

# Compliance with Saudi Central Bank Frameworks for Business Continuity Management, Counter Fraud, and Cyber Security




In today's rapidly evolving digital landscape, safeguarding business operations against unforeseen disruptions, fraud, and cyber threats is paramount. The Saudi Central Bank provides comprehensive frameworks for financial institutions to ensure compliance with the requirements.

**i**nsights


Riyadh Office:

+966 59 001 3882

 [insightss.co](http://insightss.co)

Jeddah Office:

+966 50 088 5759

 [info@insightss.co](mailto:info@insightss.co)

# Frameworks



## Business Continuity Management (BCM)

**i** Ensure Resilience in the Face of Disruption



BCM  
Governance



BCM  
Strategy



Business Impact  
Analysis



Continuity  
Planning



Testing and  
Maintenance



## Counter Fraud Framework

**i** Protect Businesses from Fraudulent Activities



01 Governance

02 Fraud Prevention

03 Fraud Detection

04 Reaction and Recovery

05 Continuous Improvement and Adaptability



## Cyber Security Framework

**i** Defend Against Cyber Threats

01 Leadership and  
Governance

02 Risk Management  
and Compliance

03 Operations and  
Technology

04 Third-Party  
Cyber Security

05 Incident  
Response

06 Awareness and  
Training



## How will Insights help?

At Insights, our IT professionals utilize decades of experience from multinational companies to implement frameworks for BCM, Counter Fraud, and Cybersecurity, ensuring your organization remains resilient, compliant, and secure. Our commitment to open communication and an easy-to-follow approach ensures that we grasp your needs and deliver customized solutions through the following services:

- 01 Conduct a comprehensive assessment of your current practices.
- 02 Identify gaps in compliance with the frameworks.
- 03 Provide a detailed report with actionable recommendations.
- 04 Develop a thorough plan to implement the frameworks within your organization.
- 05 Ensure seamless integration with your existing systems and processes.
- 06 Create and update policies and procedures to align with the requirements.
- 07 Set up systems for continuous monitoring of compliance.
- 08 Perform regular system audits to ensure ongoing compliance with the frameworks.
- 09 Verify the documentation is thorough and compliant.
- 10 Prepare timely reports and suggestions for improvements.
- 11 Offer training to your team to ensure they understand and adhere to these policies.
- 12 Stay abreast of the latest developments in regulations and best practices to enhance the services continually.



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.