired only on suspicious activities of users with elevated privileges.

Consider monitoring the activities of privileged users with the **'Activity on Sensitive Data by Privileged Users'** data privacy report to track any suspicious activity.

1.4. Application Activity

RBI Guidelines recommend application access to data be monitored closely and be flexible enough to accommodate any client session attributes for forensics, as mentioned in the following references.

RBI Guideline	Source	Audit Implication
<p>Application owner: <i>Establishing user access criteria, availability requirements and audit trails for their applications</i></p>	<p>Ref 1, Page 18, Item 4</p>	<p>Audit trail configuration needed for applications.</p>
<p>Application owners grant legitimate users <i>access to systems that are necessary to perform their duties and security personnel enforce the access rights in accordance with institution standards. Because of their internal access levels and intimate knowledge of financial institution</i></p>	<p>Ref 1, Page 21, Item 7.(i)</p>	<p>Internal user threat needs to be considered and actions of internal</p>

<p>processes, authorized users pose a potential threat to systems and data. Employees, contractors, or third-party employees can also exploit their legitimate computer access for malicious or fraudulent reasons. Further, the degree of internal access granted to some users can increase the risk of accidental damage or loss of information and systems.</p>		<p>users must be monitored/audited.</p>
<p>Ensuring that logs or audit trails, as required, are enabled and monitored for the applications</p> <p>Before the system is live, there should be clarity on the audit trails and the specific fields that are required to be captured as part of audit trails and an audit trail or log monitoring process including personnel responsible for the same.</p> <p>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.</p> <p>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.</p> <p>Applications must not allow unauthorized entries to be updated in the database.</p>	<p>Ref 1, Page 24,25, Item 11.c.2,3,5,6,15</p>	<p>Flexible auditing framework that allows for detailed audit logging of database activity, including failed login attempts, grants of access rights, and changes in system configuration.</p> <p>Detailed information in the audit trail including IP address, host name, and application specific auditable attributes to be captured.</p>
<p>With the advances in information technology, most banks in India have migrated to core banking platforms and have moved transactions to payment cards (debit and credit cards) and to electronic channels like ATMs, Internet Banking and Mobile Banking.</p> <p>Internet banking systems have security features such as ... upper limit on transaction value and SMS alerts to customers...</p> <p>Information security and appropriate access control procedures ensure that only employees who are required to know particular information have access to the same and can put through transactions. Further, a bank's systems need to be adequately secured to ensure that no un-authorised person carries out any system modifications/changes.</p>	<p>Ref 1, Page 113, Page 115, Item 2.e</p>	<p>Ability to monitor and audit database object changes.</p>
<p>System triggers that throw up exceptional transactions, to report suspicious transactions/behaviours are some of the techniques that are used for detection of frauds. The exceptional/suspicious transactions/activities reported through these mechanisms should be investigated in detail.</p>	<p>Ref 1, Page 116, Item 2.(iii).a.b</p>	<p>Cyber fraud detection and alerts on suspicious transactions. Integration of alerts with SIEM products</p>

<p><i>The transaction monitoring team should be responsible for monitoring various types of transactions, especially monitoring of potential fraud areas, by means of which, early alarms can be triggered.</i></p> <p><i>Banks should put in place automated systems for detection of frauds based on advanced statistical algorithms and fraud detection techniques.</i></p> <p><i>Banks can have dedicated email IDs and phone numbers for customers to report any fraudulent activity that they may notice.</i></p>		<p>for enabling analysis and notification.</p>
--	--	--

Recommendations:

Oracle Database Auditing Controls:

Follow the section [Sensitive Data Access](#) to create object action audit policies for sensitive data access and enforce the policy for application service accounts.

The Unified Audit trail captures many of the required attributes from the client sessions like CLIENT_PROGRAM_NAME and CLIENT_IDENTIFIER. For a complete list of attributes captured in Unified Audit trail, refer to the **UNIFIED_AUDIT_TRAIL** view definition in the Oracle Database Reference.

For additional application attributes like **transaction id, originator id, authorizer id, location** that the RBI Guidelines require in the audit trail, the Oracle unified_audit_trail allows customization by capturing the additional attributes in the APPLICATION_CONTEXTS column. Auditing Application context values, as referred in '**Auditing Application Context Values**' in the **Oracle Database Security Guide**, enables the capture of application context values set by the database applications, while executing the audited statement. For example, the HR module in an application can set the appropriate application context values so that any SQL operation that is audited while executing within the HR module can now contain additional information relevant to the execution context.

To set the values for an application context, create a PL/SQL package procedure that uses the DBMS_SESSION.SET_CONTEXT procedure. This is the only way that one can set application context values if the context is not marked INITIALIZED EXTERNALLY or INITIALIZED GLOBALLY. One can assign the values to the application context attributes at run time. Because the trusted procedure, and not the user, assigns the values, it is a secured application context. A sample procedure, which populates application context with attributes from gv\$sqlsession and userenv, and the audit configuration capturing the attributes in audit trail, is shown in [Application activity auditing sample](#).

In this way, one can extend the unified audit trail to capture any additional application attributes. Consider enforcing it for application service accounts.

RBI also recommends capturing unsuccessful logon attempts from application service accounts. Ensure that the Oracle pre-defined audit policy ORA_LOGON_FAILURES is enabled in the database to track unsuccessful login attempts.

RBI recommends that for the core Internet banking systems, finer controls like upper limit on transaction value and SMS alerts to customers be configured. Consider using Fine-grained auditing (FGA) policies as explained in [Sensitive Data Access](#), which allows configuring audit policies based on values in the database table, in-addition to configuring alerts using event handler. Additionally, alerting in Audit Vault and Database Firewall product could be leveraged, which allows alerts to be created and emailed and/or integrated with a SIEM product.

Implementing Continuous Monitoring Controls:

Leverage the following features of Oracle Audit Vault and Database Firewall:

1. Track failed logins from the application using the 'Failed Login Events' activity reports as shown in the sample below. The report shows the USER_LOGIN events where the Event Status is 'Failure'.

Target	User	Client IP	Event	Object	Event Status
LinuxSt	root	10.229.224.213	USER_LOGIN	root	FAILURE
LinuxSt	28696E76616C6964207573657229	10.178.49.42	USER_LOGIN	28696E76616C6964207573657229	FAILURE
LinuxSt	28756E6B6E6F776E207573657229	10.178.49.42	USER_LOGIN	28756E6B6E6F776E207573657229	FAILURE

Failed status of USER_LOGIN events

2. Create alerts with appropriate threshold and alert conditions such as EVENT_STATUS=FAILURE and EVENT_NAME=LOGIN. Consider configuring alerts based on time-period and frequency. For example, trigger an alert when there are three failed login attempts on Oracle Database target within a five-minute period.
3. Create a custom report to monitor activity on sensitive data access by application service accounts. Use 'Activity on Sensitive Data' data privacy report as detailed in the section [Establish Proactive Security Monitoring Practices, including Sensitive Data Access.](#)
4. Consider tracking transaction updates in critical systems such as Internet banking systems using 'Data Modification Before-After Values Report' to understand the before and after values of the update, as shown in the sample below.

Target	User	Event	Object	Data Modification	Event Status		
OrgOracle19c	TKGGU1	UPDATE	TAB1	Column	Old Value	New Value	SUCCESS
				F2	1	10	
				F4	10	100	
OrgOracle19c	TKGGU1	UPDATE	TAB1	Column	Old Value	New Value	SUCCESS
				F3	1	10	
				F4		10	

Old value of sensitive columns

New value of sensitive columns post Update

1.5. Inactive User Accounts

Inactive user accounts increase the attack surface of the applications and database, and can be used by an attacker as a means of entry. RBI Guidelines recommend establishing a mechanism to keep track of attempts to access deactivated accounts if any of the deactivated accounts need to still exit in the system.

RBI Guideline	Source	Audit Implication
<p><i>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.</i></p> <p><i>Banks should establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor.</i></p> <p><i>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</i></p>	<p>Ref 1, Page 32, item 17.(viii),(ix),(xi),(xii),(xiii)</p>	<p>Monitor activity on dormant account as part of security monitoring.</p>

<p><i>the dormancy. After a longer period, say 30 days, the account may be disabled.</i></p> <p><i>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.</i></p> <p><i>Banks should monitor attempts to access deactivated accounts through audit logging.</i></p>		
<p><i>Implement controls to minimize invalid logon counts, deactivate dormant accounts.</i></p>	Ref 2, Page 11, item 8.6	Track dormant accounts.

Recommendations:

Oracle Database Auditing Controls:

Consider creating user profile with 'inactive_account_time' and 'password_life_time' and associate it with user accounts. Create an audit policy to track all top-level actions on these inactive locked user accounts if any of these accounts need to still exit in the system. Use a cron job to schedule a periodic audit configuration for newer locked user accounts in the system and create new audit policies for these accounts.

Ensure pre-defined audit policy ORA_SECURECONFIG is enabled in the system. This captures executions of 'ALTER PROFILE' audit events if there is any un-authorized attempts to modify the user profile settings.

Implementing Continuous Monitoring Control:

To monitor usage of dormant accounts, leverage the '**Dormant User activity**' report in Oracle Audit Vault and Database Firewall as detailed in the section [Establish Proactive Security Monitoring Practices, including Sensitive Data Access](#).

1.6. Specific Components

RBI Guidelines recommend auditing specific components as highlighted here.

RBI Guideline	Source	Audit Implication
<i>Data transfer from one process to another or from one application to another, particularly for critical systems.... The process needs to be automated and properly integrated with due authentication mechanism and audit trails...</i>	Ref 1, Page 26, item 11.27	Audit of data transfer process in applications.
<i>Audit trails need to be available to document the conversion, including data mappings and transformations...Integrity of data.. Completeness.. Confidentiality of data.. Consistency of data..</i>	Ref 1, Page 27, item 12.(i)(ii)	Audit of data migration activity.
<i>Logging the auditing of key management-related activities</i>	Ref 1, Page 29, item 14.(iii).g	Audit of key management tasks.

Recommendations:

Data transfer process or data migration activity involving Oracle Data Pump can be audited. Consider auditing Data Pump export (expdp) and import (impdp) operations. Refer to '**Auditing Oracle Data Pump Events**' in the **Oracle Database Security Guide** for configuration details.

Data transfers/ transformations involving RMAN backup/ restore operations gets audited by default in the Oracle Database using mandatory auditing capabilities.

For auditing key management-related activities, ensure the Oracle pre-defined audit policy ORA_SECURECONFIG is enabled in the database. This policy monitors usage of ADMINISTER KEY MANAGEMENT privilege, which is used to manage keystores, encryption keys and secrets. Consider auditing for 'ACTIONS ADMINISTER KEY MANAGEMENT' to capture the audit record for every key management related activity (irrespective of usage ADMINISTER KEY MANAGEMENT privilege).

2. RBI GUIDELINES FOR ENSURING AUDIT INTEGRITY

RBI guidelines recommend audit trails be secure to ensure the integrity of the information, since that is the authoritative source of information for forensic analysis. Here are some key references.

