Digital Financial Services Security Cyber Resilience Toolkit

Standardization Bureau, ITU

Overview

Growing reliance on Digital Financial Services (DFS)

- Increase in payment value linked to digital commerce (2017-2019: USD 1.2 trillion to USD 1.5 trillion).
- Contribution to economic growth, reduced living costs, and increased transactional security and transparency.

Challenges faced by Emerging and Developing Economies (EMDEs)

- Technological and methodological gaps.
- Lack of compliance with established leading practices.
- Vulnerability to cyberattacks.

Cyber Resilience Toolkit

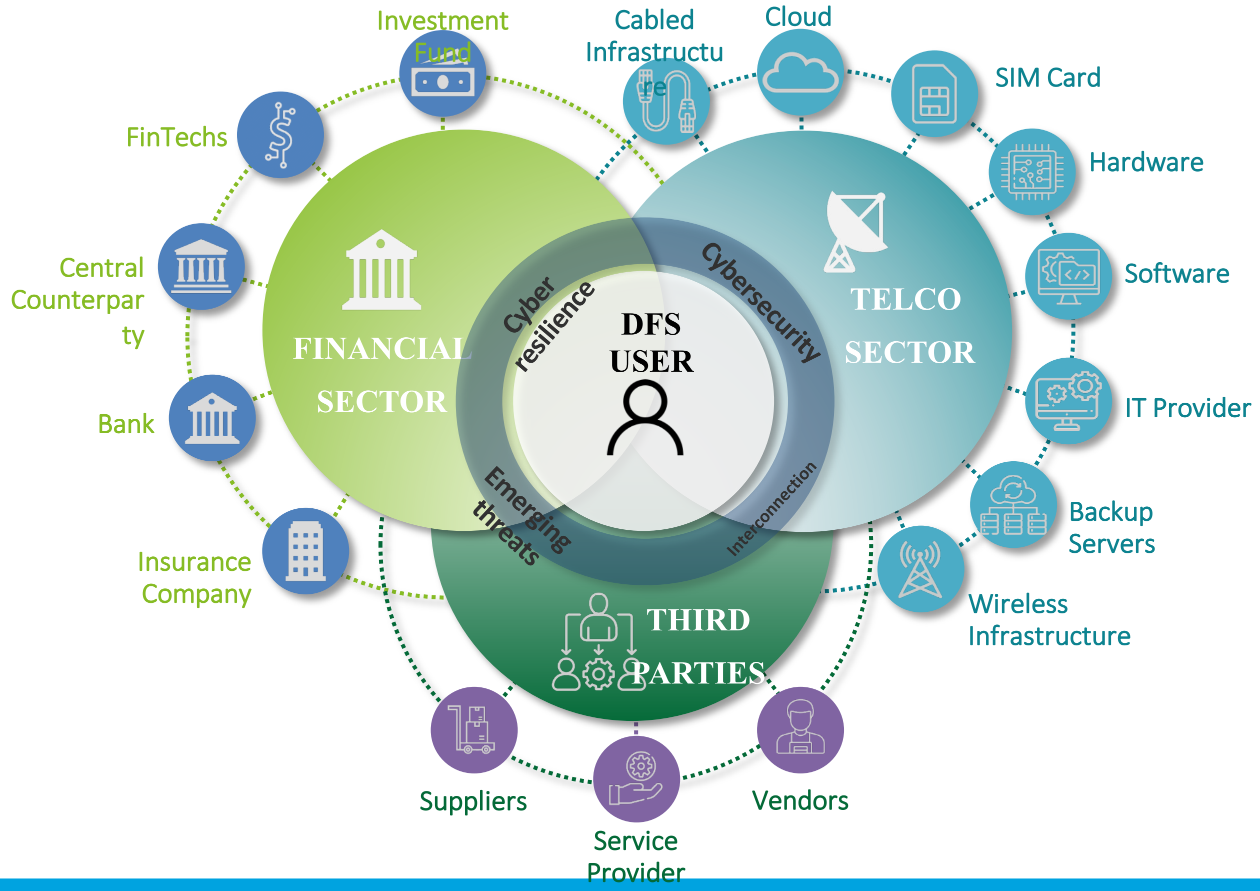
Objectives

- Facilitating cyber resilience self-assessments.
- Enhancing resiliency through strengthening peripheral and internal defenses.
- Tailoring to common threats impacting EMDEs' DFS ecosystems.

Cyber Resilience Toolkit

DFS Critical Entity Identification

- Categorizing entities based on roles and potential impact on users and national population during a cyberattack.
- Coordinating with critical entities to bolster cyber resilience.
- Criticality classification based on ownership and potential impact on consumer base.
- to identify vulnerabilities and define roadmaps for improvements.



