

Cyber Resilience Toolkit for DFS Critical Infrastructure

dfssecuritylab@itu.int

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.

DFS Cyber Resilience Toolkit



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.



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.



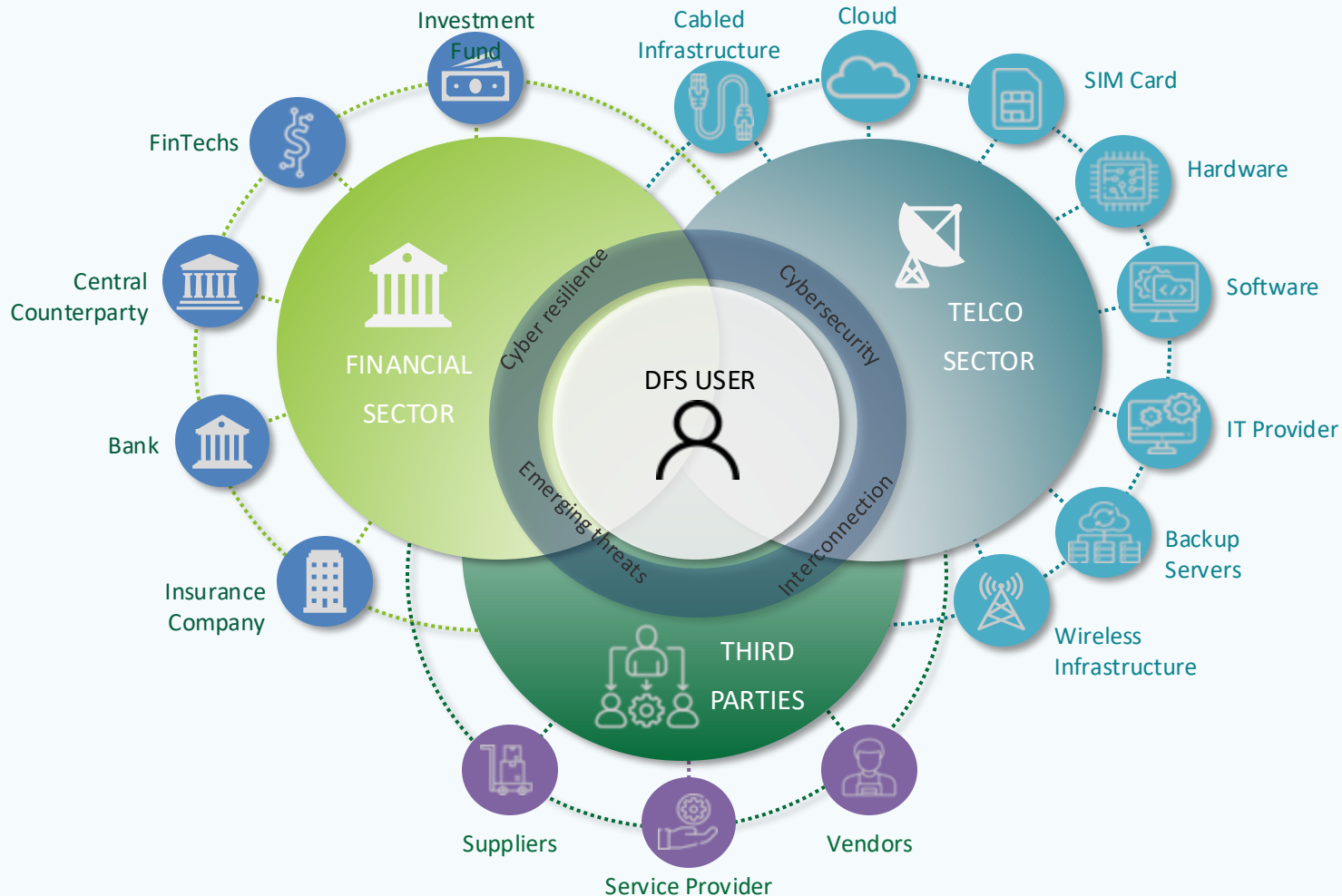
Toolkit Questions The Toolkit includes questions that aim to test the entity's cyber resilience level. The toolkit's questions must be answered truthfully to reflect the true status of cyber preparedness.