RBI Guideline	Source	Audit Implication
<i>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.</i>	Ref 1, Page 25, item 11.c.7	Application audit data integrity.
<i>The integrity of the monitoring logs and processes should be safeguarded through appropriate access controls and segregation of duties.</i>	Ref 1, Page 32, item 17.vii	Maintaining integrity of logs.
Digital evidence is similar to any other form of legal proof - it needs to withstand challenges to its integrity,..	Ref 1, Page 16, item 1.5	Digital evidence as legal proof.
<i>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,, 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.</i> <i>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.</i>	Ref 1, Page 36, item 21.i,ii	Audit trails need to be secure to protect the integrity of the audit data. Ability to define policy for retention of audit data.
<i>E-banking systems should be designed and installed to capture and maintain forensic evidence in a manner that maintains control over the evidence, and prevents tampering and the collection of false evidence.</i>	Ref 1, Page 36, item 21.vii	Audit records must be secure from alteration or destruction.
<i>Ensuring that privileged users do not have access to systems logs in which their activities are being captured</i>	Ref 1, Page 21, item 5.(xiii).f	Block privileged user access to audit logs to ensure they do not tamper it.

<p><i>Before the system is live, there should be clarity on the audit trails and the specific fields that are required to be captured as part of audit trails and an audit trail or log monitoring process including personnel responsible for the same.</i></p>	<p>Ref 1, Page 24, item 11.c.3</p>	<p>Ensure there is agreement on what audit data should be captured and how that audit data should be maintained.</p>
--	------------------------------------	--

Recommendations:

Oracle Database auditing stores audit records in a secure schema within the audited database. Oracle Audit Vault and Database Firewall extends this protection by moving the audit data into a separate secure repository that is protected from access by database administrators.

Unified Auditing in Oracle Database is inherently secure at source. Unified Audit records are written to AUDSYS.AUD\$UNIFIED, which is a read-only table. Hence, DMLs are not permitted on the unified audit trail views. Even DML and DDL operations on the underlying dictionary tables from AUDSYS schema are not permitted. Any attempt to directly delete or update contents of AUD\$UNIFIED fails as shown in the below figure, and generates an audit record.

```
SQL> connect / as sysdba
Connected.
SQL> truncate table audsys.aud$unified;
truncate table audsys.aud$unified
*
ERROR at line 1:
ORA-46385: DML and DDL operations are not allowed on table
"AUDSYS"."AUD$UNIFIED".
```

Attempts to modify the data or metadata of the unified audit internal table are mandatorily audited. Because these attempts should be considered inherently suspicious, consider creating alerts for them in AVDF.

Audit data can only be managed using the built-in audit data management package "DBMS_AUDIT_MGMT". Audit data cannot be directly updated or removed using UPDATE or DELETE SQL commands. Oracle Database mandatorily audits all executions of the DBMS_AUDIT_MGMT PL/SQL package procedures.

Oracle Database facilitates separation of duties by providing two separate audit-related roles: AUDIT_ADMIN and AUDIT_VIEWER.

AUDIT_ADMIN can configure auditing both unified audit policies and fine-grained audit policies and do administrative tasks pertaining to auditing, such as purging the audit trail. This role also contains the ability to view and analyze audit data. Typically, this role is granted to security administrators.

AUDIT_VIEWER can view and analyze audit data only and not create audit policies or truncate the audit trail. Typically, this role is granted to auditors or security analysts.

The AUDSYS schema user, where Unified Audit trail resides cannot be logged into, as shown below. Thus, Oracle Database auditing stores audit records in a schema that is protected from update and delete operations, only allowing purging of the audit trail using the AUDIT_ADMIN role.

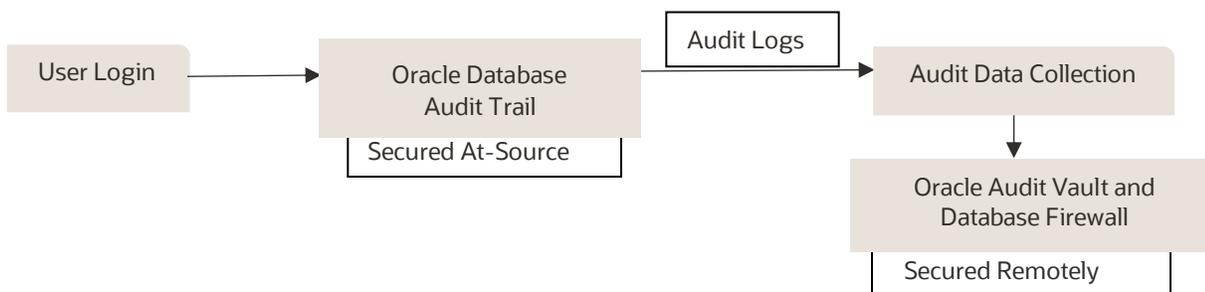
```
SQL> show user
USER is "SYS"
SQL> alter user audsys identified by Oracle123 account unlock;
User altered.
SQL> grant create session to audsys;
Grant succeeded.
SQL> connect audsys/Oracle123@cdb
ERROR:
ORA-46370: cannot connect as AUDSYS user
Warning: You are no longer connected to ORACLE.
```

To ensure further integrity of audit data, key fields of unified audit records can be written to SYSLOG utility (on UNIX platforms) or to the Windows Event Viewer (on Windows) by enabling the UNIFIED_AUDIT_SYSTEMLOG parameter. The fields in SYSLOG uniquely identify the detailed unified audit records in the UNIFIED_AUDIT_TRAIL view.

Consider encrypting audit data tablespaces with Transparent Data Encryption (TDE). Consider protecting the Unified Audit table with a Database Vault realm. It is a good practice to create a Database Vault realm around AUDSYS.AUD\$UNIFIED table so that only authorized administrators can access the Unified Audit trail and even users with SYSDBA privileges cannot access unless they are part of realm authorization list.

As a best practice recommendation, forward the audit data from its source to a remote centralized location where the individuals whose activities are audited, cannot purge the data. By removing audit data from the source Oracle Database and storing it in the secured remote location like Oracle Audit Vault and Database Firewall (AVDF) appliance, we can protect the integrity and reliability of the audit data and prove that it has not been tampered with.

AVDF is a secure data warehouse of audit data, with a highly scalable and secure repository that stores the audit data. Timely transfer of audit data from source audit trails to Audit Vault server is critical to close the window on intruders who may attempt to modify audit data and cover their tracks. Audit Vault transfers audit data on a near real time basis using the Audit Vault Agent. Audit Vault encrypts data during transmission using industry standard TLS. Audit Vault protects audit data using Oracle's industry leading database security technology. The repository is an embedded Oracle Enterprise Edition Database that includes numerous Oracle technologies, including automatic storage management (ASM), compression, partitioning, encryption, Database Vault, and privileged user controls.



AVDF uses a data warehouse schema called AVSYS. Audit data and network-based database activity event data is stored in the AVSYS.EVENT_LOG table. The AVSYS account is locked in the Audit Vault database. The Audit Vault database uses Oracle Database Vault to protect the AVSYS schema, and hence the Database Vault account manager can only unlock it. In order to do so you have to login to the Audit Vault server using root password (this is set during the AVDF installation) and then switch user to the Database Vault account manager. Thus, multiple layers of access control makes the access to the AVSYS schema very restricted.

The AVSPACE tablespace containing the AVSYS schema in the Audit Vault server's repository is automatically encrypted using Transparent Data Encryption (TDE). Hence, even archived event data is encrypted. AVDF protects audit trails with a combination of encryption and strong access controls.

To enhance the integrity of audit and network data stored in AVDF, adhere to the guidelines outlined in '**General Security Guidelines**' of the **Audit Vault and Database Firewall Administrator's Guide**.

Retention of audit trails can be configured per-database target to allow for varying business requirements. For critical systems like E-banking or core banking systems, the retention period for online and archived data can be defined to be much longer than non-critical systems. Refer to '**About Archiving and Retrieving Data in Oracle Audit Vault and Database Firewall**' in the **Audit Vault and Database Firewall Administrator's Guide** for details on configuration.

3. RBI GUIDELINES FOR CONTINUOUS SURVEILLANCE

Providing a centralized monitoring and management console for accelerating analysis, incident response, reporting, forensic investigation, and for demonstrating regulatory compliance is a vital component of a Database Activity Monitoring solution. RBI Guidelines recommend continuous surveillance and proactive security monitoring practices to detect unusual activity patterns in the database and over the network, and establish escalation and communication processes to contain security incidents.

RBI Guidelines that recommend centralized auditing, monitoring, reporting, and alerting of anomalous activity on the database are listed here, followed by recommendations on how Oracle Audit Vault and Database Firewall(AVDF) can be used to meet these requirements.

RBI Guideline	Source	Monitoring and Alerting Implication
<p><i>Developing and implementing processes for preventing, detecting, analyzing and responding to information security incidents</i></p> <p><i>Establishing escalation and communication processes and lines of authority</i></p> <p><i>Establishing the capability to investigate information security incidents through various modes like forensics, evidence collection and preservation, log analysis, interviewing, etc.</i></p> <p><i>Developing a process to communicate with internal parties and external organizations (e.g., regulator, media, law enforcement, customers</i></p> <p><i>Common incident types include, but not limited to,, unauthorised access to systems, identity theft, data leakage/loss, malicious software and hardware, failed backup processes, denial of service attacks and data integrity issues.</i></p> <p><i>A bank needs to have clear accountability and communication strategies to limit the impact of information security incidents through defined mechanisms for escalation and reporting ..</i></p>	<p>Ref 1, Page 23, item 10.(ii).a.b.d.e,</p> <p>Item 10.(iii), item 10.(iv)</p>	<p>Audit data must be collected and preserved to support forensic investigation.</p> <p>Ability to send out alerts and report on issues.</p>
<p>Potential security weaknesses / breaches (for example, as a result of analyzing user behaviour or patterns of network traffic) should be identified.</p>	<p>Ref 1, Page 25, item 11.c.13</p>	<p>Support identification of potential breaches, including unusual patterns of access to the database.</p>
<p><i>Concerns over the need to better control and protect sensitive information have given rise to a new set of solutions aimed at increasing an enterprise's ability to protect its information assets. ... data leak prevention (DLP). It provides a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework. Most DLP solutions include a suite of technologies that facilitate three key objectives:</i></p> <ul style="list-style-type: none"> <i>Locate and catalogue sensitive information stored throughout the enterprise</i> 	<p>Ref 1, Page 30, item 15.xi</p>	<p>Monitoring access to sensitive information.</p> <p>Audit policies relating to sensitive data needs to be created.</p>

