ONE PAGE SUMMARY

IT & Software › Business Intelligence › BI Security

Introduction to BI Security

Protecting Data: The Essentials of BI Security

DEFINITION

> BI Security involves safeguarding business intelligence data from unauthorized access and breaches. It ensures that sensitive information is only accessible to authorized users.

KEY CONCEPTS

Data Encryption

Converts data into a coded format to prevent unauthorized access.

User Authentication

Verifies the identity of users before granting access to BI tools and data.

Access Control

Defines who can view or interact with BI data based on their roles.

Data Governance

Establishes policies and standards for managing BI data securely.

Audit Trails

Records user activities to monitor access and changes to BI data.

EXAMPLES

→ Using two-factor authentication for BI tool access.

→ Encrypting sales data to protect customer information.

→ Implementing role-based access to limit data visibility.

MEMORY TIPS

★ Remember 'DEGAA' for Data Encryption, Governance, Access control, Authentication.

★ Think of a 'lock and key' for User Authentication.

★ Picture a 'security guard' for Access Control.

COMMON MISTAKES

✗ Neglecting regular updates to security protocols.

✗ Overlooking user training on BI security practices.

✗ Assuming all data is secure without encryption.

QUICK RECAP

BI Security is crucial for protecting sensitive business data from unauthorized access. Key components include encryption, authentication, and access control, ensuring only authorized users can access critical information.