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

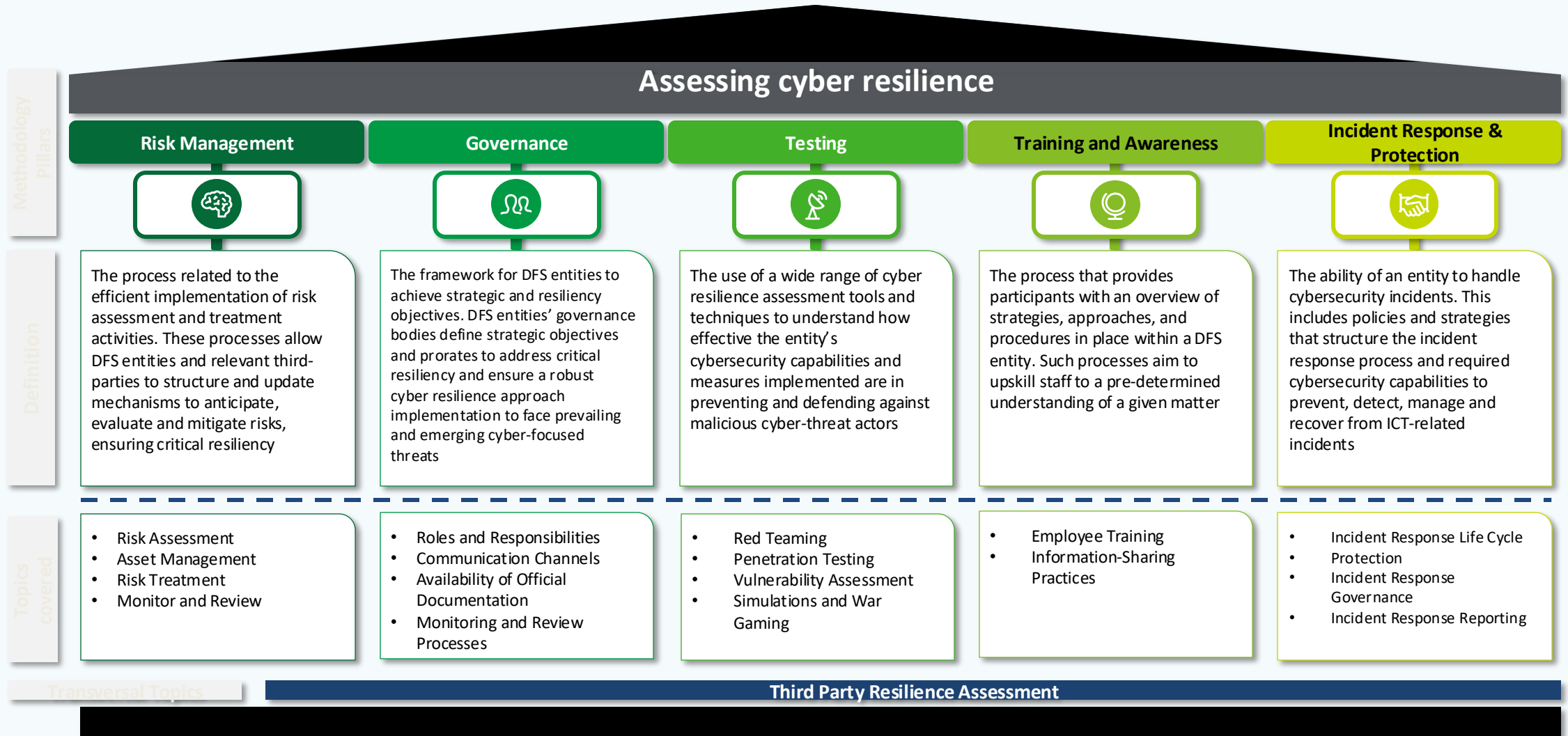
DFS Critical Entity Identification Matrix

