

ONE PAGE SUMMARY

IT & Software > Business Intelligence > BI Security

Introduction to BI Security

Protecting Data: The Essentials of BI Security

DEFINITION

BI Security refers to the measures taken to protect business intelligence data from unauthorized access and breaches. It ensures the integrity, confidentiality, and availability of sensitive information used for decision-making.

KEY CONCEPTS

Data Encryption

Data encryption involves converting information into a code to prevent unauthorized access.

Access Control

Access control restricts who can view or manipulate BI data based on user roles.

Data Governance

Data governance establishes policies for data management, ensuring compliance and security.

User Authentication

User authentication verifies the identity of individuals accessing BI systems to prevent fraud.

Audit Trails

Audit trails track user activity within BI systems, helping to identify and investigate security breaches.

EXAMPLES

- Implementing role-based access control for BI dashboards.
- Using encryption for sensitive sales data in reports.
- Conducting regular audits of user access logs.

MEMORY TIPS

- ★ Remember 'EACGA' for Encryption, Access control, Governance, Authentication.
- ★ Think of a 'lock and key' for access control.
- ★ Visualize a 'data shield' for overall BI security.

COMMON MISTAKES

- ✗ Neglecting regular updates to security protocols.
- ✗ Overlooking user training on security best practices.
- ✗ Assuming all data is safe without regular audits.

QUICK RECAP

BI Security is crucial for protecting sensitive data in business intelligence. Key measures include encryption, access control, and regular audits to ensure data integrity and confidentiality.