

# Cyber Resilience Toolkit for DFS Critical Infrastructure

Arnold Kibuuka, Project Officer, ITU  
[dfssecuritylab@itu.int](mailto:dfssecuritylab@itu.int)

March 2024



# Toolkit Overview

- A guide for DFS regulators to assess cybersecurity risks in digital finance infrastructure and enhance cyber preparedness.
- Rooted in ISO 27000 series standards and enriched by the Payment Aspect for Financial Inclusion (PAFI) report recommendations.

# The need for Coordination on Cyber resilience in DFS.

- **Different ecosystem stakeholders:** Financial institutions, Regulators, Telcos, Technology providers
- **Sectorial Interdependence:** the necessity for coordinated efforts between the Financial and Telco sectors to safeguard against cyber threats.
- **Cross-Sectoral Collaboration:** Encourages information sharing, joint cyber threat analysis, and coordinated response strategies.
- **Preparedness and Response:** Development of standardized incident response protocols and preparedness measures for effective management of cyber incidents.

# 2. DFS Cyber Resilience Toolkit

## DFS Ecosystem Understanding



### DFS Ecosystem Actors

All DFS Ecosystems see a profound and direct interconnection between critical assets and four main actors. These include the financial sector, the telecommunication sector, third-parties, and the DFS final user.



**The Technical Report** The Methodology and a deeper focus into the analysis of the DFS ecosystem is contained in a Word document, which will be shared with all relevant and identified entities.



**Methodology** The establishment of a Cyber Resilience Toolkit to self-test DFS entities' cyber preparedness dictates the definition of a resilience methodology that considers multiple international frameworks and standards.

## DFS Ecosystem Resilience Self-Assessment



### DFS Resilience Toolkit Phases

To successfully complete the self-assessment, entities and regulators are encouraged to follow an operational path divided into four critical steps.



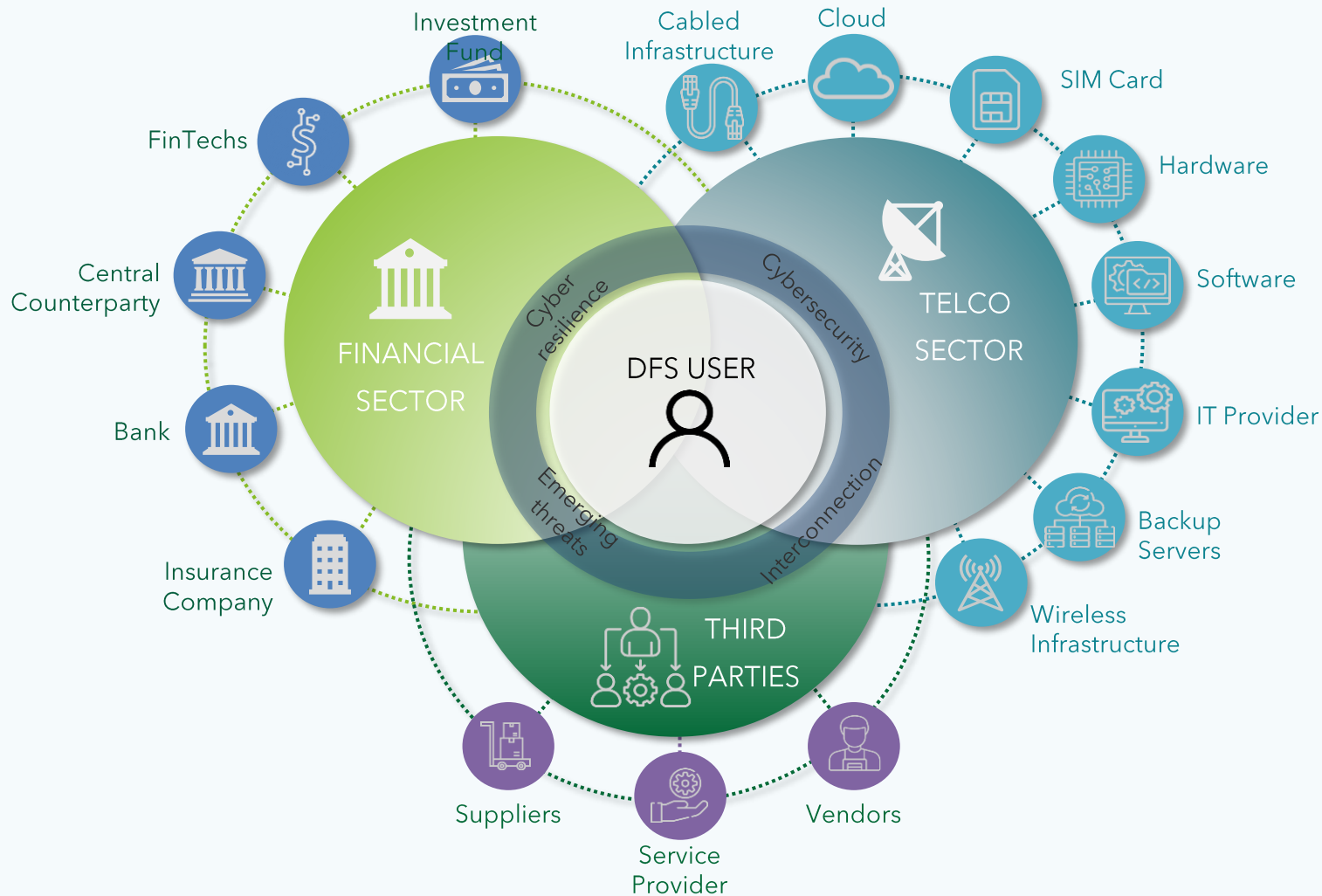
**Toolkit Questions** The Toolkit includes questions that aim to test the entity's cyber resilience level. The toolkit's questions must be answered truthfully to reflect the true status of cyber preparedness.



