Regional Cyber Risk framework

-Competition makes us faster, collaboration makes us better-

KRISTEL DE NOBREGA

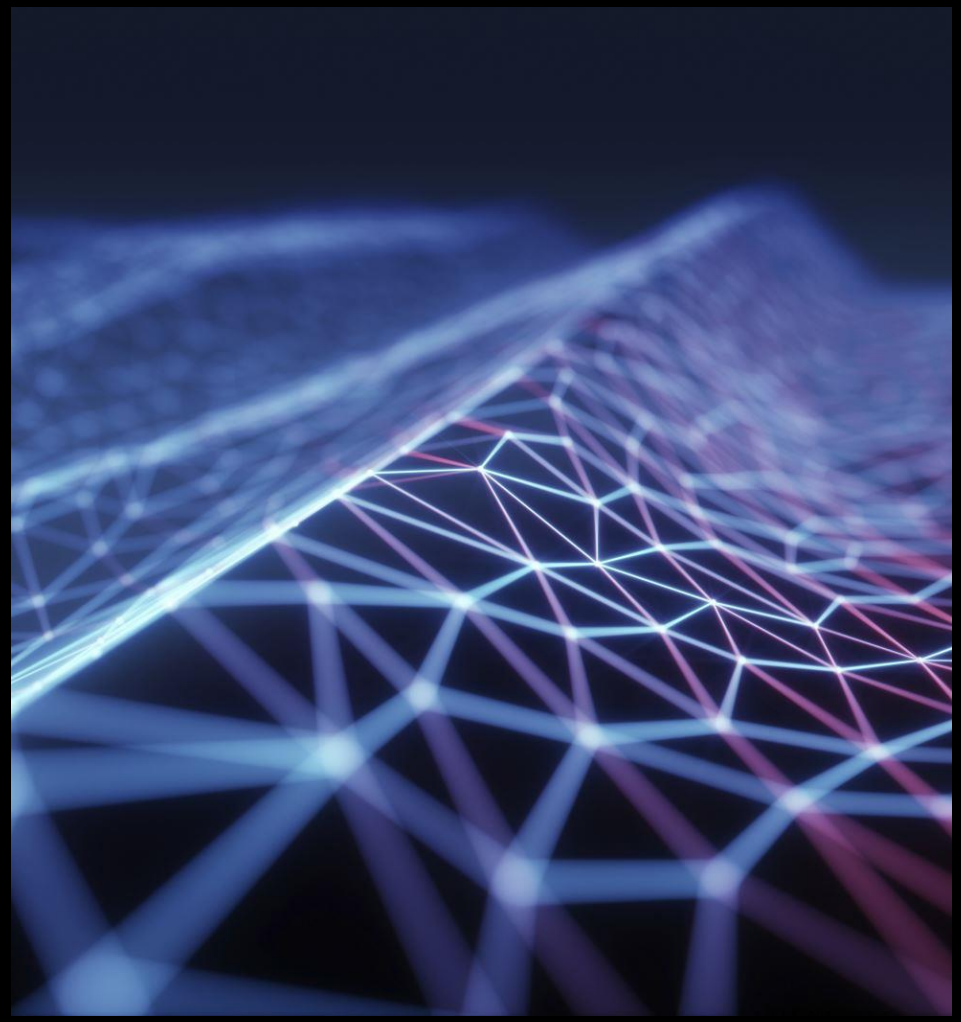
OCTOBER 2, 2020

Cyber resilience is the glue that binds us all

- Cyber attacks keep hitting the region
- Banks in the region have locations on numerous islands
- Most of current IT supervision activities are slow to pick up in this regional risk and mostly small teams to tackle the specialized area of Cyber Risk in general
- IT supervision is not uniform

Strategic overview

- Have a plan
- Have a roadmap
- Courage to press on
- Regional synergy



All you need is the plan

Setting the stage: Technology Risk Management (TRM)

