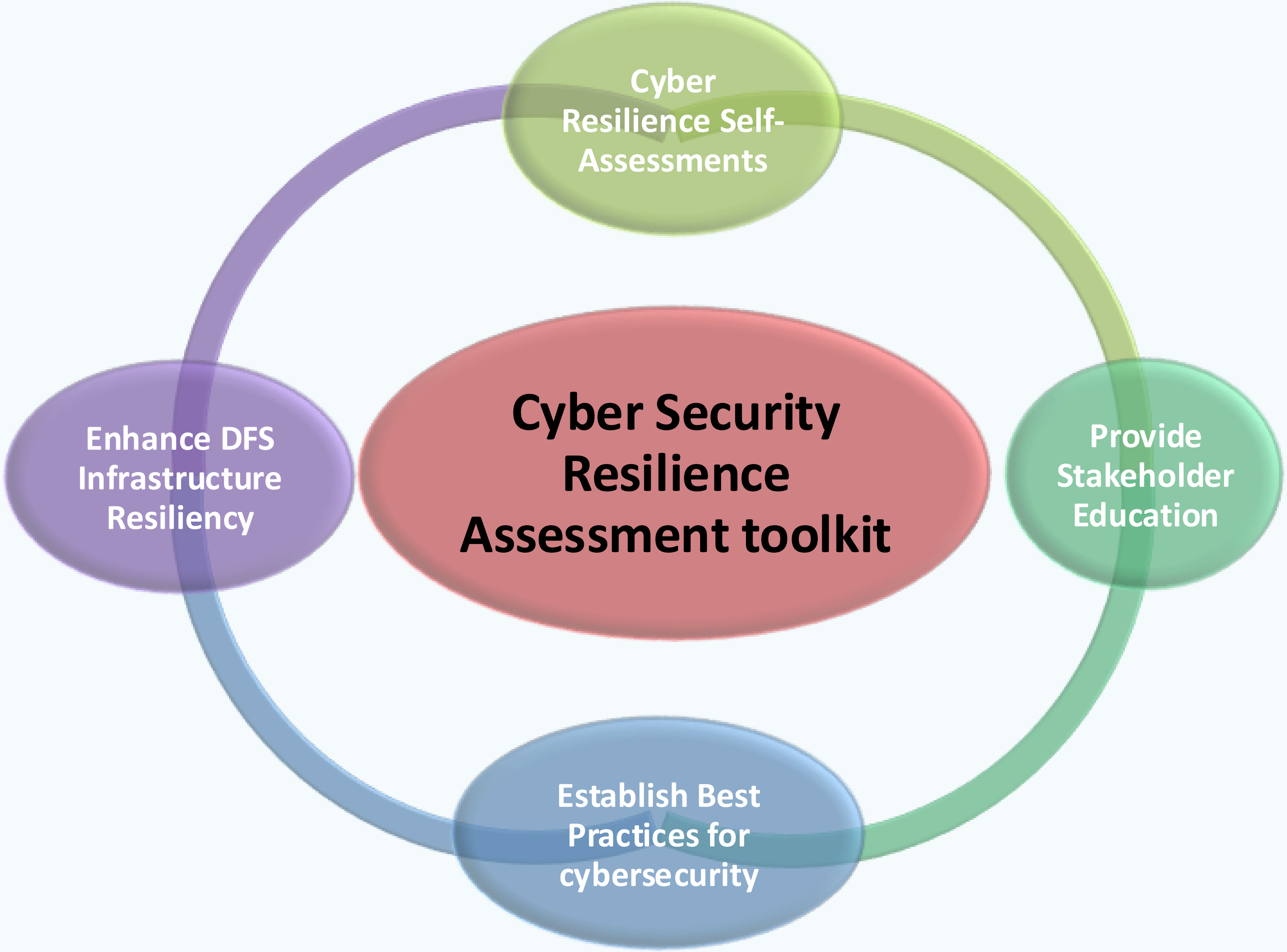
Cyber Resilience Toolkit for DFS Critical Infrastructure