Structure of the Cyber Resilience Assessment Toolkit

Source Leverage

- NIST Security and Privacy Controls (SP 800-53).
- EU's Digital Operational Resilience Act (DORA).
- ISO/IEC 27000-series (ISO 27001 and ISO 27005).
- Payment Card Industry Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA DSS).

Cyber Resilience Frameworks Comparison

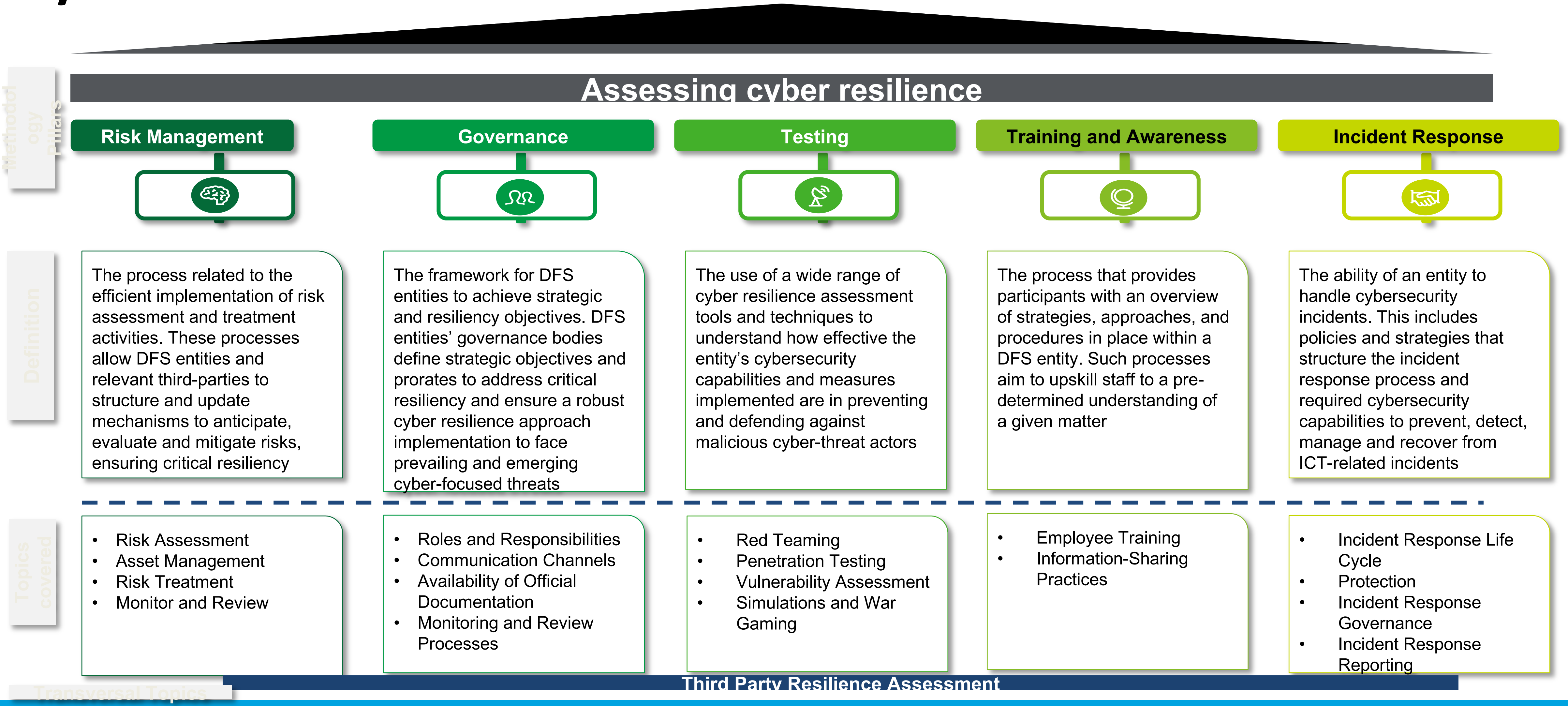
	Bank for International Settlements (BIS) – OICV-IOSCO	European Central Bank (ECB)	International Telecommunicatio n Union (ITU)	
Report	Guidance on cyber resilience for financial market infrastructures	Cyber Resilience Oversight Expectations (CROE)	DFS Cyber Resilience Assessment Toolkit	
Year	2016	2019	2023	ITU report provides an updated guidance
Domains	Governance, Identification, Protection, Detection, Response and Recovery, Testing, Situational Awareness, Learning and evolving	Governance, Identification, Protection, Detection, Response and Recovery, Testing, Situational Awareness, Learning and evolving	Risk Management, Governance, Testing, Training and Awareness, Incident Response. Each of them declined in subdomains	ITU provides a deeper level of analysis compared to ECB and BIS, by providing for each domain a sub-domain based on international standards and global guidelines
Content	The purpose of this document (Guidance) is to provide guidance for FMIs to enhance their cyber resilience.	The document presents a methodology developed by the European Central Bank to operationalize the CPMI and IOSCO Guidance on Cyber Resilience for FMIs	The document presents a methodology developed on a wider set of international standards and regulations (ISO, NIST, G7, DORA, TIBER EU)	ITU provides detailed methodological and operational guidelines in order to assess and improve the current cyber resilience level of DFS infrastructure in emerging economies. Moreover, compared to BIS and CROE, ITU provides not only the best practice but also intermediate steps to improve entities' resilience
Toolkit	Not present	Provides a set of guiding questions	Provides a toolkit to assess the DFS Cyber Resilience	ITU provides a toolkit with detailed questions to assess the resiliency, suggesting actionable improvements

