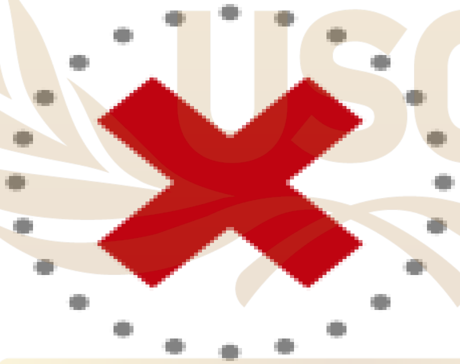
Subject of Bank risks (Ch.4)

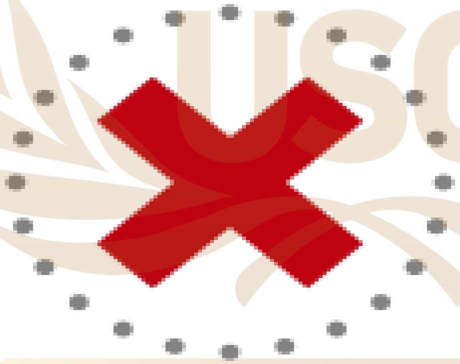
Eslam Elshafie

Non-systematic risks refer to events that cannot be fully controlled in banking activities.



Banking risks are among the key factors leading to the failure of financial institutions.

A bank's expected losses depend on unexpected events that may occur in financial markets.



Banking risks can be managed by balancing the level of return with the degree of risk.

Sound credit granting guidelines help reduce concentration risks in the bank's portfolio.

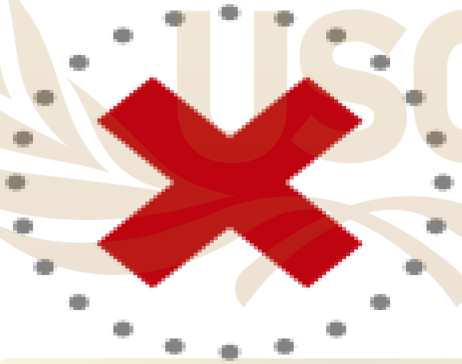
Banks can mitigate operational risks by improving internal control systems.

Economic changes increase the level of risks faced by banks during periods of instability.

Diversification of investment portfolios helps reduce risks that may affect the bank.

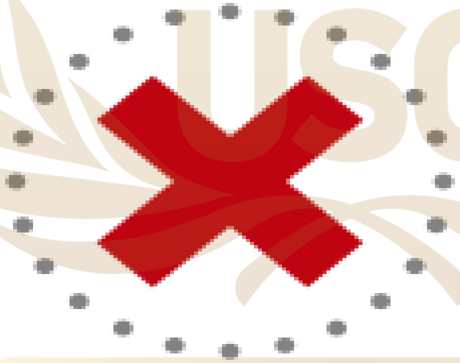
The extent of banking risks faced by banks depends on the size and complexity of their operations.

The bank can fully control economic risks by adopting precautionary policies.



Operational risks refer to risks arising from failures in the bank's personnel, systems, and processes.

Legal risks enhance the bank's profitability.



Banks can transfer risks they face to other parties to eliminate them.

Banks face operational risks due to outdated information technology systems.

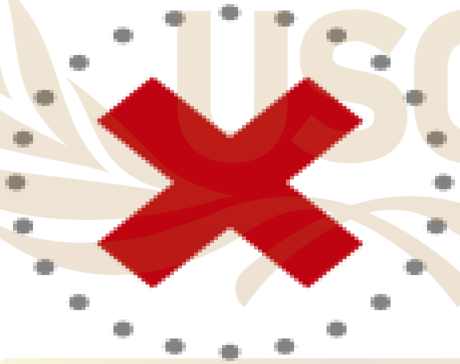
Liquidity risks depend on the bank's ability to meet its obligations as they become due.

Rapid technological advancements improve banks' ability to manage risks.