<ul style="list-style-type: none"> • Monitor and control the movement of sensitive information across enterprise networks • Monitor and control the movement of sensitive information on end-user systems 		
<p>Robust monitoring processes in place to identify events and unusual activity patterns. The strength of the monitoring controls needs to be proportionate to the criticality of an IT asset. Alerts would need to be investigated in a timely manner.</p> <p>Common monitoring processes include activity logging (including exceptions to approved activity), for example, device, server, network activity, security sensor alerts; monitoring staff or third-party access to sensitive data/information...</p> <p>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.</p>	<p>Ref 1, Page 31, item 17.(i),(ii),(xv)</p>	<p>Ability to identify unusual activity patterns, and generate alerts.</p> <p>Need to track access to sensitive data.</p>
<p>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.</p> <p>Network and host activities typically are recorded on the host and sent across the network to a central logging facility which may process the logging data into a common format. The process, called normalization, enables timely and effective log analysis.</p>	<p>Ref 1, Page 36, item 21.(i),(iv)</p>	<p>Database activity monitoring and auditing, along with the ability to monitor SQL traffic and store in a central place is needed.</p> <p>The solution should support heterogeneous databases, and support reporting and alerting.</p>
<ul style="list-style-type: none"> • All remote access to an internal network, ... • Operating systems should be configured to log access control events ... without the appropriate permissions • identify anomalies in logs and actively review the anomalies, • Network boundary devices, including firewalls, network-based IPSs, and inbound and outbound proxies may be configured to log verbosely all traffic (both allowed and blocked) arriving at the device 	<p>Ref 1, Page 36, item 21.(v)</p>	<p>Ability to identify users accessing the database remotely, and identify anomalies in access patterns and alert on events. In addition, audit logs from OS should also be captured.</p>
<p>Given the multiplicity of devices and systems, banks should consider deploying a Security Information and Event Management (SIEM) system tool for log aggregation and consolidation from multiple machines/systems and for log correlation and analysis..</p>	<p>Ref 1, Page 37, item 21.(vi)</p>	<p>Ability to forward alerts to the SIEM for aggregation and correlation.</p>
<p>Security monitoring arrangements should provide key decision-makers ... with an informed view of aspects like the effectiveness and efficiency of information security arrangements..</p> <p>Analysis performed as part of security monitoring and reporting arrangement may include</p>	<p>Ref 1, Page 37/38, item 22.(i),(iii),(iv),(v),(vi),(vii)</p>	<p>Ability to monitor SQL traffic and log it, along with database activity in a centralized way giving key decision makers a dashboard view is important. Ability to</p>

<p>...Details relating to information security incidents and their impact...</p> <p>Operational security statistics, such as firewall log data.....</p> <p>Information collected as part of security reporting arrangements should include details about all aspects of information risk like criticality of information, identified vulnerabilities and level of threats, potential business impacts and the status of security controls in place.</p> <p>Metrics can be an effective tool for security managers to discern the effectiveness of various components of their security policy and programs...</p> <p>The use of metrics needs to be targeted towards the areas of greatest criticality.</p> <p>A comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators, can be devised.</p>		<p>support ad-hoc analysis and reporting is required.</p>
<p>The first step in an investigation process is gathering the entire transaction details, documents and complete details of the customer/employee or vendor. In order to investigate into suspected cases, the group would adopt various advanced techniques including computer forensics, forensic accounting and tools to analyse large volumes of data.</p>	<p>Ref 1, Page 117, item 2.(iii).a</p>	<p>Fraud investigation requires analyzing large volumes of data with ability to store and archive data, so that historical data can also be considered as part of the forensic analysis.</p>
<p>Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.</p>	<p>Ref 2, Page 9, item 4.7</p>	<p>Database Activity Monitoring to detect unusual activity within your databases and send alerts to SIEM so that notifications can be sent to administrators for taking remedial actions.</p>
<p>Manage and analyse audit logs in a systematic manner so as to detect, understand or recover from an attack.</p>	<p>Ref 2, Page 14, item 16.2</p>	<p>Manage audit logs from multiple sources (databases, operating systems, firewall traffic), and store and analyze them to detect and understand an attack.</p>
<p>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.</p>	<p>Ref 2, Page 14, item 17.1</p>	<p>Database auditing should contain the necessary information to uniquely identify the source of activity and detect any audit setting changes.</p>
<p>Arrangement for continuous surveillance - Setting up of Cyber Security Operation Centre (C-SOC):</p> <ul style="list-style-type: none"> Ability to Provide real-time/near-real time information on and insight into the security posture of the UCB 	<p>Ref 4, Page 9, item 1.1</p>	<p>Database auditing and network-based activity monitoring are a key part of continuous surveillance, preserving evidence of who did what, when they</p>

<ul style="list-style-type: none"> • Ability to know who did what, when, how and preservation of evidence • Integration of various log types and logging options into a Security Information and Event Management (SIEM) system,... • <i>Able to monitor the logs of various network activities and should have the capability to escalate any abnormal / undesirable activities.</i> • <i>Key Responsibilities of C-SOC could include:</i> <ul style="list-style-type: none"> ○ <i>Monitor, analyse and escalate security incidents</i> ○ <i>Develop Response - protect, detect, respond, recover</i> ○ <i>Conduct Incident Management and Forensic Analysis</i> 		<p>did it, and where they did it.</p>
<p><i>Ensure proactive monitoring capabilities aligned with the banking technology risk profile</i></p> <p><i>Security analytics engine which can process the logs within reasonable time frame and come out with possible recommendations</i></p> <p><i>Deep packet inspection approaches</i></p>	<p>Ref 4, Page 9, item 1.2</p>	<p>Ability to quickly collect various audit logs centrally for processing, making it available for analysis and alerting. Additionally, there is a need to process and analyze SQL traffic.</p>
<p><i>Develop a comprehensive set of metrics that provides for prospective and retrospective measures, like key performance indicators and key risk indicators....</i></p> <p><i>Have support/ arrangement for network forensics/forensic investigation....</i></p>	<p>Ref 4, Page 10, item 4.1,item 4.2</p>	<p>Support forensic investigation, including correlation of activity across different databases.</p>

Recommendations:

Oracle Audit Vault and Database Firewall (AVDF) provides a comprehensive Database Activity Monitoring solution by collecting and consolidating audit data, monitoring and logging network traffic, policy management, raising alerts, and providing detailed reports for forensic and compliance purposes. Salient features of Oracle Audit Vault and Database Firewall include:

- a) Audit Data Collection from databases and policy provisioning
 - Collection and consolidation of audit data from Oracle and non-Oracle databases
 - Audit data collection from operating systems, file systems, and directory services
 - Display and provisioning of Oracle Database audit policies
 - Monitoring user entitlement changes and stored procedure changes for Oracle Database
- b) SQL traffic monitoring and analysis
 - Monitoring SQL traffic over the network using Database Firewall
 - Securing targets from SQL Injection attacks
 - Selectively allowing or blocking SQL traffic based on whitelists or blacklists
- c) Sensitive data activity tracking within the database and validating SQL statements before they reach the database
- d) Powerful, customizable alerts

- Alerting and Notifications based on audit data collected
 - Ability to customize and create powerful alerts based on frequency of actions, and composite conditions based on the audit data collected
- e) Reporting
- Reporting for forensics and compliance tracking
 - Ability to customize and run ad-hoc reports
 - Scheduling of reports with email based notification
- f) Audit data archiving
- g) Integration with SIEM products
- h) High availability and reliability, supporting the needs of large enterprises for continuous monitoring and auditing

Best practice recommendations to build an effective continuous surveillance solution, to help comply with RBI Guidelines, fall in the following categories:

- 3.1. [Configure Integrated Security Monitoring](#)
- 3.2. [Create Selective and Focused Audit, Firewall and Alert Policies](#)
- 3.3. [Define Alerts that are Actionable and Granular](#)
- 3.4. [Establish Proactive Security Monitoring Practices, including Sensitive Data Access](#)

Subsequent sections highlights the recommendations:

3.1. Configure Integrated Security Monitoring

RBI Guidelines lay equal emphasis on database auditing as well as tracking suspicious behavior of users over the network. It is therefore necessary to configure both database audit collection and network monitoring, which can be done using Oracle Database auditing along with AVDF to provide a comprehensive solution, which covers both Oracle and non-Oracle databases, operating systems and directory audit logs. The table shows how database auditing and network monitoring complement each other and are therefore mandatory in establishing an effective security monitoring solution.

	Database Auditing	Network Monitoring
Purpose	Support regulatory compliance and audit privileged user activities, providing guaranteed audit trail to enable control	Identify SQL-injection attempts and other unauthorized activity, enforce corporate data security policy
Information Captured	Who, what, where, when Before/After values Full execution and application context	Who, what, where, when
Pathways Monitored	All: stored procedures, direct connections, scheduled jobs, operational activities	Network
Impact on database	Requires native database auditing, performance impact determined by the amount of audit data being produced	Completely independent of database resources, negligible performance impact

Steps for configuring and implementing Database Audit collection and Network monitoring:

- a) Identify the targets to monitor
 - Audit trails supports audit data collection from a broad spectrum of targets, including
 - Database audit trails from Oracle Database, Microsoft SQL Server, MySQL, SAP Sybase and IBM DB2 for LUW. The audit data can be collected from audit tables or files.
 - Before/After values from REDO records of Oracle databases.
 - OS audit trails from Oracle Linux, Oracle Solaris, Microsoft Windows, and IBM AIX.
 - Microsoft Active Directory audit trails.
 - File systems such as Oracle ACFS.
 - Custom audit data in either database tables or XML files. Audit data for custom applications can be collected and reported.
 - Refer to '**Supported Secured Targets**' in the **Audit Vault and Database Firewall Installation Guide** for the list of targets and their versions supported.
 - Network trails support a broad set of database targets
 - By configuring the database firewall in proxy mode, network traffic to/from Oracle Database, Microsoft SQL Server, SAP Sybase, IBM DB2, and MySQL can be monitored and blocked if needed. Refer to '**Database Firewall Protection: Supported Secured Target Types and Versions**' in the **Audit Vault and Database Firewall Installation Guide** for the list of targets and their versions supported.
 - Host monitor, which captures SQL traffic from the network card and sends it over the network to a Database Firewall, can also be used for monitoring SQL traffic, but this cannot be used for blocking. The platforms where host monitor is supported, is listed in '**Host Monitor: Supported Platforms and Versions**'.
- b) Configure data retention policies for each target based on data sensitivity and corporate retention rules
 - Retention policies determine how long data is retained in the Audit Vault Server and can be used for reporting, after what time period should the data be archived, and for how long archived data can be brought back into the Audit Vault Server for reporting and forensics. Retention policies may be different for different databases monitored by the same Audit Vault and Database Firewall.
 - Refer to '**About Archiving And Retrieving Data In Oracle Audit Vault And Database Firewall**' in the **Audit Vault and Database Firewall Administrator's Guide** for configuration details.
- c) Enforce segregation of duties
 - AVDF supports two types of users: **Auditors and Administrators**.
 - Auditors can configure and provision audit policies and firewall monitoring policies for databases, as well as define, generate, and access audit reports and alerts.
 - Administrators can configure basic network and host settings for the targets, start and stop Audit Vault Agents and Database Firewalls, and configure and monitor Audit Vault Server operation. Administrators do not have access to audit information and cannot create audit policies /firewall monitoring policies.
 - A single user can have only the auditor or administrator role.
 - Within the two role categories, further separation of duties can be defined. A subset of database targets can be assigned to individual auditors and administrators, ensuring that segregation of duties is possible not only by role, but by the targets that they are allowed access to.
 - Refer to '**Managing User Accounts and Access**' in the **Audit Vault and Database Firewall Administrator's Guide** for configuration details.