Arnold Kibuuka, Project Officer, ITU

January 2025

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

Toolkit Goals



Cyber Security Resilience Assessment toolkit

Cyber Resilience Self-Assessments

Provide Stakeholder Education

Establish Best Practices for cybersecurity

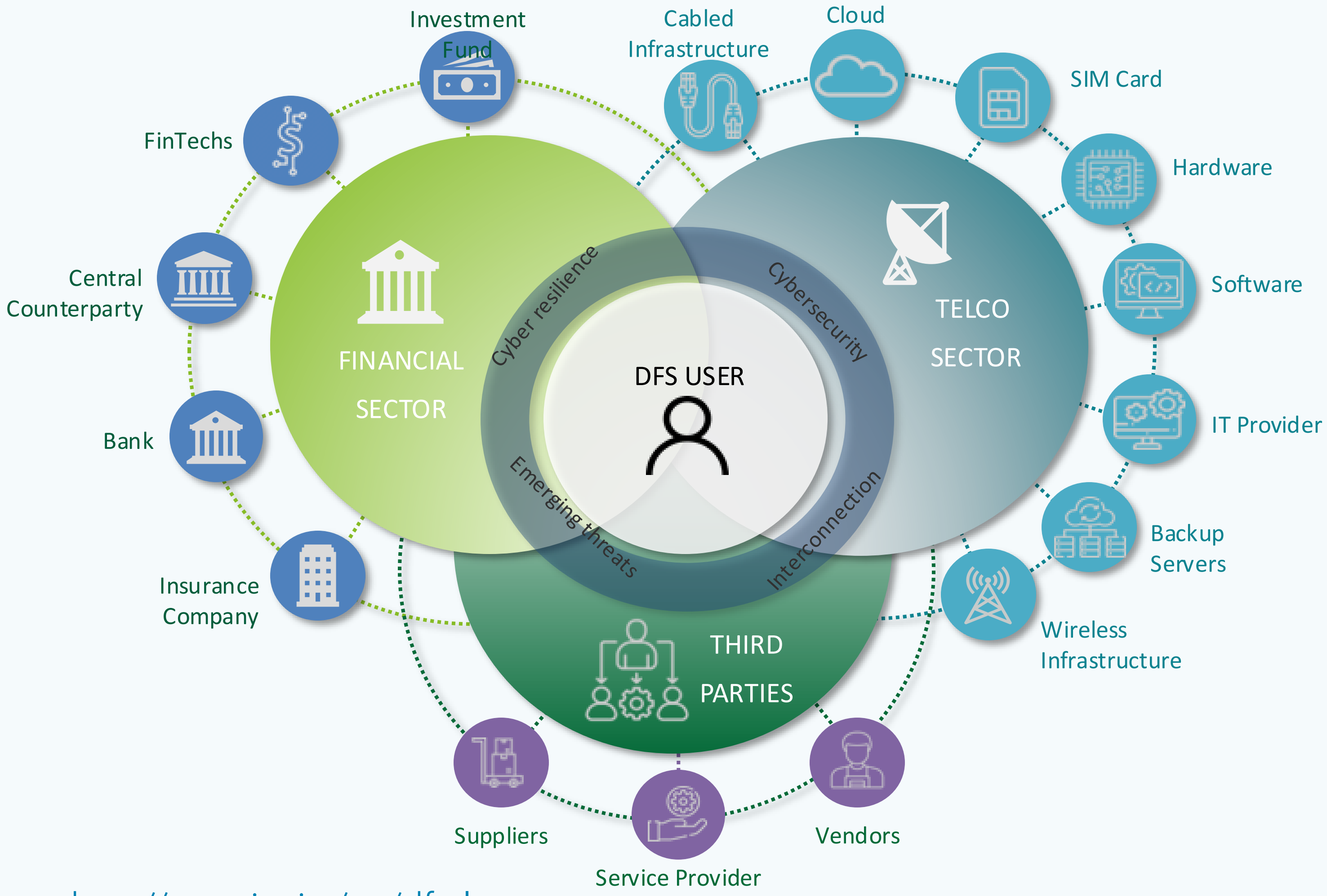
Enhance DFS Infrastructure Resiliency

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.
- Focuses on emerging economies and developing economies.
- Contains questions and a toolkit that regulators and providers can use to know the countries level of resilience.