The effectiveness of regulatory policies depends on the bank's ability to detect and address errors.

Legal risks refer to risks arising from changes in laws and regulations.

Failure of the bank's technological systems improves its ability to manage operations.

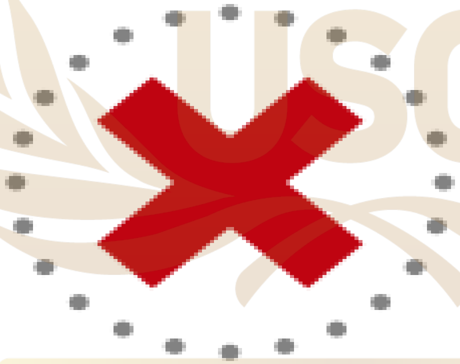


Default risks depend on the customer's ability to repay loans on time.

Sound practices help reduce the level of risks faced by the bank.

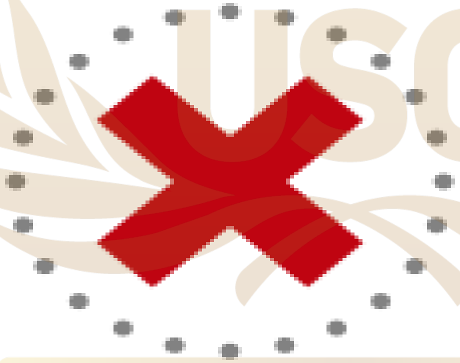
Changes in political conditions increase the level of systemic risks.

The banking risk committee operates by focusing on a single type of risk without considering other related risks.

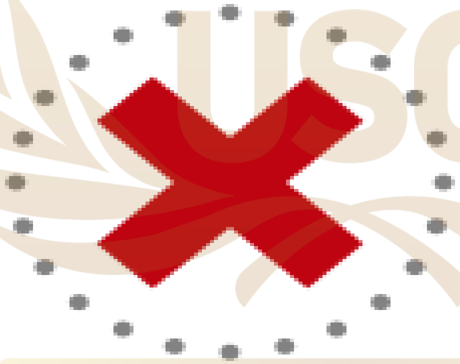


The bank manages risks by setting specific ceilings for risk-generating banking activities to reduce their negative impacts.

Risk identification is a secondary phase in banking risk management and does not require continuous action.

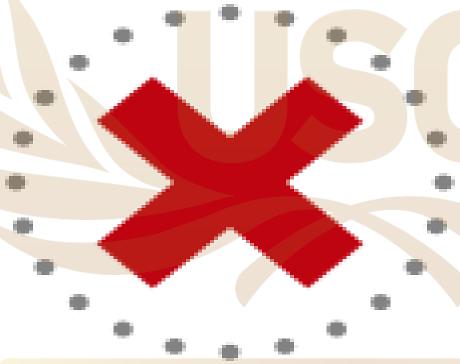


The bank's board of directors sets risk management policies without approval from senior management.

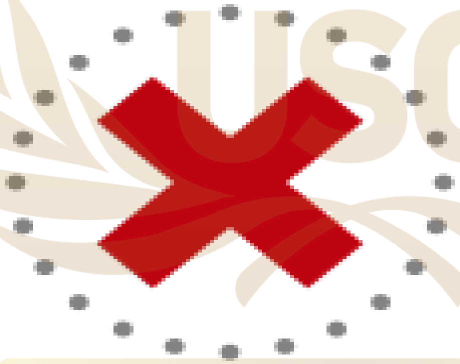


Banking risk management relies on clear segregation between individuals making risk decisions and those monitoring them.

The bank updates its risk management policies only in the event of significant financial losses.



Banking risk management focuses solely on credit risks, ignoring operational or market risks.