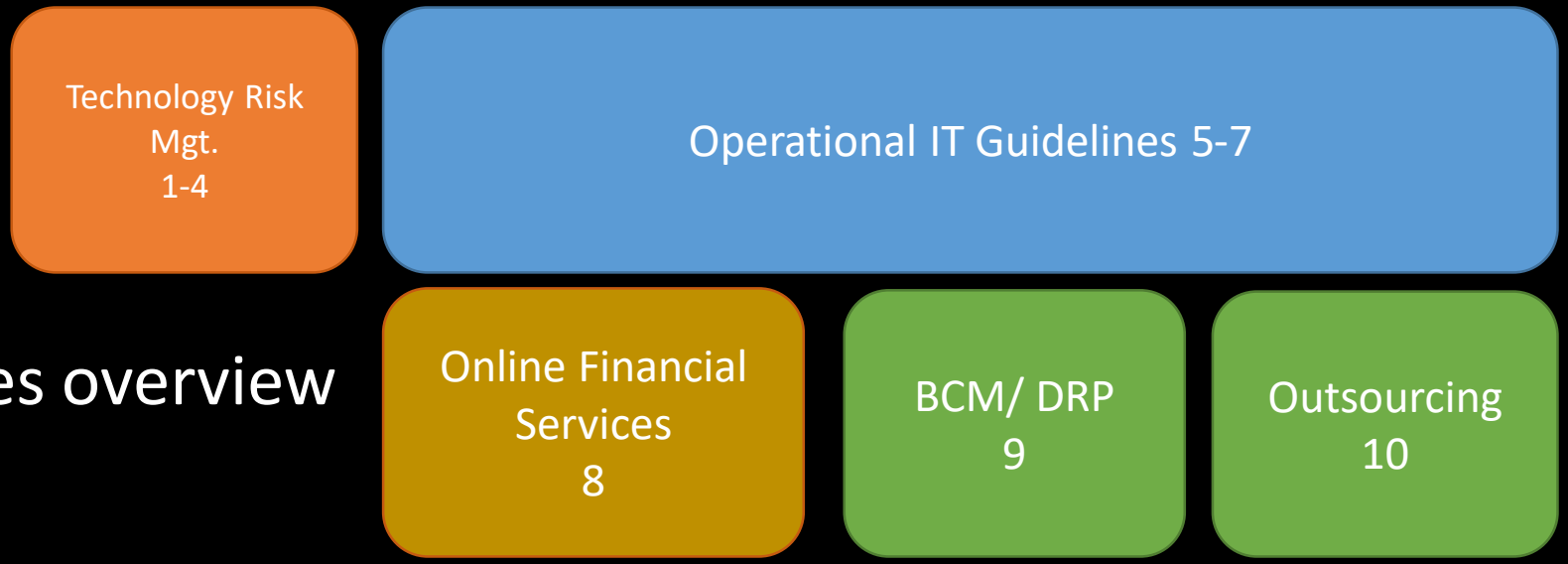
Joining forces under one framework:

- Why TRM Guidelines?
- Why this format, the scope and its applicability for an organization?
- TRM aims to mature the IT operations of the financial sector of the region

The roadmap components:

Current setup of proposed TRM document

- Technology Risk Guidelines overview



- Triage measure

Intended destination

Development of a regional cyber risk supervisory framework;

Increased awareness at CGBS level on cyber risk and cyber security initiatives;