Structure of the Cyber Resilience Assessment Toolkit

Toolkit Implementation:

- Five Pillars
  - Risk Management,
  - Governance,
  - Testing,
  - Training and Awareness,
  - Incident Response
- Four levels of cyber resilience maturity. (None, Basic, Intermediate, Advanced, Expert)
- Guided self-assessment through questions and controls.
- Infographics presenting final resilience assessment and areas for improvement.

Cyber Resilience Toolkit's Pillars

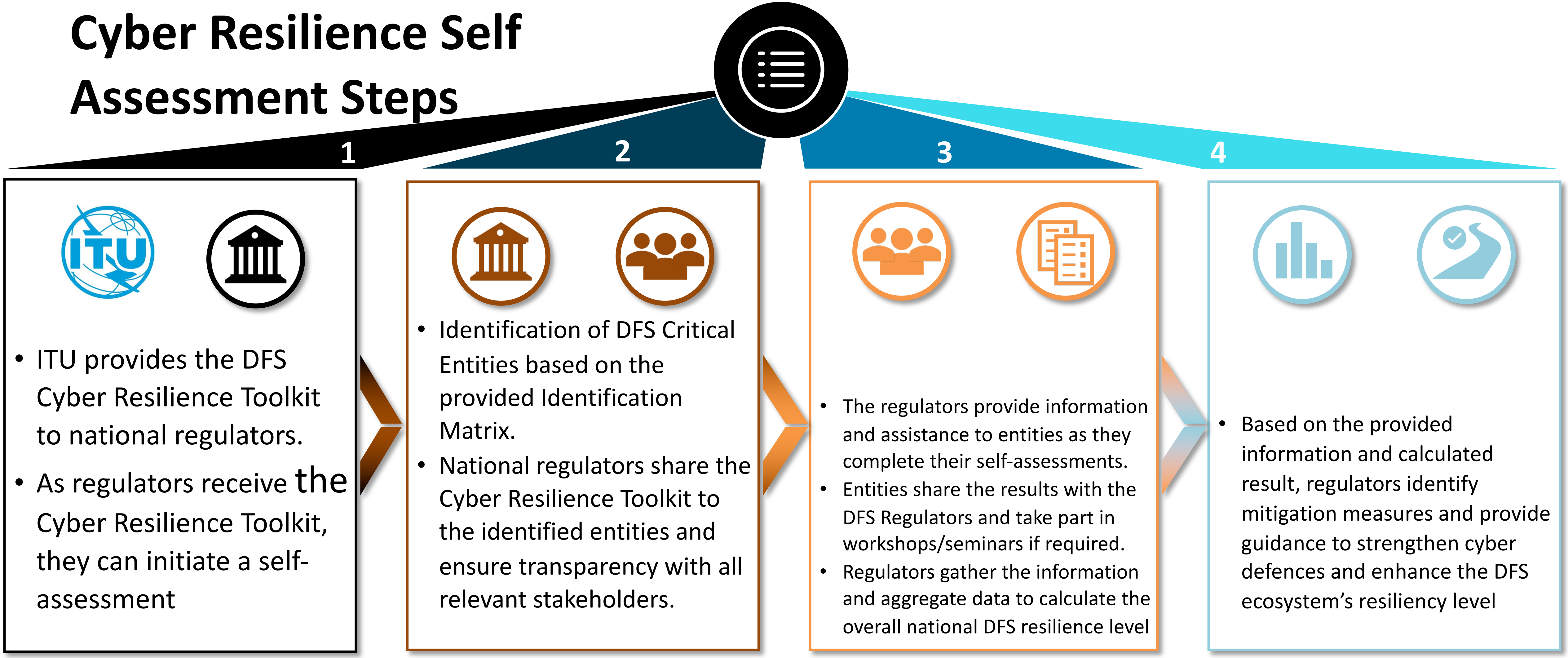


Assessing cyber resilience

Methodology Pillars	Risk Management	Governance	Testing	Training and Awareness	Incident Response
Definition	The process related to the efficient implementation of risk assessment and treatment activities. These processes allow DFS entities and relevant third-parties to structure and update mechanisms to anticipate, evaluate and mitigate risks, ensuring critical resiliency	The framework for DFS entities to achieve strategic and resiliency objectives. DFS entities' governance bodies define strategic objectives and prorates to address critical resiliency and ensure a robust cyber resilience approach implementation to face prevailing and emerging cyber-focused threats	The use of a wide range of cyber resilience assessment tools and techniques to understand how effective the entity's cybersecurity capabilities and measures implemented are in preventing and defending against malicious cyber-threat actors	The process that provides participants with an overview of strategies, approaches, and procedures in place within a DFS entity. Such processes aim to upskill staff to a pre-determined understanding of a given matter	The ability of an entity to handle cybersecurity incidents. This includes policies and strategies that structure the incident response process and required cybersecurity capabilities to prevent, detect, manage and recover from ICT-related incidents