3.2. Create Selective and Focused Audit, Firewall and Alert Policies

Be selective on what you want to audit in the database or log based on the network traffic and create alerts only on the events of interest. Fine-tuning the policies and creating targeted alerts reduces false positives (alerts where no attack exists) and false negatives (no alert when an attack does take place). While false negatives are obviously a concern, false positives can also hinder detection. When security personnel are overwhelmed with the number of alerts which are false positives, their review of alerts may be less effective thereby allowing real attacks to be reported but not suitably acted upon. RBI emphasizes the need to ensure the detection capability is adequate and effective. Three categories of policies that needs to be fine-tuned are:

a) Audit policies

Follow the recommendations highlighted in [RBI Guidelines for Database Auditing](#) to make the audit policy configuration granular and conditional.

b) Firewall policies

Follow the recommendations highlighted in [Firewall Policy](#) to make the Firewall policy configuration selective.

c) Alert policies

Follow the recommendations highlighted in [Define Alerts that are Actionable and Granular](#) to ensure alerts are specific to the conditions of interest and are targeted.

3.3. Define Alerts that are Actionable and Granular

RBI recommends establishing escalation and communication processes in the event a security incident has occurred. Alerts are a useful mechanism for defining events of interest.

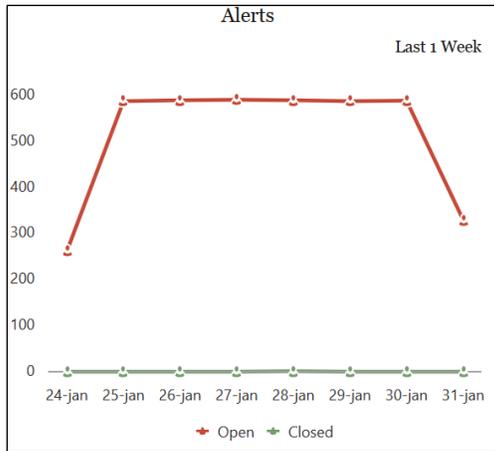
AVDF provides the ability to detect and alert on activities that may indicate attempts to gain unauthorized access to systems and/or abuse system privileges. It lets you define rule-based alerts on audit records, whether these records come from the native database audit trail, or are collected from the network by the Database Firewall. Database Firewall policies can be configured to generate alerts on network activity, providing an early-warning detective control for potential malicious activity. AVDF continuously monitors the events collected, evaluating the activities against defined alert conditions and generating an alert if the condition is met. Alerts can be associated with any database event including system events such as changes to application tables, creating privileged users, or events when someone attempts to access to sensitive business information. Any actions that are blocked by an Oracle Database Vault policy also generate an audit event on top of which an alert can be created.

Alert management capability in AVDF can be used to create alert definitions that raise alerts on the auditor's dashboard and send notifications to users for investigation. Alerts can be defined specifying a Boolean condition using SQL comparison operators (=, <, LIKE, IN, NULL, and so on) and logical operations (NOT, AND, OR) using the fields in the audit record, as shown in the screenshot below. Refer to **'Creating Alerts'** in the **Audit Vault and Database Firewall Auditor's Guide** for details on alert configuration.

Alert Name	Tracking All DBA Activity on Sensitive Schema	Type	Oracle Database
Severity	Critical	Threshold (times)	1
Duration (min)	0	Group By (Field)	- Select Field -
Description		Condition	<pre>upper(:TARGET_OWNER)='EMPLOYEESEARCH_PROD' AND upper(:TARGET_OBJECT) IN ('DEMO_HR_EMPLOYEES', 'DEMO_HR_SUPPLEMENTAL_DATA') AND UPPER(:EVENT_NAME) NOT IN ('SELECT') AND upper(:USER_NAME) IN ('DBA_DEBRA', 'DBA_HARVEY', 'DBA_NICOLE', 'EVIL_RICH', 'P U_PETE')</pre>
Status	Enabled		

Flexibility to create conditional alerts

Additionally, the AVDF dashboard provides graphical summaries of alerts as shown below. These include a summary of alert activity. Consider using the alert trend in the auditor's dashboard for analyzing the risk trends over time.



For reporting, alerts can be grouped by source, event category, and severity (warning or critical) as shown below so the security personnel can focus on high priority alerts first.

Target	Alert Policy Name	Alert Status	Alert Severity	User	Alert Time	Event Time
pdb1	Tracking All DBA Activity on Sensitive Schema	New	Critical	DBA_NICOLE	12/3/2019 12:32:06 PM	12/3/2019 12:32:03 PM
pdb1	Tracking All DBA Activity on Sensitive Schema	New	Critical	DBA_NICOLE	12/3/2019 12:32:06 PM	12/3/2019 12:32:03 PM
pdb1	Tracking All DBA Activity on Sensitive Schema	New	Critical	DBA_NICOLE	12/3/2019 12:32:06 PM	12/3/2019 12:32:03 PM

Consider configuring notifications for the generated alerts. For example, you can set up an email to be automatically sent to a user, such as a security officer, or to a distribution list. Alerts can also be forwarded to syslog. This is useful if you want to integrate AVDF with another system like the enterprise SIEM. Refer to **'Responding to an Alert'** in the **Audit Vault and Database Firewall Auditor's guide** for information on configuring notifications.

3.4. Establish Proactive Security Monitoring Practices, including Sensitive Data Access

RBI recommends banks have continuous surveillance and robust monitoring processes in place to identify suspicious events and unusual activity patterns. Use AVDF reports to establish continuous monitoring practices in your environment.

AVDF reports can be used to monitor a wide range of activities including privileged user activity on the database server, changes to database structures, and SQL statements on the network that are executed on the database server. Reports are based on the consolidated audit information from databases, operating systems, and directories, providing a holistic view of activities across the enterprise. In addition, reports can include information on database account management, roles and privileges, object management, and stored procedure changes.

Auditors can access reports interactively through a web interface, or generate PDF or XLS reports. The console's easy-to-use interactive browsing provides the ability to create color-coded charts and graphs. Columns of interest within the report can be sorted, filtered, re-ordered, added, or removed. Rules can automatically highlight specific rows so that users can quickly spot suspicious or unauthorized activity. PDF and XLS report definitions can be used to schedule automatic generation of reports, which can be delivered via e-mail attachments or URLs. Reports can also be defined to require attestation by auditors. Users can easily create new or customize PDF and XLS report templates to meet specific compliance and security requirements.

Audit Vault Server provides optimal performance by expediting report generation with the help of Oracle Database In-Memory feature, using which audit data can be stored in memory based on the selected date range, enabling reports to run faster. Furthermore, the Audit Vault Server repository schema is documented and accessible, enabling integration with third-party reporting solutions.

Various categories of built-in reports are available, including:

- a) Activity Reports
- b) Summary Reports
- c) Compliance Reports

a) Activity Reports:

Activity reports as shown below track database access activities such as audited SQL statements, application access activities, and user logins. Specialized activity reports also cover failed logins, user entitlements, before-after data modifications, changes to application tables, and database schema changes.

Activity Reports	
Summary	
Report Name	Report Description
All Activity	All audited and monitored events
Data Access & Modification	
Report Name	Report Description
Data Access	Details of read access events
Data Modification	Events that led to Data modification
Data Modification Before-After Values	Data modification events with before and after values in Oracle database
Login & Logout Events	
Report Name	Report Description
Failed Login Events	Failed Authentication attempts
Login and Logout	All successful login and logout events
Startup and Shutdown	System startup and shutdown events

Entitlement reports as shown below describe the types of access that users have to an Oracle Database, providing information about the users, roles, profiles, and privileges used. These reports are useful for tracking unnecessary access to data, finding duplicate privileges, and simplifying privilege grants. An entitlement snapshot captures the state of user entitlement information at a specific point in time. The snapshot contains the metadata of users and roles that a user has to the Oracle Database: system and other SQL privileges, object privileges, role privileges, and user profiles. An entitlement report job can be scheduled such that it periodically takes a snapshot of the user entitlements at specified intervals. After an entitlement snapshot is generated, you can compare different snapshots to find how the entitlement information has changed over time.

Entitlement Reports	
Name	Description
Privileged Users	Privileged users
User Accounts	Summary of User accounts
User Privileges	Summary of User privileges
User Profiles	Summary of User profiles
Role Privileges	Summary of Role privileges
System Privileges	System privileges and their grants to users
Object Privileges	Object privileges and their grants to users

Stored Procedure Audit reports helps track changes made to the stored procedures. There are common attack patterns that replace a stored procedure with a procedure containing malicious code. Stored procedure auditing is an essential part of protecting your database against attack.

Correlation Reports helps correlate events on the database with the Linux OS user for Oracle Database targets running on Linux. This is useful in cases where this OS user runs a shell or executes a command on the database as another user by using su or sudo.

Database Firewall reports provide detailed event information on the SQL traffic to the monitored databases. For example, details of SQL statements that had alerts enabled or were blocked can be seen. General information about SQL traffic to the databases can be seen, including statement type (DDL, DML, etc.), database username, OS username, client application name, client IP address, and Database Firewall action and threat level.

These Database Firewall reports as shown below, along with the other built-in audit reports provide a complete understanding of the security and compliance status of the database environment.

Database Firewall Reports	
Name	Description
Database Firewall Monitored Activity	Database Firewall events grouped by Client IP and Database
Blocked Statements	SQL statements blocked by Database Firewall
Database Traffic Analysis by OS User	Database Firewall events grouped by OS User and Database
Invalid Statements	SQL statements marked as INVALID by Database Firewall
Warned Statements	SQL statements marked as WARN by Database Firewall

A sample Database Firewall report, giving detailed information on the SQL traffic that is blocked by firewall policy rule is shown below.

Event Time	Target	Client IP	User	Command Text	Threat Severity	Action Taken	Policy Name
11/29/2019 3:08:53 PM	pdb1	10.0.0.19	EMPLOYEESEARCH_PROD	select a.USERID, a.FIRSTNAME, a.LASTNAME, a.EMAIL, a.PHONEMOBILE, a.PHONEFIX, a.PHONEFAX, a.EMPTYPE, a.POSITION, a.ISMANAGER, a.MANAGERID, a.DEPARTMENT, a.LOCATION, a.STARTDATE, a.ENDDATE, a.ACTIVE, a.COSTCENTER, b.FIRSTNAME as MGR_FIRSTNAME, b.LASTNAME as MGR_LASTNAME, b.USERID as MGR_USERID from DEMO_HR_EMPLOYEES a left outer join DEMO_HR_EMPLOYEES b on a.MANAGERID = b.USERID where 0=0 and upper(a.POSITION) like 'OR 0=0--%' order by a.LASTNAME, a.FIRSTNAME	major	block	3-Block Unseen HR Application Statements with DBA Exception, and monitor Data Modifications

SQL traffic that is blocked by firewall policy

b) Summary Reports:

These set of reports contain trend charts, anomaly reports and various summaries by target (DDL summary, activity summary, failed login summary) as shown below. These reports can be used to quickly review characteristics of user activity on specific targets or across the enterprise. These reports can be used to identify anomalies such as new and dormant user and client IP anomalies over time. Activities by new users, or previously dormant users, can be analyzed for potential account hijacking.

