SOX **(Sarbanes-Oxley Act)**

There is some confusion about understanding the **SOX** compliance.

The **Easiest** way to understand **SOX**

SOX **(Sarbanes-Oxley Act)** is a law that ensures companies keep their financial records honest and secure.

It was created to prevent fraud and protect investors.

Sarbanes-Oxley Act (SOX) established in 2002 to prevent fraud, fake accounting, and corporate corruption.

SOX was enacted to ensure financial integrity and accountability in publicly traded companies.

Key sections of SOX

Section 302 – Corporate Responsibility for Financial Reports

CEOs and CFOs must certify financial statements and ensure accuracy.

Requires internal controls to prevent fraud.

Section 404 – Management Assessment of Internal Controls

Companies must establish, document, and test internal controls over financial reporting.

Requires audits to verify control effectiveness.

Section 802 – Criminal Penalties for Fraud

Establishes penalties for altering, destroying, or falsifying records related to financial reporting.

Mandates data retention policies for compliance.

SOX Key Elements

Internal Controls: access control, segregation of duties, and security policies

Auditability & Transparency: Maintain logs, conduct periodic audits, and document financial transactions.

Access Management: least privilege, multi-factor authentication (MFA), and monitor privileged accounts.

Risk Management: Identify, assess, and mitigate risks related to financial data and reporting.

IT Security & Compliance: Protect financial systems from unauthorized access, data breaches, and cyber threats.

How an Organization like Bank Implements SOX Compliance

- Identity and Access Management (IAM) Controls

    Role-Based Access Control (RBAC)

    Multi-Factor Authentication (MFA)

    Separation of Duties (SoD)

- Monitoring & Audit Logging
- IT Security Controls