Roadmap and speed

Review of current documentation and assessment tool Q1

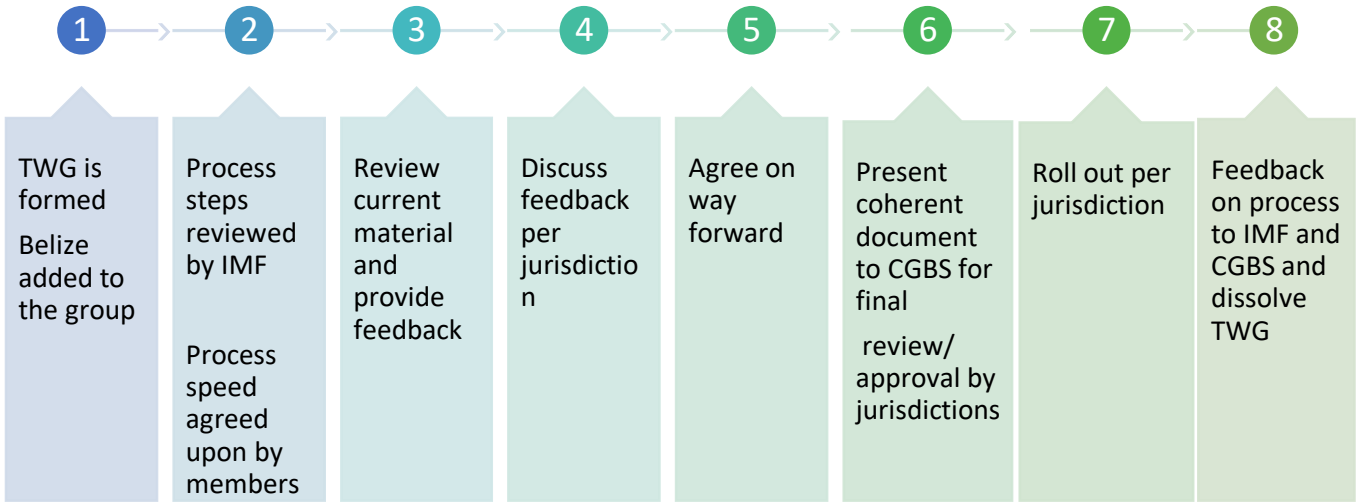
Proposal per jurisdiction on adaptions Q2

Submission for final approval

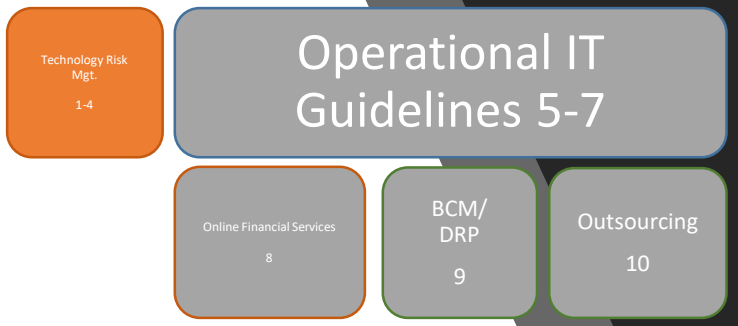
Q3 – Q4

Q4 Final regional framework

Where we are today



TECHNOLOGY RISK MANAGEMENT



Chapter 1 + 2: Why TRM guidelines?

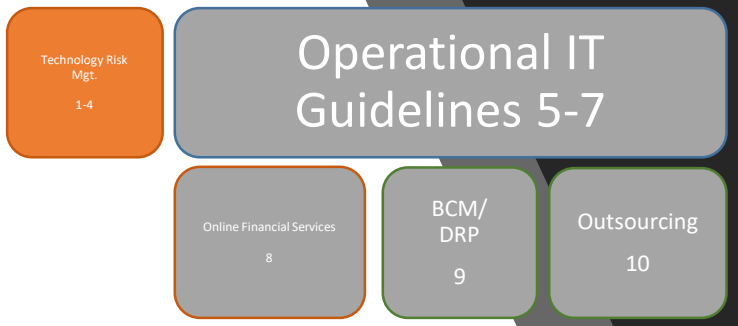
Having a mature IT environment protects each institution separately, as well as the financial sector as a whole

- Establish a sound and robust approach towards technology risk management
- Deploy strong authentication to protect customer data, transactions and systems
- Strengthen system security, reliability, resiliency and recoverability

- Aim:
  - Have clearly defined roles and responsibilities within an organization
  - Organizations should have the necessary **IT Policies, Standards, and Procedures** should be in place to manage technology risk
  - Additional focus to have **cyber security** policy to address cyber risk
  - Proper attention should be placed on education and IT awareness of staff to help minimize technology risk due to failure, internal sabotage or fraud