**Guidance Results Assessment** As entities complete the tests, the results are portrayed in bar charts, radar charts, and ad-hoc infographics to facilitate the identification of weakness, data sharing, and roadmapping.

# The DFS Ecosystem

Ecosystem actors, threats and vulnerabilities



## Most common vulnerabilities and threats



- Credential Attacks
- Systems and Platforms Attacks
- Code Exploitation Attacks
- Data Misuse Attacks
- Denial of Service Attacks
- Insider Attacks
- Social Engineering Attacks
- DFS Infrastructure Attacks
- SIM Attacks
- DFS Services Attacks
- DFS Data Attacks
- Malware Attacks
- Zero-day Attacks
- Mobile Devices Attacks
- Personal Information Attacks

# The Technical Report



The analysis of the DFS ecosystems and its main actors is contained in a technical report, which will be provided to all relevant entities and will include a tailored methodology to introduce the self-assessment Toolkit

## Key characteristics of the Word Document



Includes a deep dive into the DFS Ecosystem



Focuses predominantly on Emerging Markets and Developing Economies (EMDEs)



Includes a high-level strategic overview over the most common threats, risks, and vulnerabilities



Includes a cutting-edge methodology that takes into account the latest cyber-related policies and frameworks



The Word document lays the needed theoretical foundation to use the Toolkit and define ways to improve the ecosystem's cyber resilience level



