RTGS System Safety & Efficiency
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 mitigants for each of those risks
3. Write it all down
   - Internal policies and procedures
   - Incident Management Plan
4. Tests and drills
   1. Testing and strengthening those plans
Analysis
Types of risks

• Credit risk (CB) – extending intraday credit
  – Mitigant: collateralized credit
    • Eligible collateral: High-quality collateral. Conservative haircuts

• Liquidity
  – Operators do not face liquidity risk

• Reputational risk
  – Mitigant: Effective communication and transparency. Properly manage other risks.

• Operational risk
  – See next slide
Operational risk

• Categories of operational risk
  1. Human
    1. **Mitigant:** Training. Background checks. Access rights (segregation of duties). Backup team.
  2. Relationships with third parties
    1. **Mitigant:** Due diligence on critical providers and vendors. Comprehensive Service Level Agreements, which include response time recovery, communication, and service availability.
  3. Location
    1. **Mitigant:** Backup site not subjected to same factors
  4. System/technology
    1. Business-as-usual “incidents”
      1. Change management – upgrades/enhancements
    2. Security “incidents” – focused on cyber (see next slide)
Case Study: Cyber risk

• Mitigants
  – Prevention measures
    • IT security assurance
      – penetration testing, separate systems
    • Human security assurance
      – “Internal threat”
  – Continuous monitoring and detection
    • IT
      – Alerts
    • Human
      – Regular review of access rights, training and awareness