Topic 3: RTGS System Safety and Efficiency

Rebecca Hall, Luke Van Uffelen, Sheree Smiling Craig, Michal Volny, Maria de los Angeles Delgado de Alvarado, Andrea Friedrich, Min woo Choi, Petra Steenbakker, Elisabeth Lervik, Liudmila Gruzdeva, Maria Jose Garcia-Ravassa, Wendy Matheny
Agenda

- Tools to help mitigate the key risks that jeopardize the safety and efficiency of an RTGS system
- Continuity arrangements during a system outage
- Measures and tools to help recover operations in the event of a system outage
Key risks threatening safety and efficiency

*Reputational Risk*

Safety
- Operational Risk
- Legal Risk
- Credit Risk

Efficiency
- Liquidity Risk
- Legal Risk
- General Business Risk
Secondary Risks to RTGS
Tools to mitigate liquidity risk

- Intraday credit
- Optimization/netting
- Collateralization
Tools to mitigate legal risk

- Strong legal basis that can be articulated
- Clear and understandable rules
- Enforceable rules
Tools to mitigate general business risk

- Robust management and control systems
- High quality liquid net assets funded by equity
- Viable recovery/wind-down plan
- Viable plan for raising equity
Tools to mitigate credit risk

- Robust credit risk management framework
- Measure and monitor credit exposures
- Stress testing
- Rules and procedures to address credit losses
Primary risk to RTGS
Tools to mitigate operational risk

- Governance
  - Policies and procedures
  - Roles and responsibilities
  - Board involvement
  - Communication

- Business Continuity
  - Disaster recovery, communication plan
  - Contingency planning

- Change management
  - Scenario planning

- Information Security
  - Testing
  - Robust system controls
  - Education and awareness
Continuity arrangements and measures during a system outage

Objective: business as usual

- Based on priority list, implement critical activities
- Enact procedures for restoring most critical processes
- Depending on outage type, start recovery
- Enact communications plan
- Data backup
- Utilize tested contingency arrangements
  - E.g. back up sites
Summary

- Operational risk is key
- Strong contingency arrangements
- Planning and testing