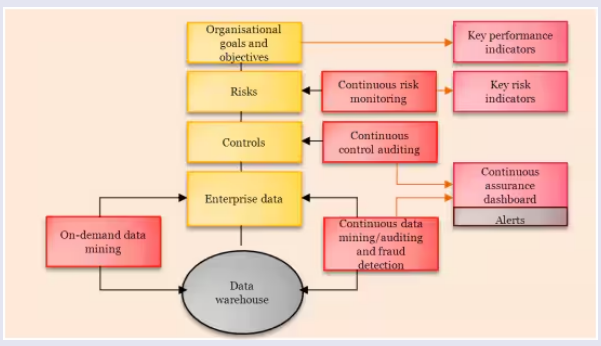
JESUS GARCIA SANCHEZ

"THE IMPORTANCE OF DATABASE AUDITING AND DBMS PERFORMANCE MONITORING"

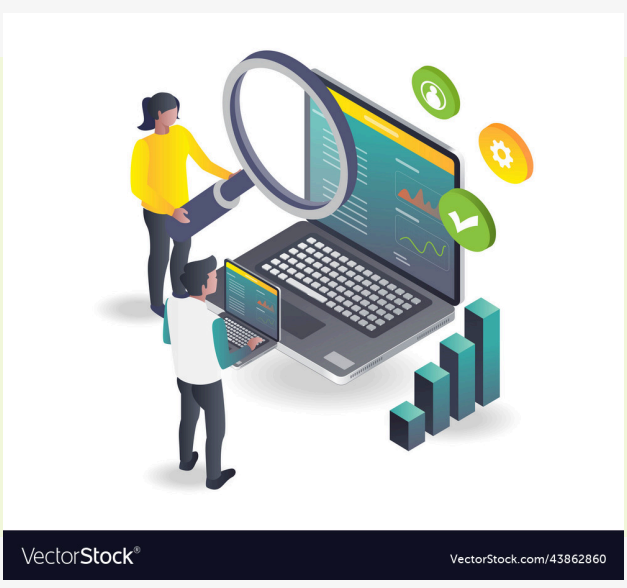


WHAT IS DATABASE AUDITING?

ISO/IEC 9075 is the international standard defining SQL (Structured Query Language), used to manage, manipulate, and query relational databases. The standard ensures interoperability and uniformity across different Database Management Systems (DBMS).

WHY IS IT IMPORTANT?

- Detects unauthorized or suspicious activity.
- Ensures regulatory compliance (e.g., GDPR, HIPAA).
- Provides accountability and traceability for actions.
- Useful for incident response and forensic analysis.



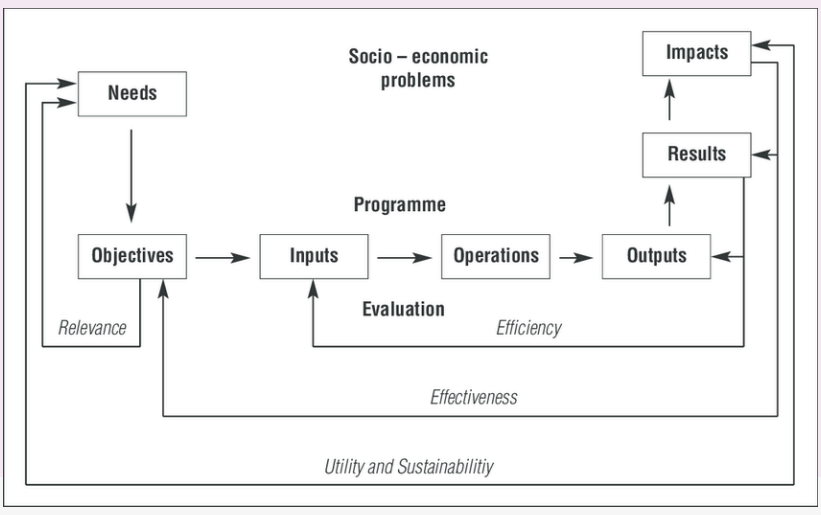
AUDIT

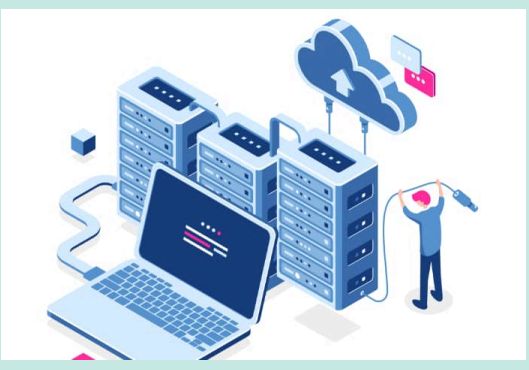
DBMS PERFORMANCE MONITORING

Performance monitoring involves observing the database's resource usage and response to operations. It ensures that the system runs optimally, can handle user demand, and responds to queries without delay.