Trend Charts	
Anomaly Reports	
Name	Description
New or Dormant User Activity	Activity by newly created or dormant users
New or Dormant Client IP Activity	Activity from newly seen or dormant client IPs
All Activity Reports	
Name	Description
Activity Summary by Client IP and OS User	Events grouped by OS User and Client IP
Activity Summary by Target	Events grouped by Target
DDL Activity Summary by Target	Schema changes grouped by Target
DML Activity Summary by Target	Data modifications grouped by Target
Failed Logins Summary by Target	Failed authentication attempts grouped by Target

The report below shows a “Dormant User activity” report where there was a recent activity by a Linux user account that was dormant since July 31, 2019.

Activity of users in the last days that are new or dormant since for Target

New or Dormant User activity

There has been flurry of activity in the last 5 days by user 'sourbasu' who has been otherwise dormant since 31/7/2019

User	Target	Target Class	Total Events ↓
sourbasu	LinuxSt	OS	3

c) Compliance Reports:

Standard out-of-the-box audit assessment reports are available and help to meet regulations such as:

- Data Privacy Reports (GDPR)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Sarbanes-Oxley Act (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Data Protection Act (DPA)
- IRS Publication 1075

One of the out-of-the-box compliance reports is the Data Privacy Report (GDPR) as listed above. Oracle Audit Vault complies with data protection directives and regulations by offering capabilities like centralized auditing, monitoring, reporting, and alerting of anomalous activity on the database. It also reports on the sensitive data in the database targets as well as any access to sensitive data by all users including privileged users.

RBI Guidelines strongly recommend locating and cataloging sensitive information. RBI Guidelines also recommend closely monitoring and controlling the movement of sensitive information across enterprise networks and on database systems.

AVDF allows importing information on sensitive data into its repository, thereby helping track activities on sensitive data using the Data Privacy Reports. Refer to '**Importing Sensitive Data Into Repository**' in the **Audit Vault and Database Firewall Auditor's Guide** for importing sensitive data discovery results from DBSAT /Oracle Enterprise Manager into AVDF.

Once the information on sensitive data has been imported, Data Privacy Reports, as shown below can be used to closely monitor access to sensitive data:

Name	Description	Schedule	Generated Report
Sensitive Data	Details of sensitive data		
Access Rights to Sensitive Data	User's access rights to sensitive data		
Activity on Sensitive Data	Activity on sensitive data by all users		
Activity on Sensitive Data by Privileged Users	Activity on sensitive data by privileged users		

A sample report showing sensitive data discovered in a specific target is shown below.

Target	Schema Name	Object	Object Type	Column Name	Sensitive Type
pdb1	EMPLOYEESEARCH_PROD	DEMO_HR_EMPLOYEES	TABLE	ADDRESS_1	FULL ADDRESS
pdb1	EMPLOYEESEARCH_PROD	DEMO_HR_EMPLOYEES	TABLE	ADDRESS_2	FULL ADDRESS
pdb1	EMPLOYEESEARCH_PROD	DEMO_HR_EMPLOYEES	TABLE	CC_PIN	CARD SECURITY PIN
pdb1	EMPLOYEESEARCH_PROD	DEMO_HR_EMPLOYEES	TABLE	COUNTRY	COUNTRY
pdb1	EMPLOYEESEARCH_PROD	DEMO_HR_EMPLOYEES	TABLE	DOB	DATE OF BIRTH
pdb1	EMPLOYEESEARCH_PROD	DEMO_HR_EMPLOYEES	TABLE	EMAIL	EMAIL ADDRESS
pdb1	EMPLOYEESEARCH_PROD	DEMO_HR_EMPLOYEES	TABLE	FIRSTNAME	FIRST NAME
pdb1	EMPLOYEESEARCH_PROD	DEMO_HR_EMPLOYEES	TABLE	LASTNAME	LAST NAME

Sensitive data in pdb1 database target

A sample report showing activity on sensitive data is shown below.

Target	User	Client IP	Event	Object	Sensitive columns	Event Status	Event Time	Comment
pdb1	SYS	192.168.122.1	GRANT	DEMO_HR_EMPLOYEES	ADDRESS_1, ADDRESS_2, CC_PIN, COUNTRY, DOB, EMAIL, FIRSTNAME, LASTNAME, NINO, POSTAL_CODE, SALARY, S...	SUCCESS	12/4/2019 6:01:16 PM	grant select on employeesea... joseph_d
pdb1	DBA_NICOLE	10.0.0.150	REVOKE	DEMO_HR_EMPLOYEES	ADDRESS_1, ADDRESS_2, CC_PIN, COUNTRY, DOB, EMAIL, FIRSTNAME, LASTNAME, NINO, POSTAL_CODE, SALARY, S...	SUCCESS	12/4/2019 6:01:15 PM	revoke update on employeesea... jack, mike, jim, jon
pdb1	DBA_NICOLE	10.0.0.150	REVOKE	DEMO_HR_EMPLOYEES	ADDRESS_1, ADDRESS_2, CC_PIN, COUNTRY, DOB, EMAIL, FIRSTNAME, LASTNAME, NINO, POSTAL_CODE, SALARY, S...	SUCCESS	12/4/2019 6:01:15 PM	revoke update on employeesea... jack, mike, jim, jon

SQL traffic details on sensitive data access captured in the report

Through these Data Privacy reports, AVDF can closely monitor the movement and access of sensitive information in the database and over the network. Enforcing controls on the access and movement of sensitive data over network can be configured using Database Firewall in proxy deployment as detailed in [Increase scrutiny of sensitive data access over network](#).

Refer to 'Reports' in the **Audit Vault and Database Firewall Auditor's guide** for in-depth details on the reports that are available in AVDF to closely monitor and track activities.

4. RBI GUIDELINES FOR MONITORING NETWORK TRAFFIC

Network traffic monitoring is an important component of Database Activity Monitoring. With near-zero overhead on the monitored databases, network-based Database Activity Monitoring requires no modification to the databases, and can monitor multiple heterogeneous database systems simultaneously. Network-based Database Activity Monitoring should be used in conjunction with database auditing so that not only local activity on the database can be captured, but also any database activity that doesn't cross the network as SQL, such as logging local or remote console connections, to make database and user changes. An effective Database Activity Monitoring solution needs to combine native database auditing with network-based monitoring for detecting intrusions.

One can classify the RBI Guidelines for network traffic monitoring into following three categories:

- 4.1. Network Segmentation
- 4.2. Deployment Topology
- 4.3. Firewall Policy

In this section, we will examine how the Database Firewall component of AVDF can help address the requirements outlined in the RBI Guidelines.

4.1. Network Segmentation

RBI Guidelines recommend multiple layers of defense, known as defense in depth and highlights that at the minimum, banks should consider protecting the perimeter and computing environment. It emphasizes that effective security deployment requires carefully configured boundary defenses that separate networks with different threat levels, different sets of users, and different levels of control. Effective multi-layered defense of perimeter networks help to lower the number of successful attacks, allowing security personnel to focus on attackers who have devised methods to bypass boundary restrictions. The following references in the RBI Guidelines highlight the importance of segmenting networks and building boundary defenses.

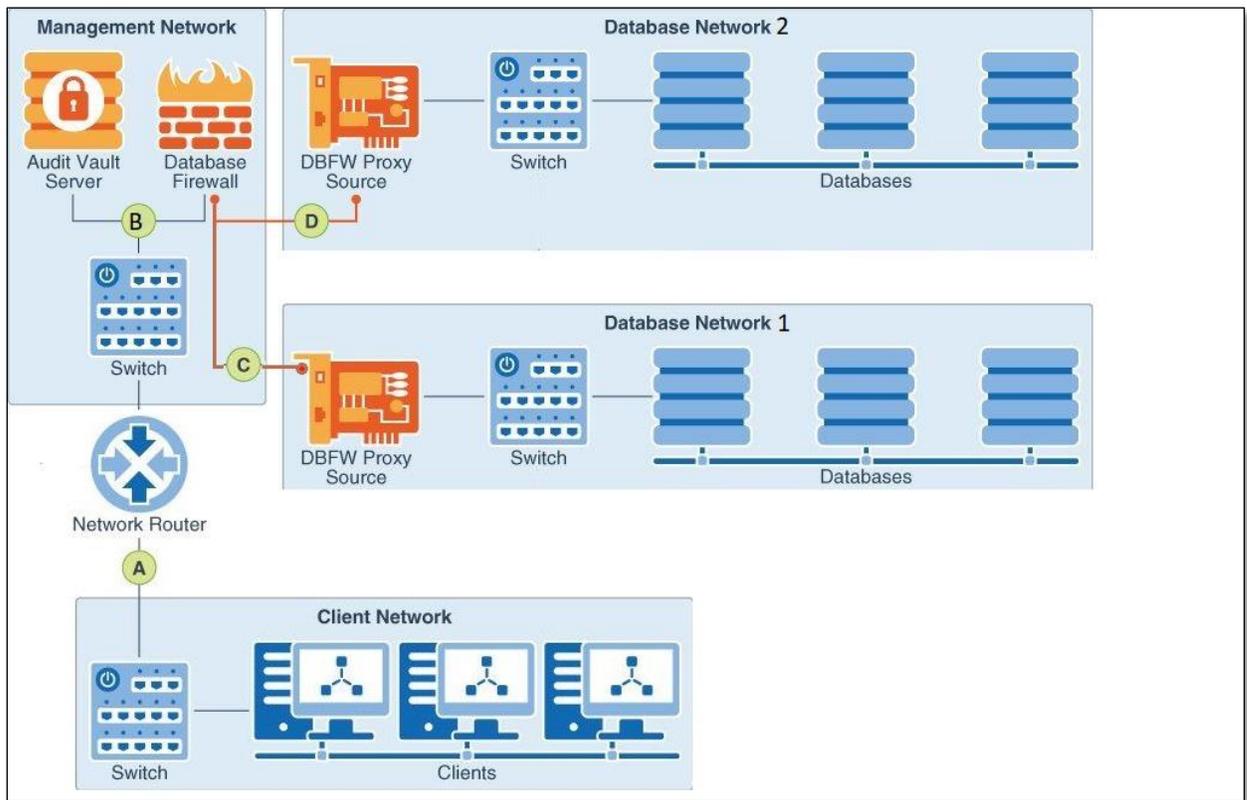
RBI Guideline	Source	Network Monitoring Implication
<p><i>Defense in depth for most organizations should at least consider the following two areas:</i></p> <p><i>(a) Protecting the enclave boundaries or perimeter</i></p> <p><i>(b) Protecting the computing environment.</i></p> <p><i>An effective approach to securing a large network involves dividing the network into logical security domains. A logical security domain is a distinct part of a network with security policies that differ from other domains and perimeter controls enforcing access at a network level.</i></p>	Ref 1, Page 39, item 24.iv	Ability to support network traffic monitoring of databases, which are in distinct enclave boundaries.
<p><i>Network configuration considerations could include</i></p> <ul style="list-style-type: none"> ○ <i>Identifying the various applications and systems accessed via the network...</i> ○ <i>Determining the most appropriate network configuration to ensure adequate security and performance for the bank..</i> ○ <i>Minimizing access to less-trusted domains and employing encryption and other controls for less secure connections</i> 	Ref 1, Page 39, item 24.v	Ability to enforce different policy rules (including blocking/monitoring levels) for less trusted domains.

