RTGS System Safety & Efficiency

Question: A central bank is seeking advice from the broader central-bank community on how to enhance the safety and efficiency of its RTGS system. The central bank has reached out to your team for insight and recommendations, including best practices, on this topic.

Recommendations

In order to enhance the RTGS system's safety and efficiency, we recommend the central bank:

1. Identify the risks its RTGS system may face
2. Identify and implement mitigants for each of those risks
3. Develop internal policies and procedures
   – Business Continuity Plan
4. Perform tests and drills
   1. Testing and strengthening those plans
5. Ensure good governance

Analysis

Key risks

- Reputational risk
  - Mitigant: Optimal management of risks, including effective communication and accountability
- Credit risk
  - Mitigant: collateral
    - Enforce high-quality collateral requirements and conservative haircuts

Operational risk

- Factors affecting operational risk
  1. People
     1. <u>Mitigant</u>: Training. Background checks. Access rights (segregation of duties). Backup team.
  2. Relationships with third parties
     1. <u>Mitigant</u>: Due diligence on critical providers and vendors. Comprehensive Service Level Agreements, which include response time recovery, communication, and service availability.
  3. Physical location
     1. <u>Mitigant</u>: Backup site (different geographic location)
  4. System/technology
     1. Business-as-usual “incidents”
        1. Change management – upgrades/enhancements
     2. Ad-hoc/one-off “incidents” – focused on cyber (see next slide)

Case Study: Cyber risk

- Mitigants
  - Prevention measures
    - IT security assurance
      - e.g. penetration and vulnerability testing, strong IT security policy
    - People
      - e.g. limit access rights, training and awareness, background checks
  - Continuous monitoring and detection
    - IT
      - e.g. Alerts, firewalls
    - People
      - e.g. Regular review of access rights, training and awareness