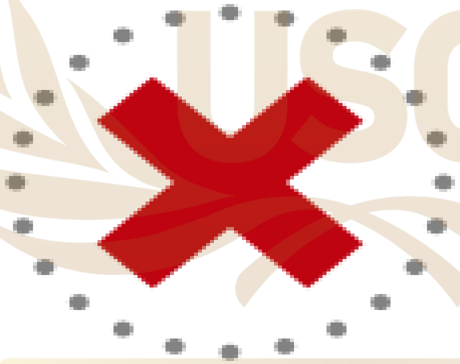
Banks are encouraged to fully disclose the risks surrounding their banking activities in line with Basel requirements.

Risk management relies on continuous updates of policies and systems to avoid financial losses associated with banking risks.

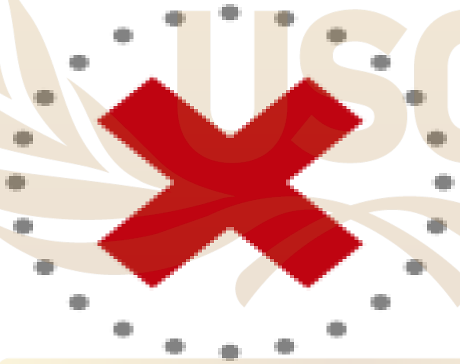
Achieving adequate financial solvency requires banks to comply with risk monitoring and periodic evaluation standards.

The stability of the Egyptian banking sector relies on the success of banks in implementing effective strategies for financial risk management.

The concept of cybersecurity focuses solely on protecting bank systems, ignoring other institutions.



Cyberattack risks refer only to factors that threaten information and customer data.

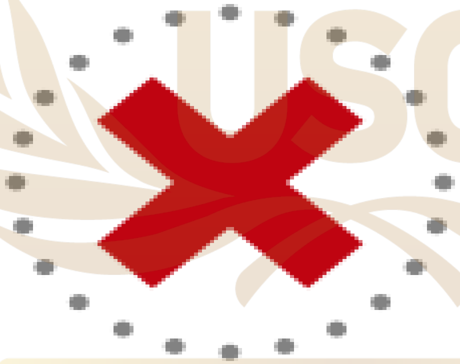


Network security is an essential part of cybersecurity strategies to protect information.

Cybersecurity includes enhancing the recovery of institutions from cyberattacks.

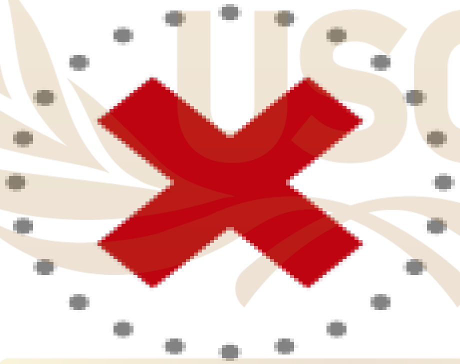
Internal control systems enhance the efficiency of banking risk management.

Banks must update customer information systems only when security breaches occur.



Sound risk management practices improve the bank's reputation in the market.

Cybersecurity relies entirely on technology without requiring regulatory measures.



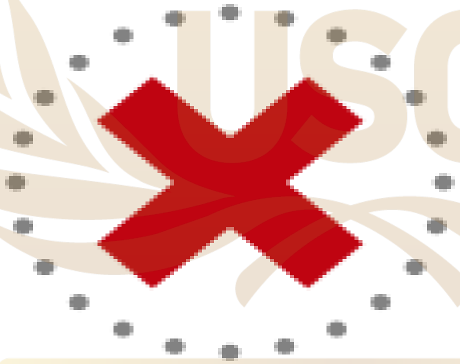
Weaknesses in information systems refer to vulnerabilities that attackers can exploit.

The success of cybersecurity strategies depends on the participation of all bank employees in their implementation.

Sufficient knowledge of modern technologies enhances cybersecurity.

Cybersecurity risk assessments require adherence to pre-defined procedures.

Cybersecurity refers to a set of measures solely focused on data protection.



The End

Thank you