It contains an annex with all provided Cyber Resilience questions

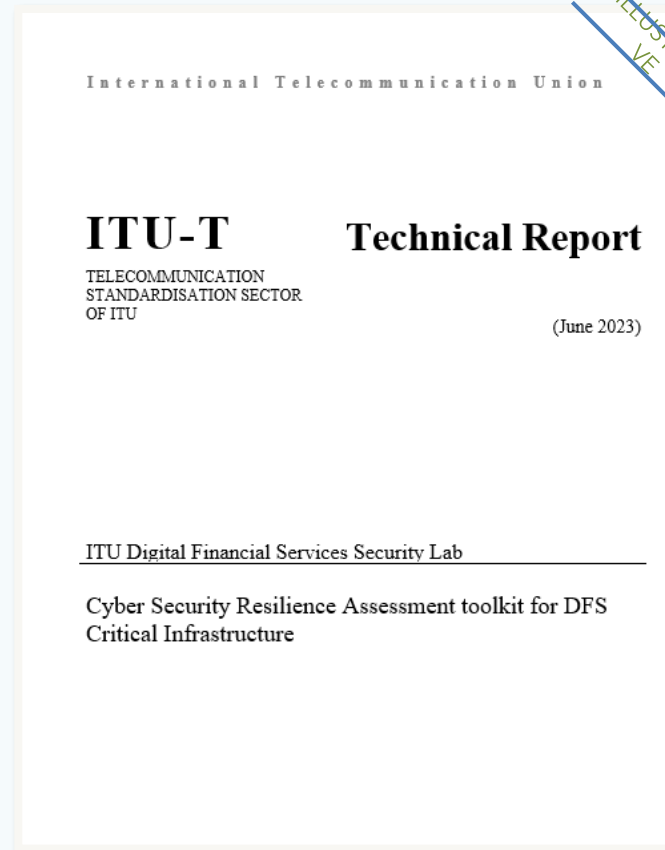
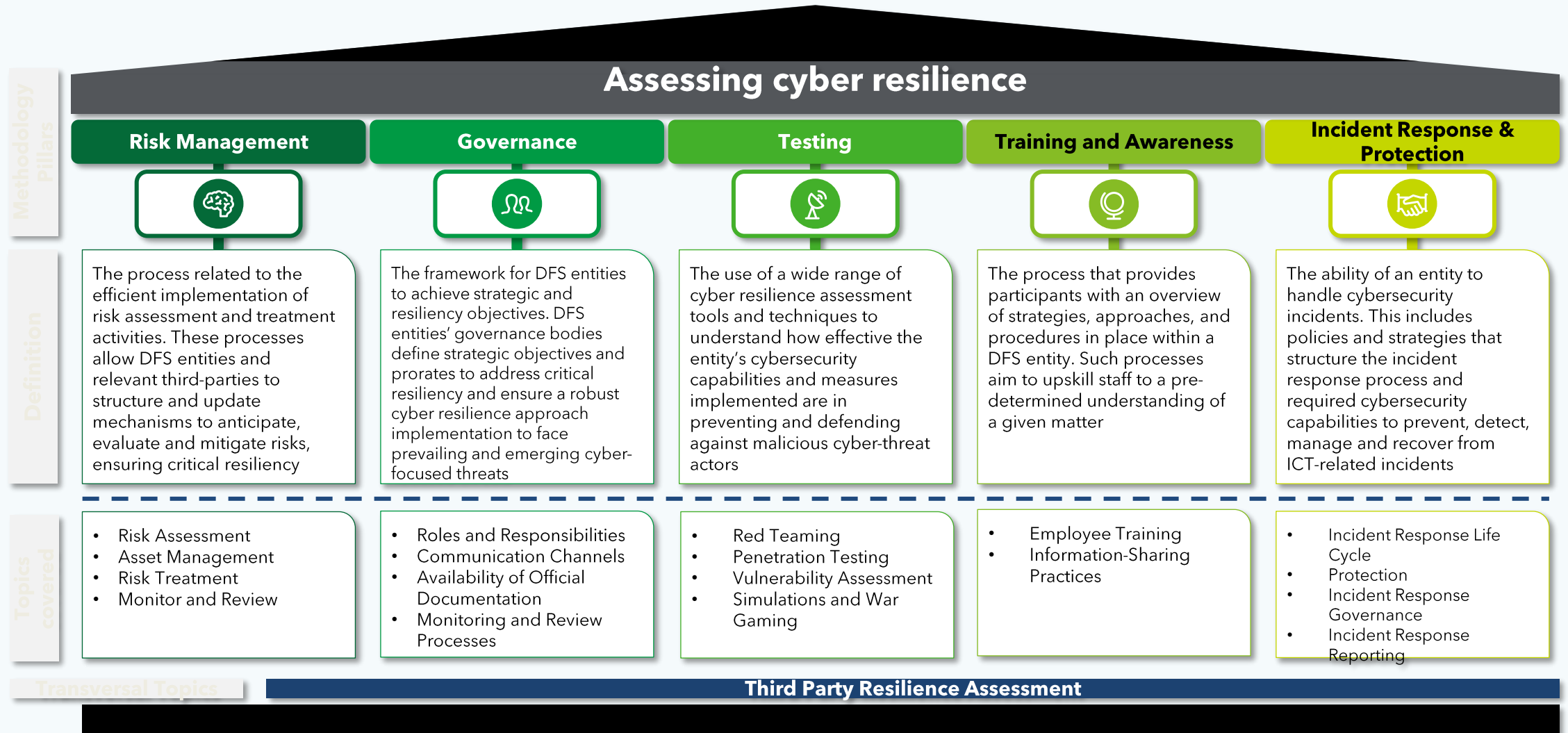