WHAT TO MONITOR:

- CPU and memory usage
- Query execution time
- Slow queries and deadlocks
- Number of active connections
- Disk I/O and buffer cache hit ratio





BENEFITS:

- Detects bottlenecks and inefficient queries.
- Prevents system crashes and slowdowns.
- Assists in capacity planning and optimization.
- Ensures high availability and better user experience.

STATISTICS & DATA

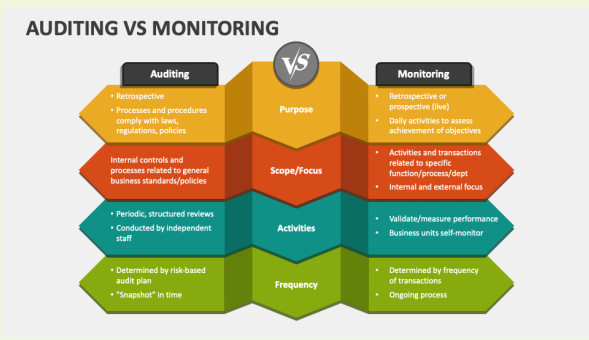
- 85% of data breaches involve unauthorized access due to lack of auditing (IBM, 2023).
- Organizations using performance monitoring reduce downtime by up to 70%.
- 60% of database performance issues come from unoptimized queries (Microsoft, 2022).
- Regular auditing reduces internal threats by 25% on average.

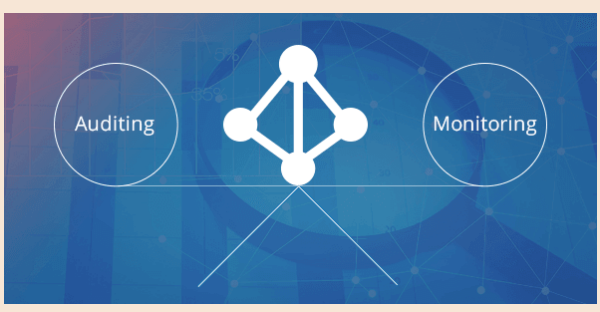
TYPES OF AUDITING:

- Standard auditing: Tracks general operations like logins, object access.
- Fine-grained auditing (FGA): Focuses on specific columns, tables, or actions.
- Unified auditing: Combines all auditing methods into a central system (e.g., Oracle 12c+).
- Compliance auditing: Designed to meet legal or corporate standards (e.g., PCI DSS).

PROACTIVE MONITORING STRATEGIES:

- Threshold alerts: Set custom limits for CPU, memory, query time, etc.
- Historical trend analysis: Helps predict future resource demands.
- Query profiling: Breaks down how queries are executed internally (joins, scans, indexes).
- Resource bottleneck analysis: Determines if problems come from storage, CPU, or app layer.





LATENCY AND THROUGHPUT

Two critical measures of DBMS performance are latency and throughput. Latency refers to how fast the system responds to a single query, while throughput measures how many operations the system can handle per second. A system with high throughput but high latency may still deliver a poor user experience. Monitoring helps strike the right balance.

SECURITY ANGLE & COMMON FAILURES

- Many organizations log user logins but fail to log data reads or exports, leaving blind spots.
- Misconfigured auditing policies can flood logs with irrelevant data, hiding real threats.
- Lack of monitoring leads to slow query buildup, causing unexpected outages during peak hours.
- Without real-time alerts, DBA teams may not know performance has degraded until users complain.

CONCLUSION

In conclusion, both database auditing and DBMS performance monitoring are essential pillars in modern data management. Auditing not only helps organizations comply with legal and security standards, but it also ensures transparency and accountability by tracking user behavior and data access. Performance monitoring, on the other hand, guarantees the efficiency and availability of the system by detecting technical issues and optimizing resource usage.

REFERENCES

[1] “X-Force 2025 Threat Intelligence Index | IBM”. IBM - United States. Accedido el 30 de mayo de 2025. [En línea]. Disponible: https://www.ibm.com/reports/threat-intelligence

[2] “Security Guide”. Oracle Help Center. Accedido el 30 de mayo de 2025. [En línea]. Disponible: https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/index.html

[3] “SP 800-92, Guide to Computer Security Log Management | CSRC”. NIST Computer Security Resource Center | CSRC. Accedido el 30 de mayo de 2025. [En línea]. Disponible: https://csrc.nist.gov/pubs/sp/800/92/final

[4] “| A. James Clark School of Engineering, University of Maryland”. A. James Clark School of Engineering, University of Maryland. Accedido el 30 de mayo de 2025. [En línea]. Disponible: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds