Thomas Murray

Risk Intelligence | Due Diligence | Cyber Security

CSD Risks

Jim Micklethwaite, MD, Financial Markets

2 May 2024

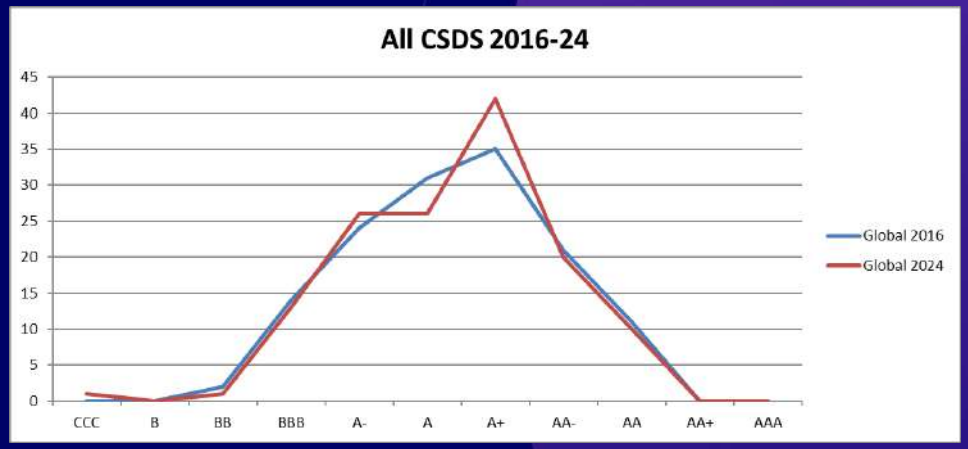
Introduction

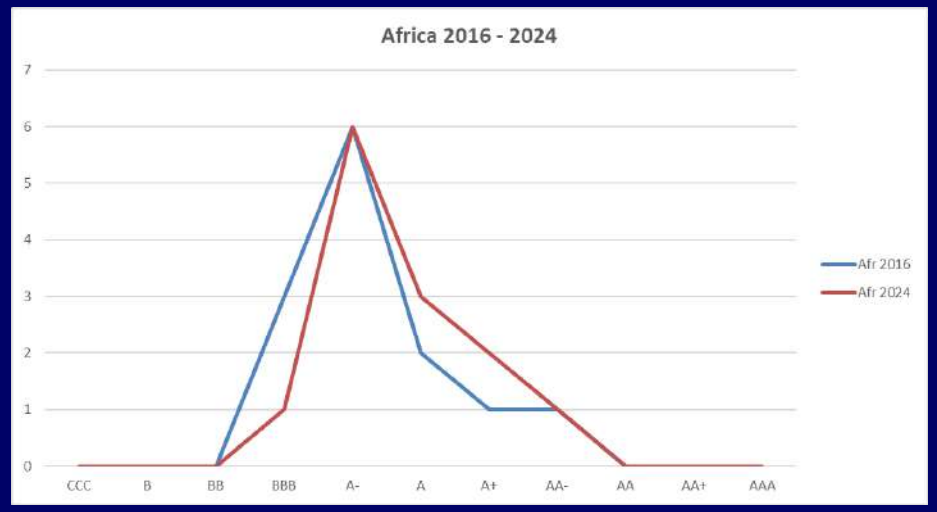
- TM CSD Risk Assessments
- Enterprise Risk Management Frameworks
- Commonly Considered Risks – Operational, Compliance, Business, Financial risk
- Uncommon Considered Risks – Political, sovereign, project, cyber
- Risks from third parties/members

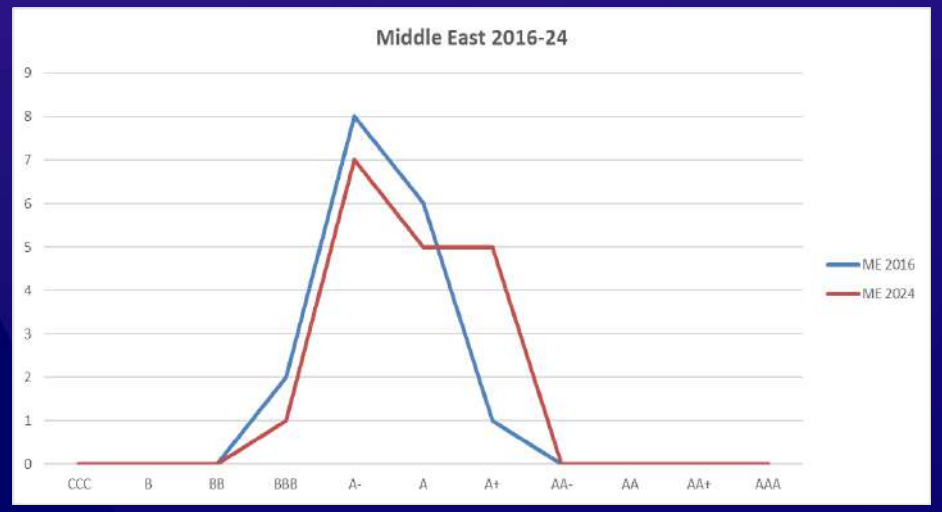
TM CSD Risk Assessments

- Established in 2001 for GCs to support Net Man and Risk functions
- Includes, but is broader than 17-f(7), tracked against best market practices
- Supported by participants and open to CSDs for review
- ‘Living’ reports rather than questionnaire-based, continuously updated
- Risks ‘posed by’ the CSD to participants and underlying investors
- 8 risks assessed based around core functions Settlement, Safekeeping, Asset Servicing + Operational, Financial and Oversight/Transparency
- Cyber and ESG assessments added as accompanying risks