TABLE OF CONTENTS	
	Page
<b>PRELIMINARY ELEMENTS</b> .....	<b>3</b>
CONTEXT .....	3
SUMMARY .....	3
SCOPE .....	3
KEYWORDS .....	3
REFERENCES .....	4
TAXONOMY AND TERMINOLOGY .....	9
Terms defined elsewhere: .....	9
Terms defined here .....	18
ABBREVIATIONS AND ACRONYMS .....	19
<b>CYBERSECURITY RESILIENCE ASSESSMENT TOOLKIT FOR DFS CRITICAL INFRASTRUCTURE</b> .. 21	
1 OVERVIEW .....	21
2 CYBER RESILIENCE TOOLKIT .....	22
2.1 Objectives .....	22
2.2 DFS Critical Entity Identification Matrix .....	22
2.3 Structure of the Cyber Resilience Assessment Toolkit .....	23
2.4 How regulators would use the Toolkit for the cyber resilience assessment of DFS entities .....	25
2.5 Example .....	26
3 MAPPING THE DFS INFRASTRUCTURE .....	28
3.1 Identified Actors .....	28
3.2 DFS Vulnerabilities, Most Common Threats, and Related Mitigation Measures .....	31
3.3 Main Considerations on Mapping the DFS Infrastructure .....	38
4 ESTABLISHING A METHODOLOGY .....	40
4.1 Risk Management .....	42
4.1.1 Risk Assessment .....	42
4.1.2 Risk Treatment .....	46
4.1.3 Monitor and Review .....	48
4.1.4 Third-Parties' Risk Management .....	49
4.2 Governance .....	51
4.2.1 Roles and Responsibilities .....	51
4.2.2 Communication Channels .....	52
4.2.3 Availability of Official Documentation .....	53
4.2.4 Monitoring and Review Processes .....	54
4.2.5 Third-Parties' Governance .....	54
4.3 Testing .....	56
4.3.1 Red Teaming .....	56
4.3.2 Penetration Testing .....	57
4.3.3 Vulnerability Scanning .....	58
4.3.4 Simulations and War Gaming .....	59
4.3.5 Third-Parties' Testing .....	60
4.4 Training and Awareness .....	62
4.4.1 Employee Training .....	62
4.4.2 Information-Sharing Practices .....	63
4.4.3 Third-Parties' Training and Awareness .....	65
4.5 Incident Response .....	66
4.5.1 Incident Response Life Cycle .....	66
4.5.2 Incident Response Governance .....	73
4.5.3 Incident Response Reporting .....	75
4.5.4 Third-Parties' Incident Response .....	77
<b>CONCLUSION</b> .....	<b>79</b>
<b>APPENDIX A - DFS CYBER RESILIENCE ASSESSMENT TOOLKIT QUESTIONS</b> .....	<b>80</b>