Topics covered	• Risk Assessment • Asset Management • Risk Treatment • Monitor and Review	• Roles and Responsibilities • Communication Channels • Availability of Official Documentation • Monitoring and Review Processes	• Red Teaming • Penetration Testing • Vulnerability Assessment • Simulations and War Gaming	• Employee Training • Information-Sharing Practices	• Incident Response Life Cycle • Protection • Incident Response Governance • Incident Response Reporting

Transversal Topics: Third Party Resilience Assessment

Cyber Resilience Self Assessment Steps



1

- ITU provides the DFS Cyber Resilience Toolkit to national regulators.
- As regulators receive the Cyber Resilience Toolkit, they can initiate a self-assessment

2

- Identification of DFS Critical Entities based on the provided Identification Matrix.
- National regulators share the Cyber Resilience Toolkit to the identified entities and ensure transparency with all relevant stakeholders.

3

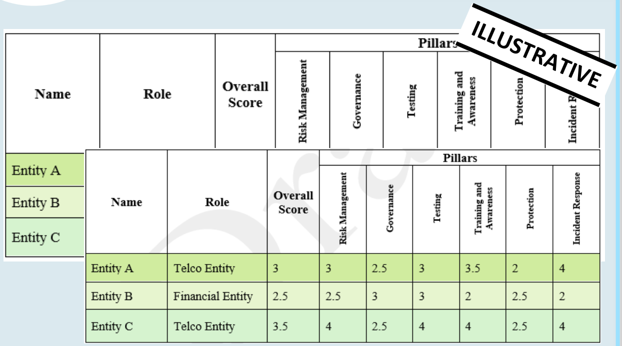
- The regulators provide information and assistance to entities as they complete their self-assessments.
- Entities share the results with the DFS Regulators and take part in workshops/seminars if required.
- Regulators gather the information and aggregate data to calculate the overall national DFS resilience level

4

- Based on the provided information and calculated result, regulators identify mitigation measures and provide guidance to strengthen cyber defences and enhance the DFS ecosystem's resiliency level

How the results would be interpreted and displayed

Data Aggregation



ILLUSTRATIVE

Name	Role	Overall Score	Pillars					
			Risk Management	Governance	Testing	Training and Awareness	Protection	Incident R
Entity A								
Entity B								
Entity C								

Name	Role	Overall Score	Pillars					
			Risk Management	Governance	Testing	Training and Awareness	Protection	Incident Response
Entity A	Telco Entity	3	3	2.5	3	3.5	2	4
Entity B	Financial Entity	2.5	2.5	3	3	2	2.5	2
Entity C	Telco Entity	3.5	4	2.5	4	4	2.5	4

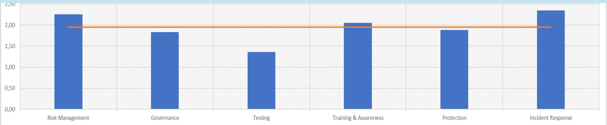
The regulator aggregates the information sent by the relevant entities to understand the overall **ecosystem's cyber resilience level**