Comparison 2016-2024







Main Improvements

- Extension of DVP arrangements
- Embracing of custody model
- Separation of CSDs
- Increased SWIFT adoption and higher STP
- New CSD systems
- Electronic voting
- Adoption of ERM practices

Enterprise Risk Management Frameworks

- Identify risks to the CSD and ‘posed by’ the CSD (PFMI)
- Identification, quantification, methodology, assessment, treatment and monitoring
- Board determines entity’s risk appetite and tolerance limits after response
- Should include third-parties (‘TPRM’) – effect from/to
- 3-lines of defence model – 1st: business/operations (risk owners), 2nd: risk mgmt and, 3rd: audit
- Independent Risk Dept reporting lines
- Toolkit – documentation, risk register/heatmap, training, KRIs, monitoring systems and data, audit and review

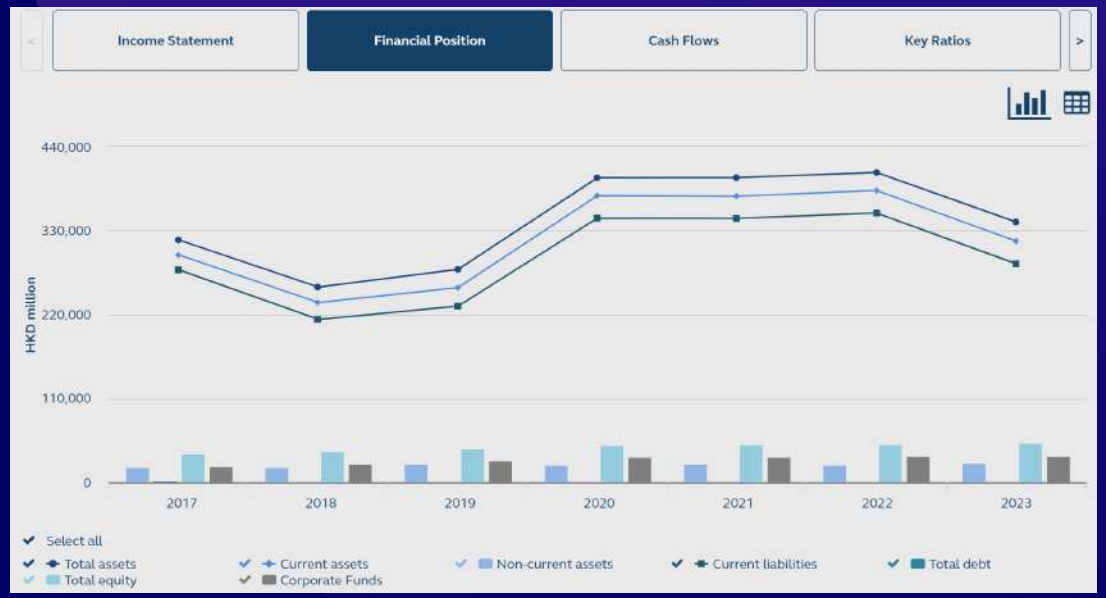
Commonly Considered Risk Categories

- Operational - external (Acts of God/Man) and internal (technology, controls breakdown, negligence, error or fraud)
- Business – commercial, outsourcing
- Regulatory – compliance, legal, data protection
- Financial – credit, liquidity, investment, accounting/reporting

Uncommonly Considered Risk Categories

Political	-	domestic instability, ideological shift, international conflict
Sovereign	-	capital flight, market closure
Project	–	system replacements, major process changes
Cyber	–	data loss, operational disruption,