# Methodology

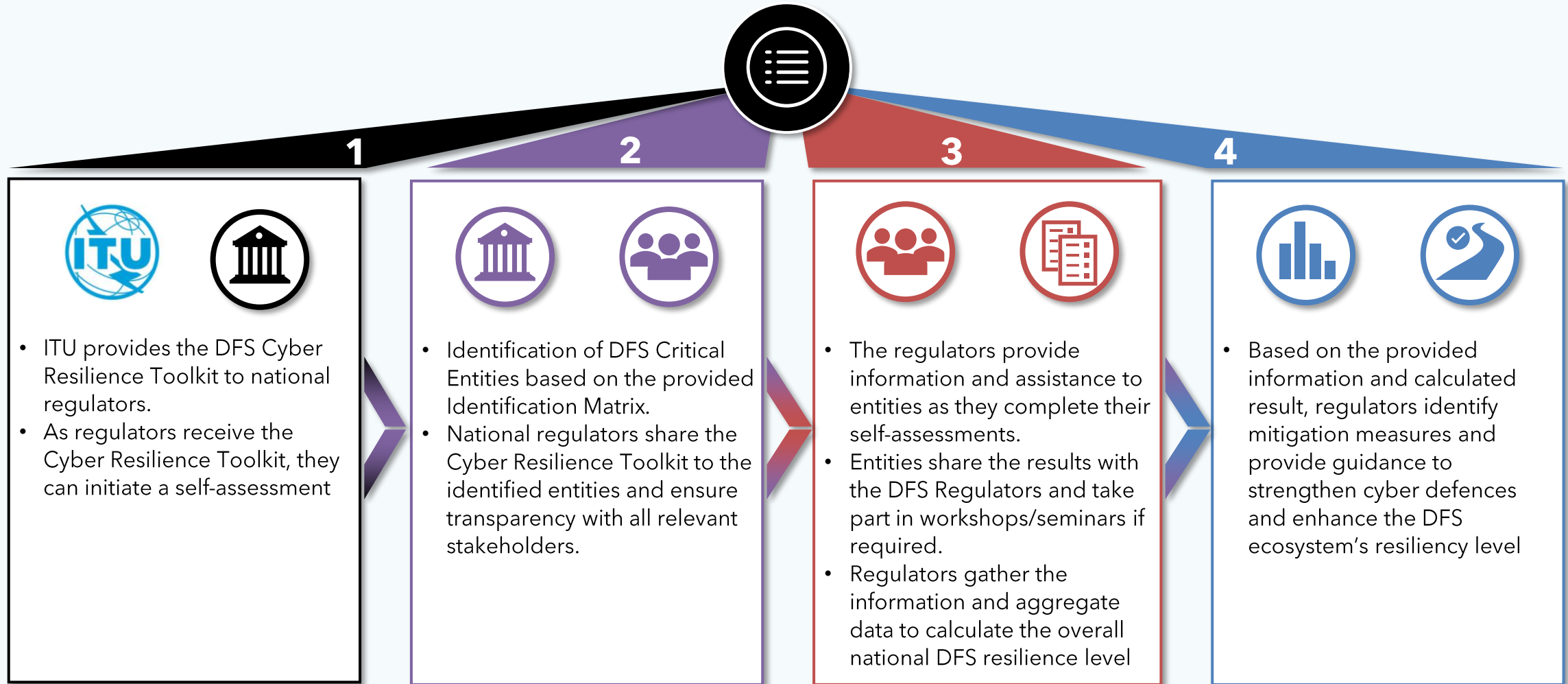
The DFS Resilience Toolkit's Pillars represent the main areas or categories of focus for the DFS Ecosystem Resilience analysis. Each Methodology Pillar leads to the definition of a specific categories of questions within the Toolkit



# Assessment phases



Below is an overview of the expected phases of toolkit's life-cycle. The process begins from the interactions between ITU and national regulators and progress towards the gathering and analysis of data and results





# Toolkit - Questions (1/3)

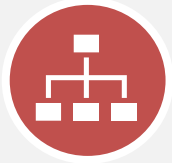


Toolkit's Questions are provided to users in categories. Each Category, or toolkit's sheet containing specific questions related to the corresponding methodology's Pillar.