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**
Disclaimer	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

Assessing cyber resilience

Methodology Pillars	Risk Management	Governance	Testing	Training and Awareness	Incident Response & Protection
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

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

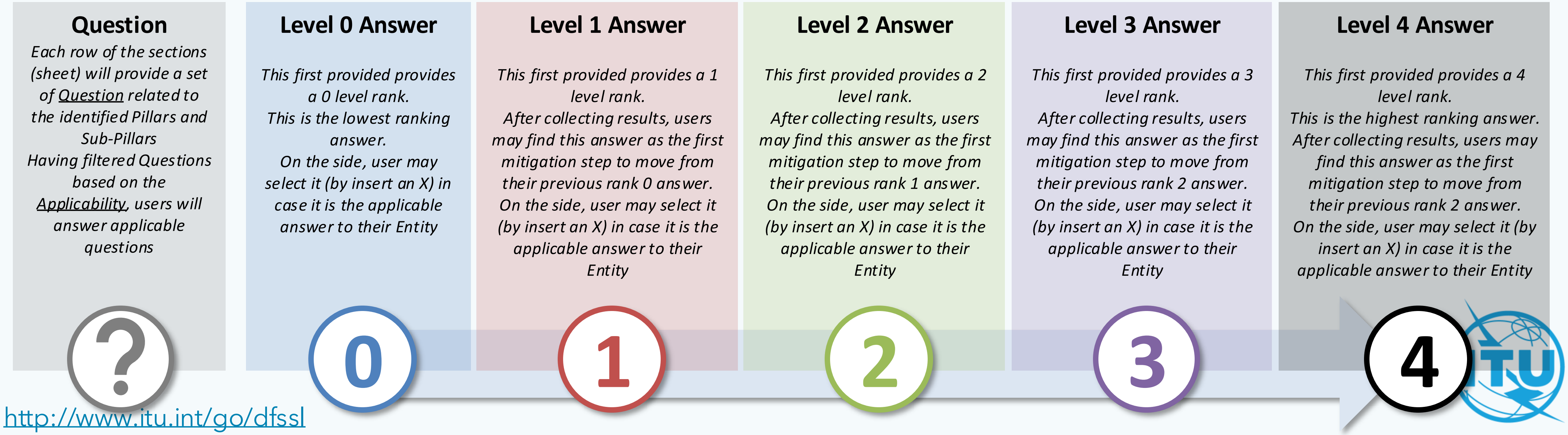
Each row of the sections (sheet) will provide a set of Question related to the identified Pillars and Sub-Pillars
Having filtered Questions based on the Applicability, users will answer applicable questions

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	



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

Level 0 Answer

This first provided provides a 0 level rank. This is the lowest ranking answer. On the side, user may select it (by insert an X) in case it is the applicable answer to their Entity

Level 1 Answer

This first provided provides a 1 level rank. After collecting results, users may find this answer as the first mitigation step to move from their previous rank 0 answer. On the side, user may select it (by insert an X) in case it is the applicable answer to their Entity

Level 2 Answer

This first provided provides a 2 level rank. After collecting results, users may find this answer as the first mitigation step to move from their previous rank 1 answer. On the side, user may select it (by insert an X) in case it is the applicable answer to their Entity

Level 3 Answer

This first provided provides a 3 level rank. After collecting results, users may find this answer as the first mitigation step to move from their previous rank 2 answer. On the side, user may select it (by insert an X) in case it is the applicable answer to their Entity

Level 4 Answer

This first provided provides a 4 level rank. This is the highest ranking answer. After collecting results, users may find this answer as the first mitigation step to move from their previous rank 2 answer. On the side, user may select it (by insert an X) in case it is the applicable answer to their Entity