Data Analysis

ILLUSTRATIVE

Pillar	Resiliency Score	Resilien
Risk Management	2,25	INTERMEDIATE
Governance	1,83	BASIC
Testing	1,36	BASIC
Training & Awareness	2,05	INTERMEDIATE
Protection	1,89	BASIC
Incident Response	2,35	INTERMEDIATE

Overall	1,95	BASIC



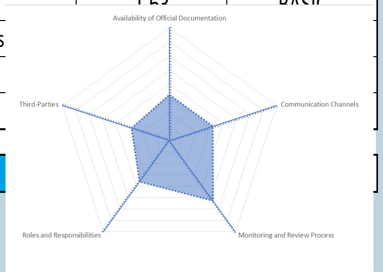
The regulator assesses the data and **granularly reviews** the entities' analysed pillars to understand what are the **weaknesses and vulnerabilities**

Data Interpretation

ILLUSTRATIVE

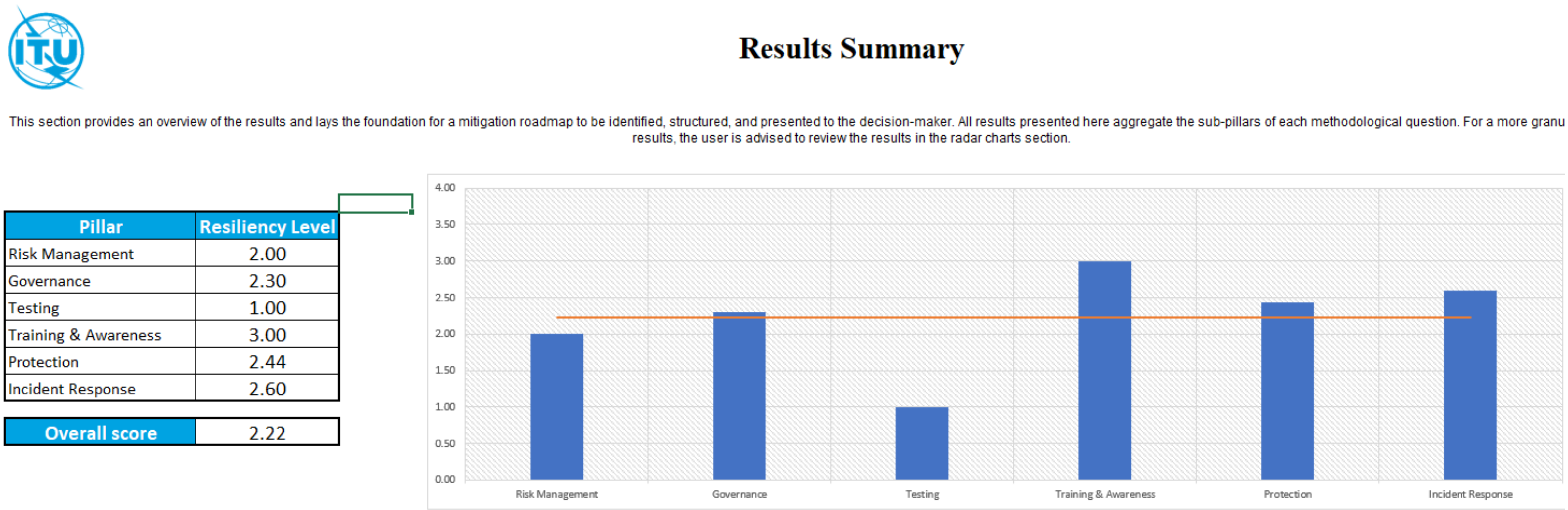
Subpillar	Resiliency Score	Level
Availability of Official Documentation	1,63	BASIC
Communication Channels	1,63	BASIC
Monitoring and Review Process		
Roles and Responsibilities		
Third-Parties		

Governance		



The data is interpreted and presented to facilitate the definition of **operational roadmaps** for the short, medium, and long-term.

Results assessment summary: Cyber Security Resilience Assessment toolkit



Results Summary

This section provides an overview of the results and lays the foundation for a mitigation roadmap to be identified, structured, and presented to the decision-maker. All results presented here aggregate the sub-pillars of each methodological question. For a more granu results, the user is advised to review the results in the radar charts section.

Pillar	Resiliency Level
Risk Management	2.00
Governance	2.30
Testing	1.00
Training & Awareness	3.00
Protection	2.44
Incident Response	2.60

Overall score	2.22

Questions

Contact: dfssecuritylab@itu.int

https://figi.itu.int/figi-resources/dfs-security-lab/