## DFS Toolkit's Pillars



**Risk Management**



**Governance**



**Testing**



**Training & Awareness**



**Protection**



**Incident Response**



## DFS Toolkit's Domains



### **Risk Management**

*Identification, estimation and prioritisation of risk related to multiple diverse actors and processes.*



### **Governance**

*The framework for DFS entities to achieve strategic and resiliency objectives. This is critical to ensure a robust cyber resilience approach implementation to face prevailing and emerging cyber-focused threats*



### **Testing**

*Assessment of an organization's cybersecurity capabilities and measures implemented to understand how effective they are in preventing and defending against malicious cyber-threat actors*



### **Training & Awareness**

*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*



### **Protection**

*Guidelines provision for securing the entity's data, systems, networks, and applications. Furthermore, it assesses how to establish an incident response capability to prepare the organisation for malicious cyber events*



### **Incident Response**

*The ability of an organisation to handle cybersecurity incidents. This includes policies and strategies that structure the incident response process and required cybersecurity capabilities to detect, manage, and recover from ICT-related incidents*

# Toolkit - Questions (2/3)



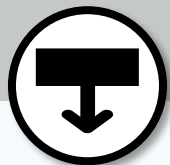
Each question, or row of the Toolkit's sheet, is composed of several columns. For each column, the cell provides information concerning the specific question such as Pillar and Sub-pillar, ID, Applicability and Question's content.

**Cyber resiliency Questions are structured as follows:**

Pillar	Subpillar	ID	Applicability	Question
Risk Management	Third-Parties	RM.01	FS Entity / Telco Entity	Is the entity reliant on a specific supplier? Does it have a business continuity plan in place in case suppliers or other linked services are unavailable?

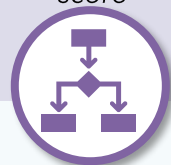
## Pillars

Main category of Methodology's Pillar. Each section (sheet) of Toolkit's questions will have the same Pillar as reference. This distinction will be leveraged to further analyse and detail overall score



## Sub-Pillar

Sub-categories of Methodology's Pillar. Depending on the specific Pillar, each section (sheet) of Toolkit's questions will have several sub-pillars as reference. This distinction will be leveraged to further analyse and detail overall score



## ID

Identificatory code to facilitate cross-communication



## Applicability

Applicability of the question to the nature of the actor undertaking the assessment  
The user will filter the applicability column to ensure that it is only shown applicable questions. The categories identified are:

- FS Entity
- Telco Entity
- FS Entity / Telco Entity
- FS Regulator
- Telco Regulator
- FS Regulator / Telco Regulator



## Question

Each row of the sections (sheet) will provide a set of Question related to the identified Pillars and Sub-Pillars. Having filtered Questions based on the Applicability, users will answer applicable questions



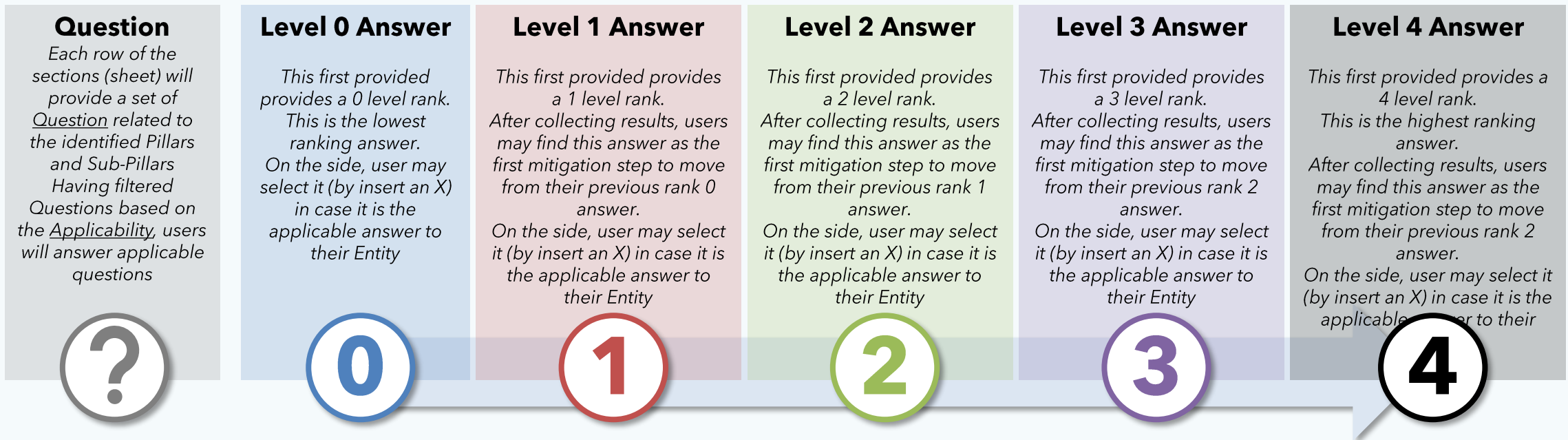
# Toolkit - Questions (3/3)