Some applications and business processes may require complete segregation from the corporate network, for example, preventing connectivity between corporate network and wire transfer system.		
Critical infrastructure of UCB (viz., NEFT, RTGS, SWIFT, CBS, ATM infrastructure) should be designed with adequate network separation controls	Ref 3, Page2, Item 4.4	Ability to support network separation by providing a monitored ingress point for database traffic.

Recommendation:

If databases are located on different subnets (logical security domains), Database Firewall can use different network interface into each of them for outbound connections from Database Firewall.

In proxy deployment mode, ensure that all database clients connect to the Database Firewall, which in turn connects to the database servers in different logical security domains using the corresponding network interfaces. Proxy mode of deployment supports blocking of SQL traffic in-addition to monitoring and is ideal for enforcing strict access control for less-trusted domains. In the diagram below, databases are segmented into two logical security domains, Database Network 1 and Database Network 2.



A SQL statement between the client application and database server goes through the following steps.

- A:** The clients connect to the Database Firewall Traffic Proxy through the Network Router.
- B:** The extracted SQL data from the client traffic is analyzed and sent to the Audit Vault Server based on the Database Firewall policy.
- C:** The traffic is forwarded to the target database in logical security domain1 by the Database Firewall over proxy source, which represents the network interface for domain1.
- D:** The traffic is forwarded to the target database in logical security domain2 by the Database Firewall over proxy source, which represents the network interface for domain2.

The response from the database is returned to the Database Firewall, and then through the Network Router to the client. The management network is separate from database networks.

The firewall can be configured to run in proxy mode (where the client traffic goes through the firewall), or in out-of-band mode or in host-monitor mode. In out-of-band/ host-monitor deployment mode, the Database Firewall receives a copy of the database traffic for monitoring and is not in-line with the traffic from the clients. Hence, in this configuration the database firewall can only be used for monitoring and not blocking. As part of the configuration, ensure that the host-monitor deployed within the logical security domains is able to forward the traffic to the Database Firewall and connect to the Audit Vault server. Consider out-of-band /host-monitor deployment mode when you want to monitor the traffic, and there are other network perimeter controls to ensure stricter access (such as blocking) to the less-trusted domains.

For database systems requiring complete segregation from the rest of the corporate network due to the sensitivity of data, consider having a dedicated Database Firewall appliance instance for the specific security domain.

4.2. Deployment Topology

RBI Guidelines specify the firewall types to choose from, and recommend selecting a firewall type based on characteristics of the security zone, such as the amount of traffic, the sensitivity of the systems and data, and applications, as stated in references below:

RBI Guideline	Source	Database Firewall Implication
<p><i>Financial institutions have four primary firewall types from which to choose: packet filtering, stateful inspection, proxy servers, and application-level firewalls. Any product may have characteristics of one or more firewall types. The selection of a firewall type is dependent on many characteristics of the security zone, such as the amount of traffic, the sensitivity of the systems and data, and applications.</i></p> <ul style="list-style-type: none"> ○ <i>Packet Filter Firewalls</i> ○ <i>Stateful Inspection Firewalls....</i> ○ <i>Proxy Server Firewalls</i> ○ <i>Application-Level Firewalls....</i> 	<p>Ref 1, Page 40, item 24.vii.a</p>	<p>To be able to classify the firewall as one of the RBI recommended firewall types.</p>

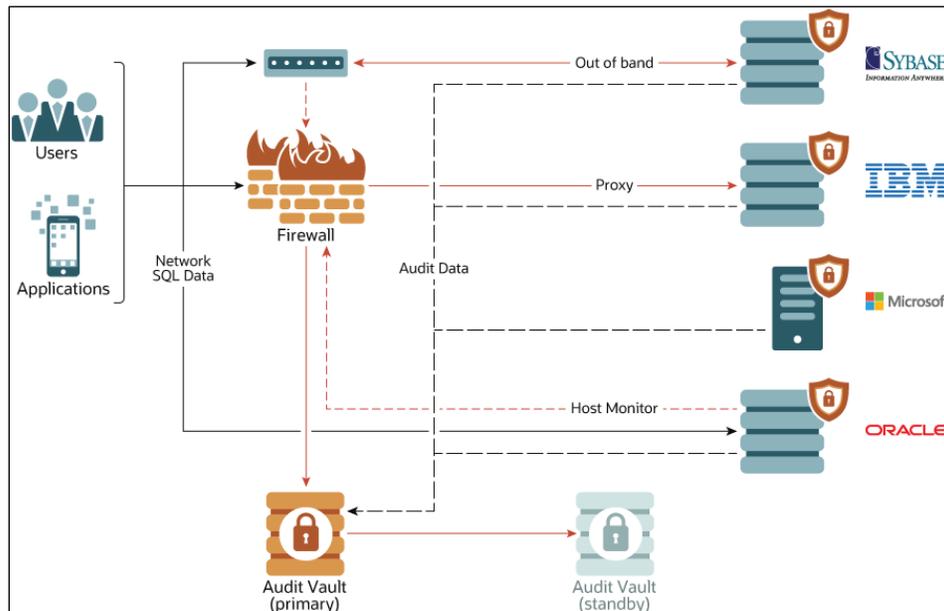
Recommendation:

There are three deployment modes for Database Firewall. The capabilities of the firewall, and characteristics of its implementation, are dependent on the deployment mode.

- a) Proxy: One can configure Database Firewall in proxy mode such that all traffic to the database server is routed through the Database firewall. The proxy mode of deployment supports both active and passive monitoring of database activity. In this deployment mode, the Database Firewall can monitor and alert on SQL traffic, and can block or substitute SQL statements as specified in the policy.
- b) Out-of-Band: In this mode of monitoring, the Database Firewall receives a copy of the network traffic, including client requests to the database and the database's response to those requests. Use spanning ports, network taps, or packet replicators to copy database traffic to the firewall. In this mode, the Database Firewall can monitor and alert on SQL traffic, but cannot block or substitute SQL statements.
- c) Host Monitor: This is a specialized application of out-of-band. Database Firewall supports a local server-side collection agent called the Host Monitor. This agent captures SQL traffic reaching the database server and securely

forwards it to Database Firewall, effectively functioning as a packet replicator. In this deployment mode, the Database Firewall can monitor and alert on SQL traffic, but cannot block or substitute SQL statements.

These deployment modes are represented in the diagram below.



Proxy deployment mode:

In this mode, the Database Firewall is in-line with the SQL traffic and the clients connect to the Database Firewall over TCP. The Database Firewall makes an outbound connection to the database and forwards the SQL traffic only if the incoming requests are allowed by the firewall policy. In this mode, the Database Firewall is an intermediary between internal and external IP addresses. Hence, in proxy deployment mode, the Database Firewall acts as a combination of Proxy Server and Application Firewall for the SQL traffic. Other controls, including traditional network firewalls or Database Vault should be used to block direct access to the database that attempt to bypass the Database Firewall.

Database Firewall supports the following protocols:

- Oracle DB: Transparent Network Substrate (TNS)
- MS SQL Server: Tabular Data Stream Protocol (MS-TDS)
- Sybase: TDS
- MySQL: MySQL
- DB2: DARDA V5 specification (Distributed relational database architecture)

As a database proxy, the Database Firewall can understand and validate client properties including client IP address, program module, and operating system user. The Database Firewall is not a general-purpose proxy, for instance there is no access to information about packets nor caching capability. As an application firewall, the Database Firewall can understand and validate database commands and offers logging capability as well as additional screening of the SQL statements. Database Firewall policies are used to enforce access control, for example, allow only certain users access database from specified IP addresses.

Host Monitor/ Out-of-band deployment mode:

In this mode, the Database Firewall receives a copy of database traffic, and can be configured only for monitoring and alerting on network SQL traffic. Hence, the Database Firewall does not behave as an application firewall because it is not in-line with the database traffic. This deployment mode cannot be used to enforce access control.

Consider using the proxy mode of deployment for very critical or sensitive database systems, which in addition to monitoring and alerting, need a stricter prohibition of unauthorized activities at a layer closer to where the sensitive data

resides. This would constitute the last layer of defense in a defense-in-depth protection strategy of highly secured domains with strictly enforced access controls.

Non-proxy mode of deployment is recommended for database systems which are relatively less critical, or have other complementary perimeter protection devices like filtering routers, web application firewall, gateways which already have the capability to enforce stricter access control including blocking traffic.

All three modes of deployment (Proxy, Out-of-Band and Host Monitor) can monitor SQL traffic encrypted with Oracle Native Network encryption for Oracle Databases.

4.3. Firewall Policy

RBI Guidelines emphasize the need for an effective firewall policy management to make sure that the IT infrastructure is secured against unauthorized and potentially harmful traffic. Using a database firewall effectively requires creating and establishing intelligent and targeted firewall policy decisions. A firewall policy dictates how Database Firewall should handle SQL traffic for specific IP addresses, address ranges, protocols, applications, and content types (e.g., session content) based on the organization’s information security policies. RBI Guidelines pertaining to structuring an effective firewall policy are listed below.