- Controls: Focus will be on internal governance of technology risk

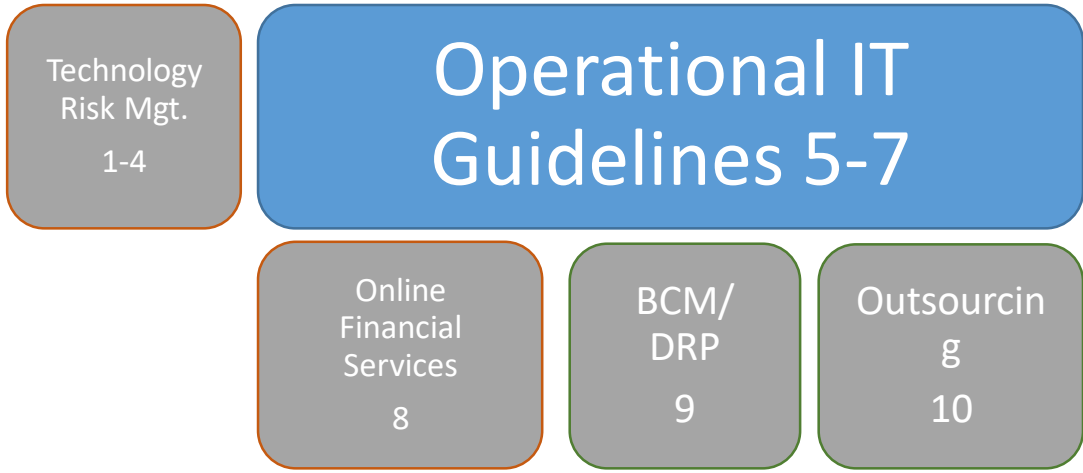
TECHNOLOGY RISK MANAGEMENT (cont.)



- Aim:
  - To have organizations perform a **risk asset assessment** in order to classify and take appropriate protection measures of their information systems.
  - Include the setup and maintenance of a **cybersecurity program**.
  - **Conduct and complete risk identification**, to quantify potential impact and consequences of their risk on the overall business.
  - **Risk treatment** strategy should be developed. Not all risks can be addressed simultaneously. Banks are forced to prioritize and implement appropriate risk-reduction controls or insure residual risks.
  - **Risk monitoring & reporting** to setup a risk registry and monitor the highest severity risks closely. The risk landscape keeps evolving, a “solid” technology today may have vulnerabilities tomorrow, which should result in new unforeseen risk treatments.

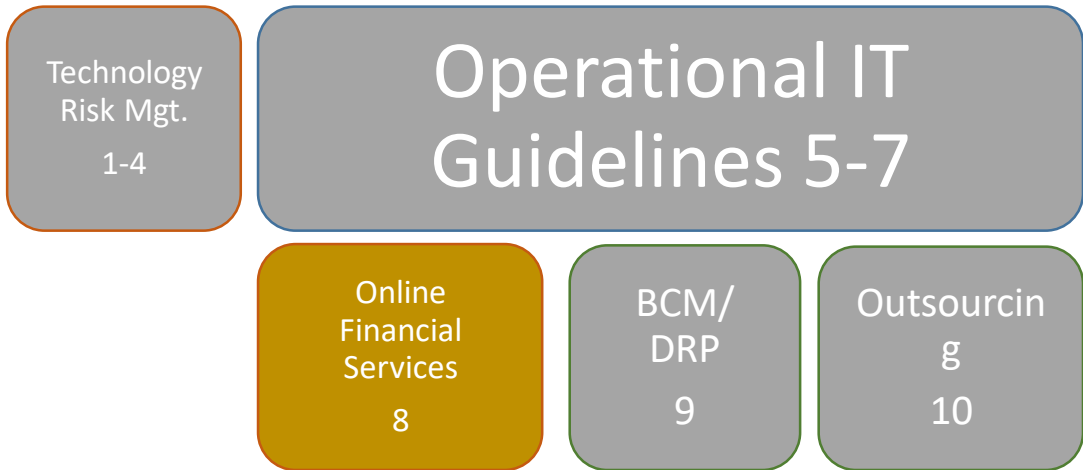
5. OPERATIONAL IT GUIDELINES

- Aim:
  - **Create a foundation** for IT maturity and IT project management
  - Focus specifically on **security requirements, testing of systems**, and end user development
  - Ensure **Problem and Incident Management** are effective
  - Elaborate extensive Data center protection
  - Operational infrastructure protection
    - Data Back up management
    - Technology refresh management
    - Network and Security Management
    - Vulnerability Assessment and Penetration testing
    - Patch Management
    - Security Monitoring
  - Audit planning and remediation tracking included in the yearly IT landscape