Below is an overview of the second part of Toolkit's Questions.



## Cyber resiliency Questions are structured as follows:

Question	Resilience level 0	Resilience level 1	Resilience level 2	Resilience level 3	Resilience level 4
Is the entity reliant on a specific supplier? Does it have a business continuity plan in place in case suppliers or other linked services are unavailable?	Yes, the entity relies on a supplier, but it currently has no business continuity plan.	Yes, the entity is reliant on a supplier. It has a preliminary continuity plan, but it is still basic and not fully functioning	Yes, the entity is reliant on a supplier, but management has started to diversify the relationships with other third-parties	No, the entity is not reliant on a specific supplier but it has no business continuity plan	No, the entity is not reliant on a specific supplier, and it has a coherent, over-reaching, and functioning business continuity plan



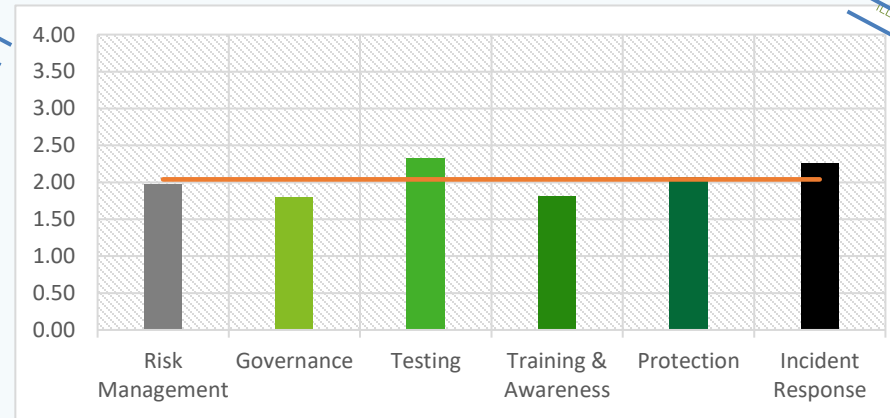
# Toolkit - Results



The self-assessment's results will provide information based on Overall score, Pillars' score and Sub-pillars' score, and will facilitate the identification of weaknesses in the ecosystem

## Overall Score

Pillar	Resiliency Score	Resiliency Level
Risk Management	1,97	BASIC
Governance	1,79	BASIC
Testing	2,33	INTERMEDIATE
Training & Awareness	1,81	BASIC
Protection	2,07	INTERMEDIATE
Incident Response	2,26	INTERMEDIATE
<b>Overall</b>	<b>2,04</b>	<b>INTERMEDIATE</b>