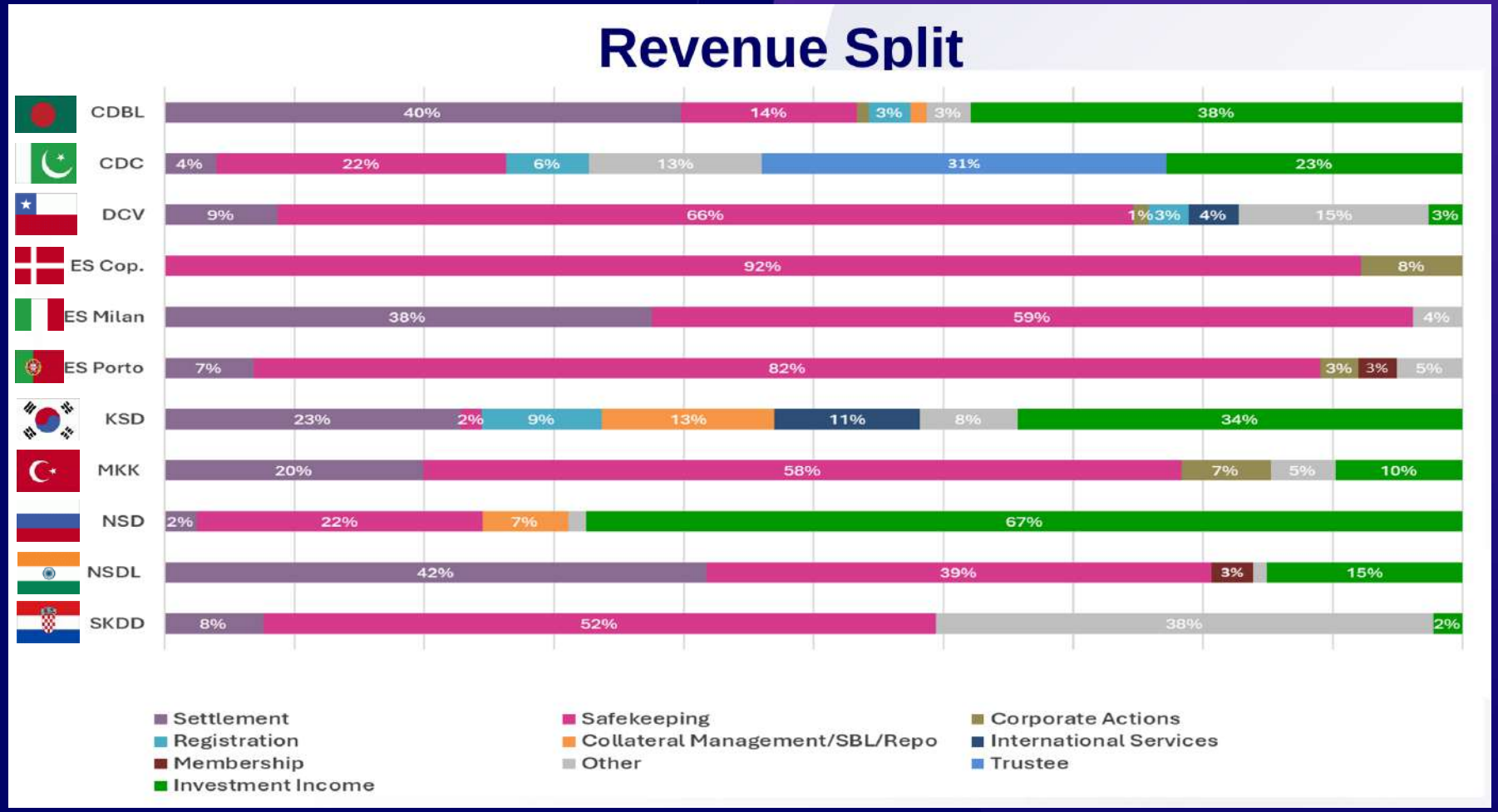
Political Risks - HK Exchanges (HKEx)



Sovereign Risk

- Main services affected would be settlement, registration and safekeeping.
- Most CSDs charge members % per transaction for settlement and % of assets under custody for safekeeping.
- Scenarios used in the analysis (based on historical defaults) suggest a decrease of the transaction volumes or/and the market capitalisation by 20 - 50% based upon a flight of capital or even a market closure.
- Resulting effect on after tax profits would be between 10-25% depending on diversity of revenues
- Capital buffer above the minimum of 6-months operating expenses

Business Diversification as Risk Mitigator



Project Risk

2003 - Canada CDSX over budget from CAD 17.5m to CAD +30m.

May 2018 – Euroclear Finland Infinity system implemented 8 mths late . System issues caused settlement disruptions repeatedly until Sept 2023 when they joined T2S.

Dec 2021 – Keler Service Development Program (KSDP). Repeated technical issues up with major outage in Aug 2022. Multi-million write-down and executive management clear-out.

Nov 2022 - ASX Settlement scrapped proposed DLT replacement for CHESS after six years, wrote off AUD 250m and replaced ExCo. New proposed CHESS replacement consultation.

Cyber Risk

- Nov 2022 – Malware attack on CDSL. Disconnected from participants and ceased settlement. Took two days to recommence operations.
- Increasing regulatory pressure to respond to Cyber threat with EU Digital Operational Resiliency Act (DORA) – risk mgmt, incident mgmt, testing, third parties, info sharing
- USA, UK, Singapore, Hong Kong and others – operational resilience guidelines
- CPMI-IOSCO – Guidance on Cyber Resilience for Financial Market Infrastructure (2016)

Controlling Risk from Participants

- Only 18% of CSDs globally (19% in AMEDA) influence the minimum capital requirements for their participants. Mostly imposed by regulators and central banks based purely on activity, not risk. Mainly in CCP models where capital varies by risk.

Membership Criteria	Global %	AMEDA %
IT Minimum Capabilities	78	64
DR/BC Facilities	29	36
Intl. Comms Standards	30	22
Min. Mgmt Qualifications	29	28
Reputation/ performance	4	0
Cyber risk profile	0	0

Thank You