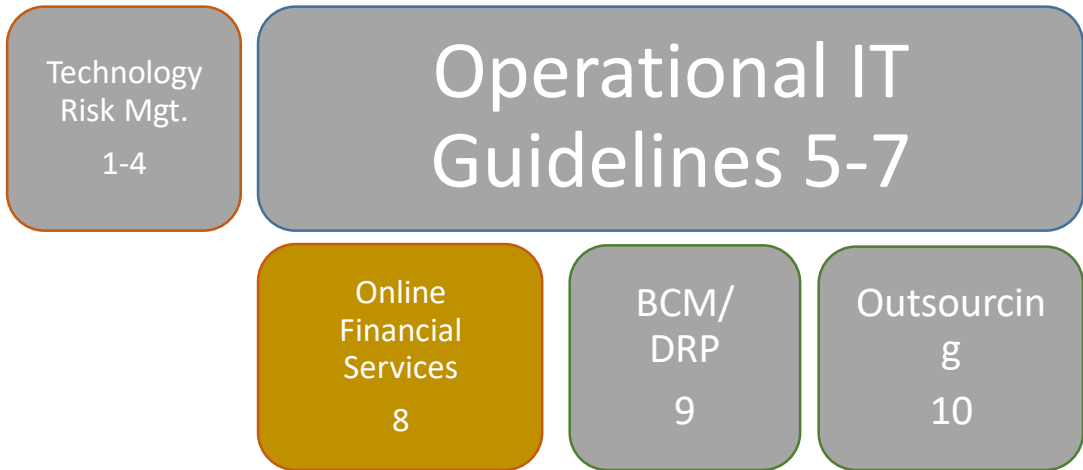
8. Online Financial Services

- Aim:
  - To ensure safe service delivery for online systems
  - Mobile Online Services and Payments Security **focused on CIA**
  - **Strong authentication** for end users, minimizing attack surface for MITMA or other cyber attacks
  - Payment Card Security (ATM's, Credit and Debit Card), NFC technology security and app security for transactions should be in place.
  - Have measures to detect and prevent card and payment fraud also in CNR or CNP scenarios.
  - Adhere to compliancy to PCI-DSS, DDA and CDA
  - Enforce ATMs and Payment Kiosk physical) security measures such as CCTV, tamper-resistant keypads, anti-skimming devices with procedures for ensuring detection and response are required.

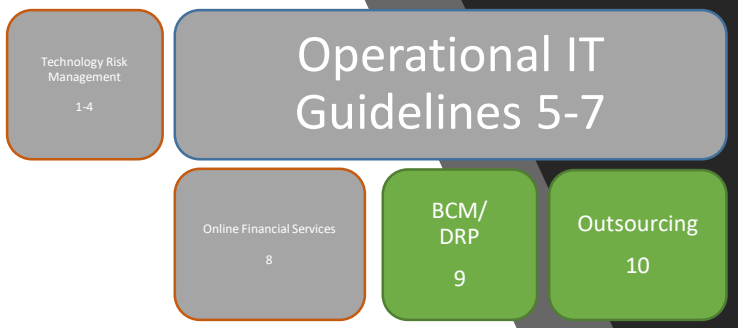


8. Online Financial Services

- Control:
  - Focus on minimizing exposure to MITMA and cyber attacks
  - Protect and secure the payment methods or platforms against fraud and abuse
  - Having procedures in place to detect fraud on ATMs and payment kiosks



9.BCM/DRP + 10. OUTSOURCING



- Aim:
  - Extend the current Business Continuity and Outsourcing guidelines with relevant specific elements for IT:
    - Disaster Recovery Plans (DRP)
    - Systems availability
    - Recovery testing
    - Cloud computing services
- Control:
  - Intensify attention on IT landscape within both guidelines

Opportunities that a regional TRM provides

- Overall elevation of the maturity level of the IT landscape of the financial sector

- Faster information sharing:
  - Opportunity for innovative projects such as TIBER-CAR
  - Cyber Security Resilience of the Regional financial sector will mature into a front runner for other vital infrastructure sectors
  - Communication to the end user by the institutions in case of a data breach in line with current international standards

Regional Triage system

Inspired by CROE (ECB)

Thank you!