RBI Guideline	Source	Firewall Policy Implication
<p><i>A firewall policy states management’s expectation for how the firewall should function and is a component of the overall security management framework. Acceptable inbound communication types for the organization need to be explicitly defined in the firewall policies. ...</i></p> <p><i>At a minimum, the policy should address various aspects like Firewall topology and architecture and type of firewalls being utilized, physical placement of the firewall components, permissible traffic and monitoring firewall traffic,, responsibility for monitoring and enforcing the firewall policy, protocols and applications permitted, regular auditing of a firewall’s configuration and testing of the firewall’s effectiveness, and contingency planning.</i></p> <p><i>Given the importance of firewalls as a means of access control, good firewall related practices include:</i></p> <ul style="list-style-type: none"> ➤ Using a rule set that disallows all inbound and outbound traffic that is not specifically allowed .. ➤ <i>Restricting network mapping capabilities through the firewall, primarily by blocking inbound ICMP (Internet Control Messaging Protocol) traffic</i> ➤ Logging activity, with daily administrator review and limiting administrative access to few individuals ➤ <i>Using security monitoring devices and practices to monitor actions on the firewall and to monitor communications allowed through the firewall</i> 	<p>Ref 1, Page 41, item 24.vii.a</p>	<p>To be able to reject any SQL traffic not explicitly allowed and log SQL traffic as specified in the policy.</p>
<p><i>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.</i></p>	<p>Ref 1, Page 25, item 11.c.6</p>	<p>To capture unsuccessful logon attempts and access to sensitive data.</p>

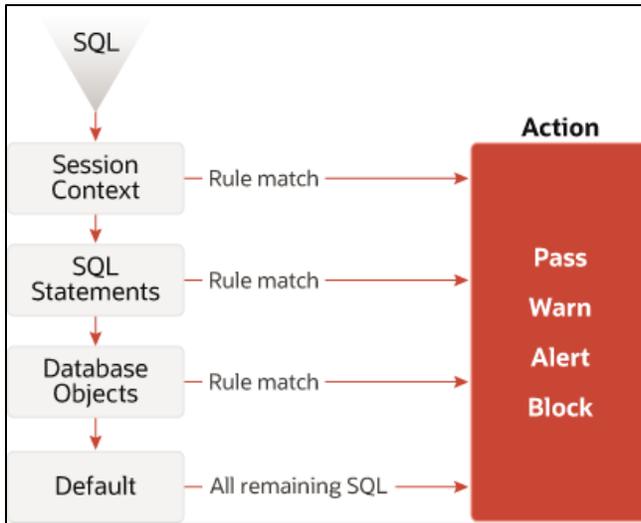
<p><i>Banks' networks should be designed to support effective monitoring. Design considerations include network traffic policies that address the allowed communications between computers or groups of computers, security domains that implement the policies, sensor placement to identify policy violations and anomalous traffic, nature and extent of logging, log storage and protection..</i></p> <p><i>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.</i></p>	<p>Ref 1, Page 32, item 17.iii, v</p>	<p>To detect and block anomalous database traffic.</p>
<p><i>Network boundary devices, including firewalls, network-based IPSs, and inbound and outbound proxies may be configured to log verbosely all traffic (both allowed and blocked) arriving at the device</i></p>	<p>Ref 1, Page 37, item 21.v.e</p>	<p>Ability to configure logging of all traffic that passes through the firewall.</p> <p>To be able to monitor traffic across the network boundary.</p>
<p><i>Banks use third-party service providers in a variety of different capacities. It can be an Internet service provider (ISP), application or managed service provider (ASP/MSP) or business service provider (BSP). These providers may often perform important functions for the bank and usually may require access to confidential information, applications and systems.</i></p>	<p>Ref 1, Page 38, item 23.i</p>	<p>To report on third-party service provider activities within the database.</p>
<p><i>Firewalls: The main purpose of a firewall is access control. By limiting inbound (from the Internet to the internal network) and outbound communications (from the internal network to the Internet), various attack vectors can be reduced.</i></p>	<p>Ref 1, Page 40, item 24.vii.a</p>	<p>To block any communications not explicitly allowed.</p>
<p><i>Network access by system engineers should be monitored and reviewed closely to detect unauthorized access to the network.</i></p>	<p>Ref 1, Page 46, item 24.viii.r</p>	<p>Close scrutiny on system engineers by constructing policies specific to these users.</p>
<p><i>Banks may sometimes provide employees, vendors, and others with access to the institution's network and computing resources through external connections.</i></p> <p>Logging remote access communications, analyzing them in a timely manner, and following up on anomalies...</p> <p><i>.. subject the inbound and outbound network traffic to appropriate perimeter protections and network monitoring</i></p> <p>Logging and monitoring the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access</p> <p><i>Implementing controls consistent with the sensitivity of remote use. For example, remote use to administer sensitive systems or databases may include the controls like restricting the use of the access device by policy and configuration,...</i></p>	<p>Ref 1, Page 46, item 25.i, item 25.iii.h,i,j,l</p>	<p>Enabling remote access with greater monitoring along with logging. All details such as IP, user, time, etc. needs to be captured.</p>
<p><i>Instituting strong controls over remote access by privileged users</i></p>	<p>Ref 1, Page 20, item 5.(xiii).b</p>	<p>Privileged user remote access monitoring to be done using policies specific to these users.</p>

Comprehensively address network and database security: ... 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.	Ref 2, Page 3, item 9	To be able to reject unauthorized access patterns, and alert on those as needed.
Consider implementing whitelisting of authorised applications / software/libraries, etc Mechanism to block /prevent and identify installation and running of unauthorised software/applications	Ref 2, Page 8, item 2.1,item 2.2	Allow whitelisting of applications, network addresses, and operating system users for controlling access to databases protected by the firewall.
Have mechanism to automatically identify unauthorised device connections to the bank's network and block such connections. Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints. Security Operation Centre to monitor the logs of various network activities and should have the capability to escalate any abnormal / undesirable activities	Ref 2, Page 9, item 4.6, item 4.7, item 4.9	Close supervision of network access and creation of policies that alert on unusual access.
Implement controls to minimize invalid logon counts, deactivate dormant accounts. Monitor any abnormal change in pattern of logon.	Ref 2, Page 11, item 8.6, item 8.7	Monitors invalid logins and detect changes in logon patterns.
Consider implementing whitelisting of internet websites/systems. Consider implementing secure web gateways with capability to deep scan network packets including secure (HTTPS, etc.) traffic passing through the web/internet gateway	Ref 2, Page 14, item 13.3, item 13.4	Ability to whitelist and create policies is needed.
Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints. Firewall rules shall be defined to block unidentified outbound connections, reverse TCP shells and other potential backdoor connections .	Ref 4, Page 7, item 1.1, item 1.2	To detect unusual activities in databases.

Recommendation:

RBI recommends that a good firewall practice should disallow all inbound traffic that is not specifically allowed or permitted—traffic that is not needed by the organization. This practice, known as **deny by default**, decreases the risk of attack. **Whitelisting** is a *deny by default* approach. Because of the dynamic nature of hosts, networks, protocols, and applications, deny by default (i.e. whitelisting) is a more secure approach than permitting all traffic that is not explicitly forbidden (i.e. blacklisting). To set up a whitelist policy, create a policy that monitors “normal” user behavior and use the observed SQL traffic to create whitelist policies.

The Database Firewall policy is a combination of different rules like Session Context Rules, SQL Statement Rules, Database Object Rules and Default Rules. Database Firewall in AVDF is a multi-stage Firewall policy rule-processing engine as shown below in the diagram. The rule processing happens sequentially with the first match determining the appropriate action.



a) **Session Context Rules:**

Session context rules based on whitelisting approach, provides a powerful means of controlling SQL requests based on known sets of session attributes. These rules override all other policy rules and determine the action, logging level and threat severity to use when certain session activity is observed. Session attributes that can be used are the following:

Session Attributes Sets	Description
IP Address Sets	Specified set of IP addresses of database clients
Database User Sets	Specified set of database user login names
Database Client Sets	Specified set of client programs
OS User Sets	Specified set of operating system user names

Consider creating **'Session Context rules'** to allow specific traffic from trusted application paths without needing them to go through further processing in the Database Firewall policy engine (e.g. SQL requests from a trusted set of whitelisted client IPs). Combining multiple sets (for example, IP with database user or IP with OS user) provides flexibility in narrowing down the permitted traffic through the Database Firewall. Any traffic, which does not fit the whitelist, is subjected to monitoring or blocking using a combination of Action, Logging, Threat Severity and Escalation.

A sample session context rule is shown below, that allows the SQL traffic from specific set of whitelisted DBA users (as configured in the set 'Allow DBAs') to pass through the firewall policy.

Set Action, Logging Level and Threat Severity values commensurate with the risk level of session attributes being used. For instance, a policy that whitelists database users (e.g. DBA users) from whitelisted client IP address set can have 'Action=Pass, Logging Level=Unique, Threat Severity=Minimal'. However, if there were database users corresponding to third-party service providers, even if the SQL request comes from whitelisted client IP address set, we would want to monitor them closely. The Action, Logging Level and Threat Severity values can be set to 'Action=Alert, Logging Level=Always, Threat Severity=Moderate' to always alert on their access. With increasing risk proposition, alter these settings to a more rigorous logging strategy.

b) SQL Statement rules:

SQL Statement rules are executed after the session context rules. The Database Firewall automatically captures, analyzes the actual SQL traffic and classifies similar SQL statements into groups known as clusters. Consider creating whitelists of SQL Cluster sets and specify Action, Logging level and Threat severity for each SQL cluster set in the analyzed SQL policy rule. Whitelists of "normal" behavior could also be automatically created by running the Database Firewall in training mode with **Log Unique** default policy (where it logs unique SQL statement) and capturing a set of expected SQLs representing normal traffic, such as the set of SQL generated in a test or QA system.

A sample SQL Statement rule is shown below, that allows a trained set of SQL statements from HR application to access the database (as configured in the set 'Normal HR Application SQL').

<input type="checkbox"/>	Rule Name	Profile Name	Cluster Sets	Action	Logging Level	Threat Severity	Description
<input type="checkbox"/>	Expected HR Application Traffic	Authorized HR Application Access	Normal HR Application SQL	pass	log_unique	insignificant	Expected SQL Traffic from HR Application to protected database

Allow the trained SQL traffic as specified in the set 'Normal HR Application SQL'

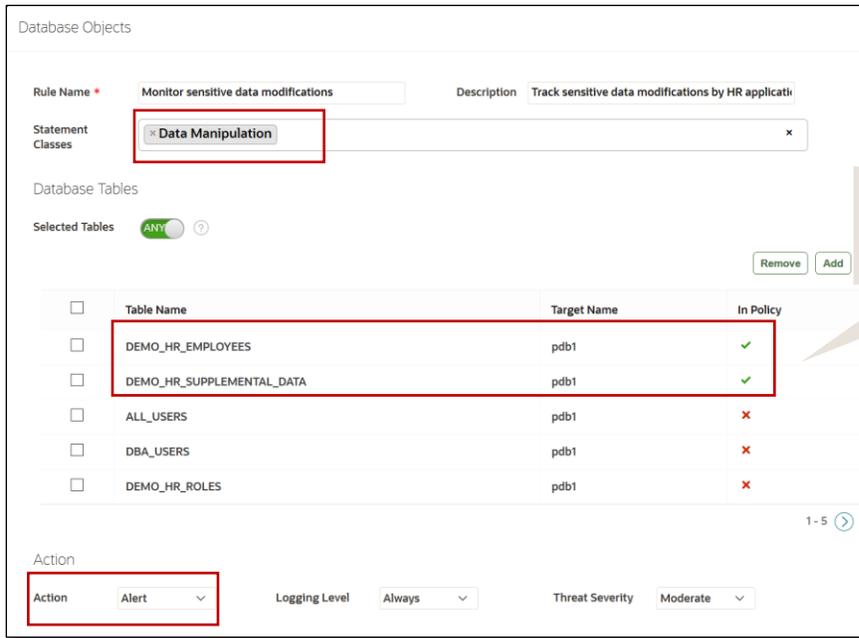
It is recommended to use SQL Statement firewall policy rules only when all the trusted application paths accessing the database are well known, including the expected SQL traffic. Any anomaly in the SQL network traffic, which is not yet profiled, can be captured with this rule. Utilize this firewall policy rule for databases with highly sensitive and/or critical IT assets, especially for applications accessible over the public internet.

c) Database Object rules:

Database Object rules can be used to prevent or allow specific types of SQL statements (DML, DCL, etc.) acting on specific database objects such as tables and views. Consider these rules to increase scrutiny of sensitive data access over network. Database object rules let you closely monitor network activities on sensitive tables in the database. These rules can prevent or allow specific types of SQL statements acting on specific database tables. For instance, allow only SELECTS on application tables but warn/alert if there are attempts to perform data modification on sensitive application tables.

