Business Intelligence Concept

Agenda

Here, we will cover:

- OLTP vs. OLAP
- BI Tools
- Dashboards
- Scorecards
- Security

OLTP vs. OLAP

OLTP	OLAP
• Optimized for processing transactions in real time. • Stores data in a highly normalized form (typically operational data). • Designed for transactional processing – handling small, fast transactions. • Characterized by a high volume of short transactions.	• Optimized for complex querying and analysis. • Stores data in a denormalized, multi-dimensional format. • Designed for analytical processing - handling complex queries over a large volume of data. • Characterized by low volume of complex queries.

OLTP vs. OLAP

OLTP	OLAP
• High level of consistency required. • Typically used in transactional environments such as banking, retail, and e-commerce. • OLTP systems require a high level of availability, as downtime can impact business continuity.	• Consistency can be relaxed for faster querying. • Typically used in Business Intelligence and data warehousing environments for complex reporting and analysis. • OLAP systems can tolerate some downtime, as they are not critical for real-time requirements.

BI Tools

- Business Intelligence (BI) tools are software applications used to gather, store, analyse, and provide access to data that supports the decision-making process.
- BI tools enable users to perform tasks such as data mining, report generation, data visualization, and dashboard creation.
- Popular BI tools include Tableau, Power BI, Oracle BI, SAP Business Objects, and IBM Cognos.
- BI Tools can be categorized into – Self Service tools, Cloud-based BI tools, mobile BI tools, and open-source BI Tools.

Features of BI tools

- Data Integration: Offers data integration capabilities that enable users to integrate data from different sources, such as databases, spreadsheets, and cloud-based applications.
- Data visualization: Provides data visualization capabilities that allow users to create interactive charts, graphs, and dashboards to represent data in a meaningful way.
- Data Analysis: Offers advanced data analysis capabilities, such as predictive analytics and data mining, that allow users to discover patterns and trends in data.
- Collaboration: Enables users to share reports and dashboards with others within an organization.
- Mobile Support: Allows access to data and reports from smartphones and tablets.
- Security: Features such as role-based access control and data encryption to ensure data security and privacy.

Dashboards

- A dashboard is a visual representation of data that provides users with an at-a-glance view of key performance indicators (KPIs) and metrics.
- Dashboards are used to monitor business performance and help make data-driven decisions.
- Data is typically displayed in the form of charts, graphs, tables, and other visualizations.
- Dashboard can be customized to meet the specific needs of different users and departments.

Dashboard – Key Features

- Real-time data – Provides up-to-date information as and when available in real-time or near real-time.
- Interactive – Allows users to interact with the data, like drill down, to get more detailed information.
- Mobile-friendly – Dashboards can be accessible from multiple devices, on demand.
- Customisable – To meet specific needs of users and departments (sales view vs. inventory view).
- Alerts and notifications – Ability to send alerts and notifications to users when KPIs or metrics fall outside the expected ranges.

Scorecards

- A scorecard is a business management tool that is used to measure progress toward strategic and operational goals and objectives.
- It provides a high-level overview of key performance indicators (KPIs) and metrics that are relevant to the organization.
- Scorecards can be used to communicate performance data to stakeholders and enable data-driven decision-making.
- They are often used in conjunction with other BI tools, such as dashboards, reports, and analytics.
- They can be customized to suit the needs of different stakeholders and can be updated on a regular basis to reflect changes in objectives or performance.

Scorecards – Key components

- Objectives: Specific and measurable goals that the organization wants to achieve.
- KPIs: Indicators that measure progress towards achieving the objectives.
- Targets: Desired level of performance for each KPI.
- Actuals: Actual performance data of each KPI.
- Variance: The difference between the actual and the target.
- Trend: Direction and rate of change over time for each KPI.
- Comments: Additional context that helps explain the performance data.
- Score: A summary measure that combines the KPIs into a single value that represents overall performance.

Security

- Security in Business intelligence refers to protection of sensitive data and information and their access.
- BI security includes multiple layers of protection, including physical, technical, and administrative measures.
- Physical Security: Restricting access via physical means– access cards, biometrics, surveillance cameras
- Technical Security: Security protocols to protect data during transmissions, such as encryption and secure connections, authorization, and authentication mechanism.
- Administrative security: Establish policies and procedures to manage user access, monitor activity, and respond to security incidents.
- BI Security also involves data governance and compliance with regulations and standards.

Summary

A brief recap:

- OLTP (Online Transaction Processing) systems are designed for the transactional processing of data, while OLAP (Online Analytical Processing) systems are designed for the analysis processing of data
- BI (Business Intelligence) tools are software applications used to analyze and report on data in order to support decision-making in organizations.
- Dashboards are visual displays of key performance indicators (KPIs) and other important metrics that provide at-a-glance insights into business performance
- Scorecards are tools to help organizations track and measure progress toward specific goals/objectives
- Security in data warehousing involves implanting measures to ensure that data is protected from unauthorized access, disclosure, or modification.