		Entity ownership			
		Private	Private – Government Owned Corporation	Government - Local	Government - Federal
Entity's Customers (as % of the overall potential national consumer base) impacted by a disruption of services provided	< 20%	Non-Significant	Minor Entity	Minor Entity	Critical Entity
	20%	Minor Entity	Minor Entity	Major Entity	Critical Entity
	40%	Minor Entity	Major Entity	Major Entity	Critical Entity
	60%	Major Entity	Major Entity	Critical Entity	Critical Entity
	80%	Major Entity	Critical Entity	Critical Entity	Critical Entity
	> 80%	Critical Entity	Critical Entity	Critical Entity	Critical Entity
<u>Disclaimer</u>	Due to the nature of the DFS ecosystem, small and private enterprises may retain a close relationship with government and federal organisations, potentially representing a point of entry for malicious actors or malevolent lateral movement. For this reason, this toolkit warns that while the presented categorisation of private, government, and federal organisations stands in most cases, the interconnected nature of the DFS architecture urges a closer analysis of each entity before judging their positions and role in the ecosystem.				

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



Toolkit – Questions (1/3)

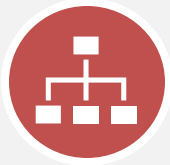
Toolkit's Questions are provided to users in categories. Each Category, or toolkit's sheet containing specific questions related to the corresponding methodology's Pillar.



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?

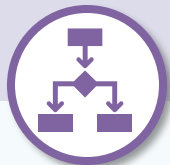
Pillars

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



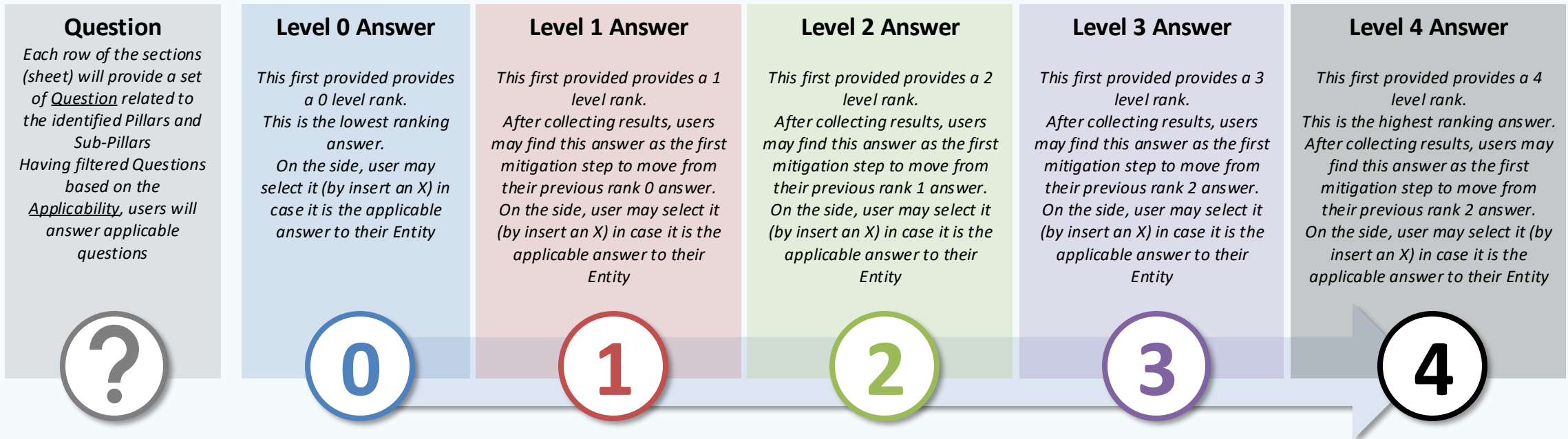
Toolkit – Questions (3/3)

