**Data base auditing models**-

Database auditing models refer to frameworks and methodologies used to perform auditing activities on databases. Auditing involves monitoring and reviewing database activities, including data access, data modifications, and system events, to ensure compliance, detect security breaches, identify anomalies, and support forensic investigations. Here are some common database auditing models:

 

1. Basic Audit Model: The basic audit model focuses on recording and analyzing essential audit trail information. It typically involves capturing and storing audit logs that contain details such as user activity, data modifications, logins, and system events. The audit logs are reviewed periodically for compliance and security purposes.
2. Standard Audit Model: The standard audit model builds upon the basic model and incorporates more comprehensive auditing practices. It involves the systematic collection and analysis of audit data, including tracking user activities, monitoring data changes, and correlating events to identify patterns or anomalies. The standard model often includes predefined audit policies and rules for specific events or activities.
3. Continuous Monitoring Model: The continuous monitoring model goes beyond periodic reviews and adopts real-time or near-real-time monitoring of database activities. It leverages automated tools and technologies to continuously capture and analyze audit data, providing immediate visibility into database operations. This model is particularly useful for detecting and responding to security incidents promptly.
4. Compliance-Oriented Model: The compliance-oriented model focuses on meeting regulatory and industry-specific compliance requirements. It involves aligning auditing practices with relevant standards such as PCI DSS (Payment Card Industry Data Security Standard), HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation), or specific industry regulations. The model ensures that audited data is collected, retained, and reported in accordance with compliance mandates.
5. Behavior-Based Audit Model: The behavior-based audit model utilizes advanced analytics and machine learning techniques to analyze database activities and detect suspicious or abnormal behavior. It establishes baselines of normal behavior and identifies deviations that may indicate unauthorized access, data breaches, or malicious activities. This model focuses on anomaly detection and supports proactive security measures.
6. Forensic Audit Model: The forensic audit model emphasizes gathering and analyzing digital evidence from databases for investigations and legal proceedings. It involves preserving audit logs, maintaining data integrity, and employing forensic techniques to reconstruct events or recover deleted or modified data. Forensic audits are conducted following strict procedures to ensure the admissibility and reliability of the evidence.
7. Privileged User Monitoring Model: The privileged user monitoring model focuses on monitoring and auditing activities performed by privileged users, such as database administrators (DBAs) or system administrators. It involves tracking privileged user actions, accessing sensitive data, modifying database configurations, or performing administrative tasks. The model helps detect unauthorized or inappropriate actions by privileged users and ensures accountability. 

It's important to note that the specific auditing model used can vary depending on the organization's requirements, industry regulations, and the complexity of the database environment. Organizations may also adopt a combination of multiple models to meet their auditing needs. Implementing a robust auditing model requires defining clear audit objectives, establishing audit policies and procedures, leveraging appropriate auditing tools and technologies, and regularly reviewing and analyzing audit data to identify security risks and compliance gaps.