These rules are often used for controlling behavior of privileged users over the network where it might be necessary to stop them from accessing specific sensitive application database objects.

A sample database object rule is shown below, that raises an alert if SQL traffic has any DML activity (insert, update or delete) on any of the two sensitive tables.



Alert if there is any DML activity on any of the two sensitive tables

d) Default rule:

The default Rule is a catch-all rule where SQLs that does not match any of the above rules are acted upon. In the whitelisting approach, it is recommended to alert with major threat severity so that any unseen SQL traffic is alerted on and marked as actionable. In highly critical systems, consider using a blocking/ blocking-with-substitution action after the firewall is trained to understand all the normal expected traffic.

A sample Default rule is shown below which blocks all unseen SQL traffic.

Block and alert unseen SQL traffic

Rule Name	Action	Logging Level	Threat Severity
Default Rule	block	log_always	major

The various rules are explained in detail in **'Database Firewall Deployment'** in the **Audit Vault and Database Firewall Concepts Guide**.

Consider incorporating the following firewall policy configuration best practices to help comply with RBI Guidelines:

1. Allow specific whitelisted SQL traffic using Session Context rules

Whitelist based on trusted application path as discussed earlier and consider incorporating combination of session attributes in the whitelisting rules. Consider incorporating the following:

- a) Whitelist the client IP addresses that are authorized to access the database systems. For instance, corporate network addresses that trusted clients will use to access the database. Any remote access not originating from whitelisted client IP addresses warrants a higher level of scrutiny as indicated in RBI Guidelines and can be configured to send an alert or be blocked.
- b) Whitelist the database client programs that are authorized to connect to the database over specific client IP address.
- c) Whitelist the database users (application service accounts) expected from the client IP addresses accessing the database systems using authorized client programs. Consider creating a combination of client IP address, database users (application service accounts) and database client programs.

- d) While application service account's access from known set of client IP address from known database client may present a low risk, it is essential to detect unusual activities in case this account is hijacked or misused by employees with knowledge of the credentials. Consider using an escalation policy in Session Context rules to detect any anomaly.

A sample escalation policy is shown below, that allows SQL traffic to pass the firewall. But if the same SQL traffic is seen multiple times (as configured in threshold), the SQL traffic is blocked and replaced with a substitution SQL statement.

The screenshot shows a configuration window for an escalation policy. At the top, the 'Action' is set to 'Pass', 'Logging Level' is 'One-Across-Ses', and 'Threat Severity' is 'Minimal'. A red box highlights the 'Set threshold for escalating action' section, which is checked. Below it, 'Threshold' is set to 3, 'Threshold Time (in seconds)' is 120, and 'Threshold Action' is 'Block'. A 'Substitution SQL' field contains the text 'select 100 from dual where 1=2'. A callout box points to the threshold settings with the text: 'Block and substitute the SQL statement only if it is seen 3 times in 120-second window'.

- e) Database administrators are frequently given direct /SSH access to the database server. Database and operating system auditing should be used to closely monitor their activities. For remote database access, it is imperative to monitor and closely review the activity by these privileged administrators, especially if there is any deviation from normal pattern of access. Consider monitoring the following actions of these privileged administrators over the network:
- o If the privileged database users are accessing over the network from the whitelisted client IP addresses. Generate an alert with setting (Action =Warn, Logging Level=Unique) and indicate the threat severity to a level that is actionable.
 - o If privileged database users are accessing from non-whitelisted client IP address, further firewall policy rules like Database Object rules, SQL Statement rules and Default Rules can factor in increased scrutiny of their actions.
 - o Repetitive SQLs attempts by privileged database users from whitelisted client IP addresses firing the same SQL in specified threshold can be flagged as potential anomaly by creating an escalation policy where Logging Level and Threat Severity can be increased.
- f) If there are third party service providers in the system (differentiated by specific OS user/database user), subject them to a higher level of scrutiny as indicated in RBI Guidelines even if their access is through whitelisted client IP address. Recommend not whitelisting these users.

2. Increase scrutiny of sensitive data access over network

Access to sensitive objects in the database system always warrants higher scrutiny if it is not through established application trusted paths as indicated by RBI Guidelines. Some of the use-cases that need to be alerted, as indicated in the RBI Guidelines include

- a) Administration or other privileged access to sensitive or critical IT assets
- b) Remote access through public networks to sensitive assets and activities carrying higher risk like third-party fund transfers
- c) Third-party access to sensitive data/information
- d) Any modifications in sensitive master data

Consider choosing an escalation policy to change the action settings if there are repeated attempts. For instance, while privileged users doing SELECTS on sensitive application tables can potentially be flagged as a low risk, recommend alerting if there are repetitive attempts in a specific threshold time.

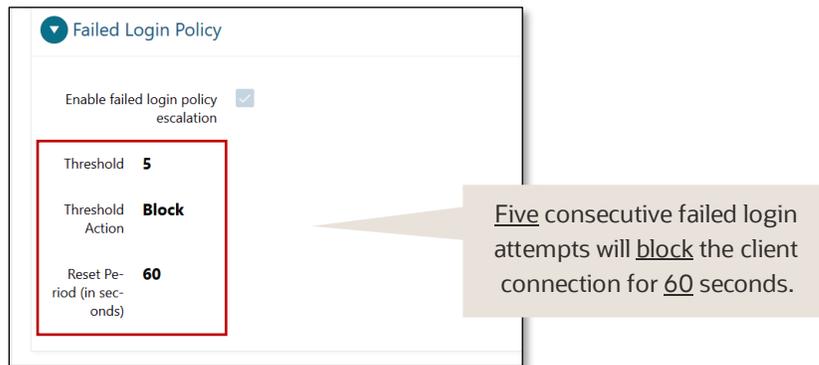
3. In the default rule, block or rigorously monitor all traffic

Use the default rule to block / monitor with 'Action=Alert, Threat Severity=Major' for all the traffic reaching this final Default rule to ensure the SQL traffic is monitored rigorously.

4. Use firewall policy rules to detect abnormal login attempts

RBI recommends minimizing invalid logon counts. These actions are typical of Denial-Of-Service attacks or intruders attempting to gain access to authorized system using brute-force attempts. If the database users are non-existent in the Oracle Database, audit events will not be generated for failed login attempts even with ORA_LOGON_FAILURES predefined policy. With Database Firewall, one can detect these login attempts using failed login policy settings.

A sample policy configuration is show below, that detects five consecutive failed login attempts and blocks the client connection for a minute.



Consider following these best practices for enabling logging in Database Firewall policy:

- a) Be selective in what you log
- b) Log all SQL for users with elevated privileges
- c) Set Policy action to 'Pass' regular application activity
- d) Log SQL only for sensitive activity from applications
- e) Use threat levels to prioritize events

The Database Firewall sends the captured firewall events to the Audit Vault Server. There is a default alert policy rule called 'Database Firewall Alert', which processes all the firewall events in 'Warn' or 'Block' status (as determined by the Action in the firewall policy rules), and generates alerts.

A sample alert report is shown below, that provides the details of the alerted SQL traffic using the default firewall alert policy.

Alerts							
Manage Alert Status							
	Target	Alert Policy Name	Alert Status	Alert Severity	User	Alert Time ↓	Event Time
<input type="checkbox"/>	pdb1	Database Firewall Alert	New	Warning	EMPLOYEESEARCH_PROD	12/5/2019 10:07:10 PM	12/5/2019 10:04:53 PM
<input type="checkbox"/>	pdb1	Database Firewall Alert	New	Warning	EMPLOYEESEARCH_PROD	12/5/2019 10:07:10 PM	12/5/2019 10:04:53 PM

In addition, rule-based alerts can be defined on the event data received from the Database Firewall. Alert conditions are flexible and can include more than one event, and the events can come from different databases.

For continuous monitoring of network activity for detecting unusual traffic patterns, consider using Database Firewall reports as given in [Establish Proactive Security Monitoring Practices, including Sensitive Data Access](#).

CONCLUSION

Database Activity Monitoring is one of the key requirements for RBI compliance on cyber security regulations. RBI recommends that banks address network and database security comprehensively.

By using Oracle Database's native auditing feature, and Oracle Audit Vault and Database Firewall (AVDF), banks can not only accelerate their implementation but also achieve comprehensive security controls for their sensitive data.

APPENDIX

Application Activity Auditing Sample

A sample procedure, which populates application context attributes from gv\$session and userenv, and the audit configuration which captures the context attributes in the audit trail, is shown below.

```
-- Look up gv$session fields
SELECT V.PROGRAM INTO program_name
FROM GV$SESSION V
WHERE V.audsid = sys_context('USERENV', 'SESSIONID')
AND V.inst_id = sys_context('USERENV', 'INSTANCE')
AND V.SID = SYS_CONTEXT('USERENV','SID');

DBMS_SESSION.SET_CONTEXT('app_ctx', 'UNIQUE_SESSION_ID', DBMS_SESSION.UNIQUE_SESSION_ID );
DBMS_SESSION.SET_CONTEXT("app_ctx", 'PROGRAM', program_name);
DBMS_SESSION.SET_CONTEXT('app_ctx', 'SERVICE_NAME', sys_context('USERENV', 'SERVICE_NAME'));

--Enabling audit of app_ctx application context

AUDIT CONTEXT NAMESPACE app_ctx ATTRIBUTES UNIQUE_SESSION_ID, PROGRAM, SERVICE_NAME;

Unified Audit trail with APPLICATION_CONTEXTS field populated:

APPLICATION_CONTEXTS

-----

(APP_CTX,PROGRAM=sqlplus@oracle047.us.oracle.com(TNSV1-V3));
(APP_CTX,SERVICE_NAME=adm.DEV);(APP_CTX,UNIQUE_SESSION_ID=029D07880001);
```

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

Copyright © 2020, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Accelerate DAM Readiness to RBI Guidelines
June, 2020
Angeline Janet Dhanarani, Database Security Product Management