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	



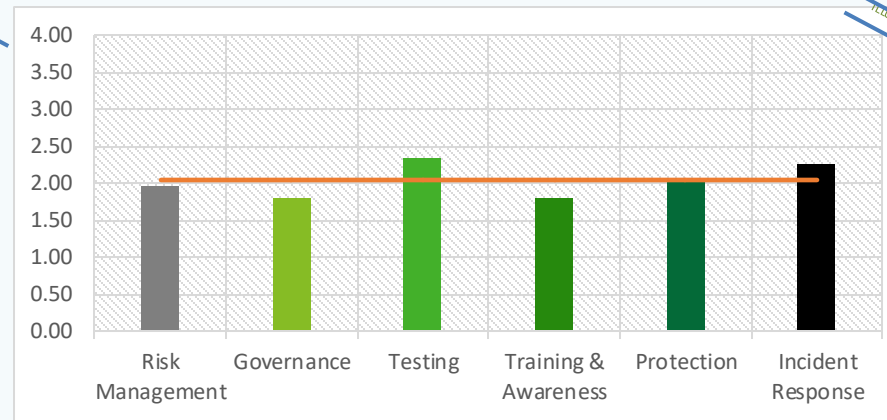
Toolkit - Results

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
Overall	2,04	INTERMEDIATE



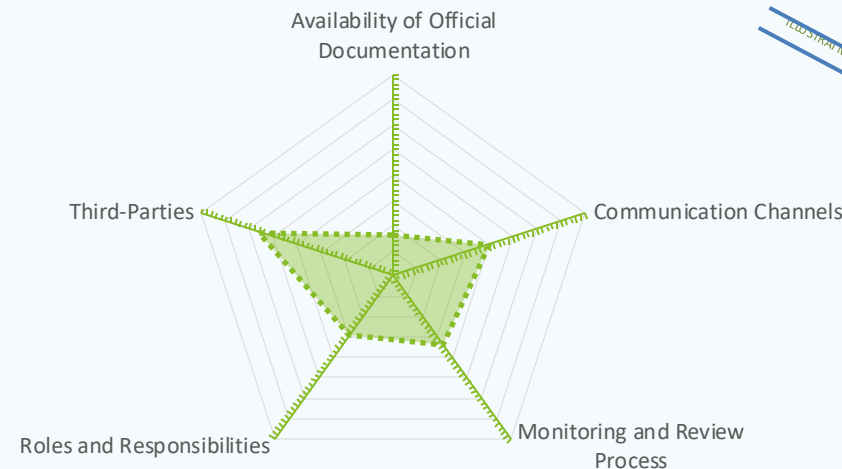
DFS Resilience toolkit Score

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
Governance	1,79	BASIC



ITU technical support Cyber Security resilience assessment for DFS critical infrastructure using the toolkit

01

Phase 1

- Identify Focal Points
- Identify Critical Infrastructure for DFS
- Identify Key Personnel
- ITU Mission for the capacity building
- Briefing of the critical infrastructure service providers identified.

02

Phase 2

- Capacity building on the cyber resilience assessment toolkit
- Knowledge transfer for the regulator on filling out and evaluating a real case questionnaire for the cyber resilience

03

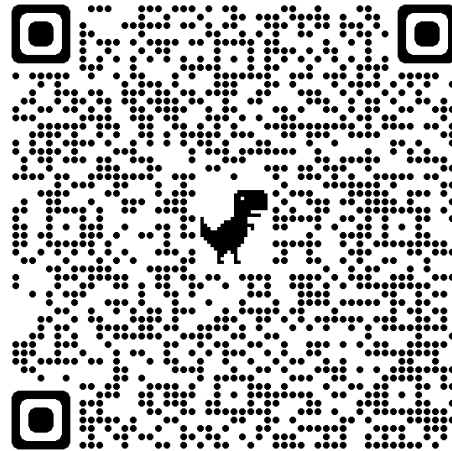
Phase 3

- Coordination with the service providers to respond to the questionnaire for the cyber resilience assessment and assist wherever necessary.
- Analysis of the responses received.
- Report Preparation and review
- Communication of results
- Prioritize Enhancements
- Development of Road Map for monitoring cyber resilience of DFS

04

Phase 4

- Coordination meetings for roadmap implementation.
- 4.2 Second cyber resilience assessment after 1 year.



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

Contact: dfssecuritylab@itu.int

Thank you!