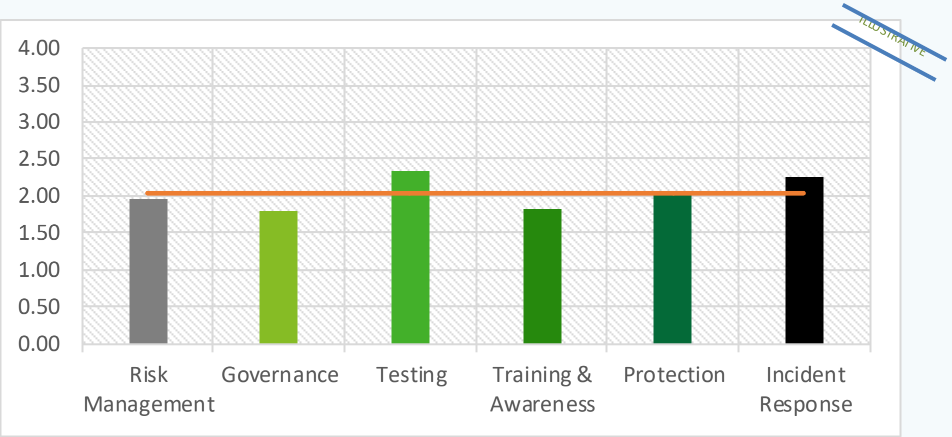
ITU DFS Security Lab

Toolkit - Results

The self-assessment's results will provide information based on Overall score, Pillars' score (None, Basic, Intermediate, and Sub-pillars' score, and will facilitate the identification of weaknesses in the ecosystem

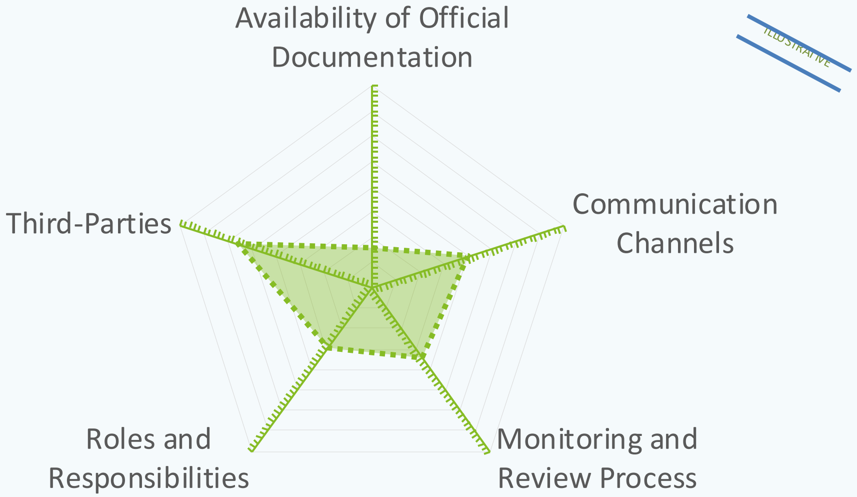
Overall Score

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



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



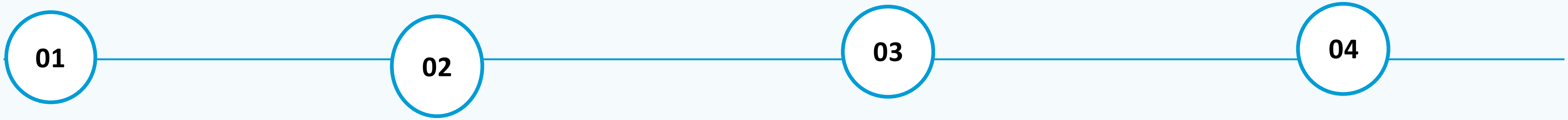
DFS Resilience toolkit Score

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.

Technical assistance for Cyber Resilience Assessment toolkit

Technical assistance for regulators to facilitate cyber resilience self-assessments and enhance the resiliency of the Digital Financial Services (DFS) infrastructure.



Phase 1: Planning and Focal Point Identification (Month 1-2)

- First meeting
- 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

Phase 2: Explaining the Cyber resilience assessment toolkit with a tabletop exercise. (Month 3-4)

- Phase 3 planning
- 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

Phase 3: Cyber resilience Assessment of Critical Infrastructure (Month 4-5)

- 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

Phase 4: Roadmap for Cyberresilience and follow up (Duration: 12 months after phase 3)

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

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

Contact: dfssecuritylab@itu.int

Thank you!