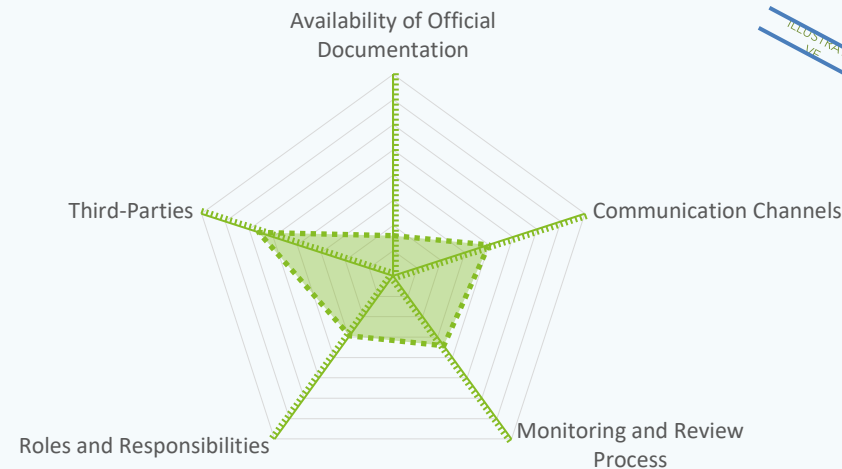
## DFS Resilience toolkit Score

The DFS Cyber Resilience Toolkit provides entities and regulators undertaking the self-assessment with:

- An **overall score** showing the cyber resilience level of the user per Pillar.
- An **individual score** per Pillar, showing the cyber resilience level of the user per Sub-pillar. The radar charts allow the user to understand the main shortcomings for each Pillar and Sub-pillar.

## Governance Score

Subpillar	Resiliency Score	Resiliency Level
Availability of Official Documentation	0,80	NONE
Communication Channels	2,00	INTERMEDIATE
Monitoring and Review Process	1,71	BASIC
Roles and Responsibilities	1,47	BASIC
Third-Parties	2,80	INTERMEDIATE
<b>Governance</b>	<b>1,79</b>	<b>BASIC</b>



# How can it support you?

The Cyber Resilience Toolkit and Methodology support the correct identification of cyber threats, risks, and mitigation measures. The document provided includes strategic points of cutting-edge and innovative methodological frameworks that will facilitate the improvement of DFS actors' resilience levels, cyber preparedness, and knowledge of the most common threats, risks, and vulnerabilities.



## Advantages

### Tailored set of DFS questions

The ITU Cyber Resilience Assessment documents provide a tailored set of DFS-focused questions that aim to review, assess, and strengthen the digital financial ecosystem. This includes a particular focus on DFS actors, threats most commonly identified in DFS operations, and scenarios specific to digital financial services.

### Focus on Emerging Markets

While digital financial services expand worldwide, this ITU document focuses predominantly on instances related to emerging markets and developing economies. This methodology and the affiliated toolkit support the identification of threats and risks that may cause critical service disruption in emerging economies. By initiating the self-assessment, DFS actors mitigate the risk of malicious operations and take steps to improve peripheral and internal defences.

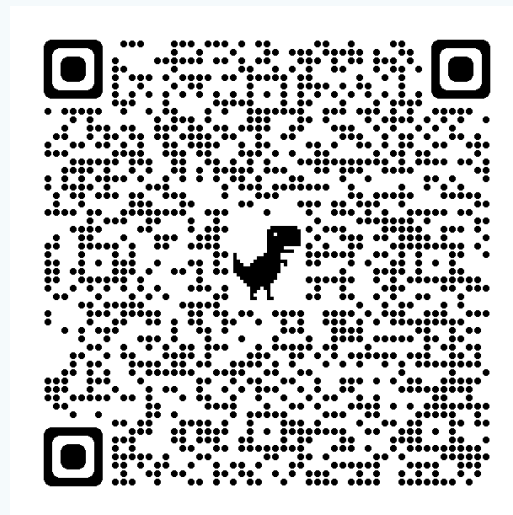


### Cutting-edge frameworks

The documents take into consideration the latest cutting-edge cybersecurity methodological frameworks, such as the EU-sponsored Digital Operational Resilience Act (DORA). By including such frameworks, the Cyber Resilience Assessment Toolkit and Methodology want to support emerging economies and more developed realities in embarking in strategic and tactical managerial overhauls that would increase short-term and long-term cyber resilience.

### Identification of improvement measures

The documentation shared with this project will facilitate the identification of weaknesses in any world-wide DFS ecosystems. The profiling of risks, threats, and vulnerabilities will in turn enhance regulators' ability to standardize incident response plans, define operational roadmaps, and mitigate threats.



<http://www.itu.int/go/dfssl>

**Contact:** [dfssecuritylab@itu.int](mailto:dfssecuritylab@itu.int)

**Thank you!**