30 APRIL 2026

Strengthening Cyber Resilience of DFS Critical Infrastructure

Resilience Gaps, Development Partner Roles & Sustaining Capacity in DFS Markets

Endashaw Tesfaye

United Nations Capital Development Fund (UNCDF)

Virtual | Zoom · 14:00–15:00 CET

Where Are the Largest DFS Resilience Gaps?

Q1 | Three persistent vulnerability tiers observed across UNCDF-supported markets

Perceptions and perspective from the market.

PROVIDER LEVEL

Smaller FSPs & Fintechs

- No dedicated cybersecurity teams or ring-fenced budgets
- Absent or untested incident response plans
- Legacy core systems — unpatched, poorly monitored
- Third-party tech reliance with no vendor risk controls
- Agent networks as the primary attack surface

HIGH RISK

SUPERVISORY LEVEL

Regulators & Supervisory Authorities

- Limited technical staff to assess and enforce cyber norms
- Outdated licensing frameworks — no/minimal cyber risk criteria
- Low uptake of tools like the ITU CSRA Toolkit
- Reactive posture: enforcement triggered by incidents, not audits
- Poor cross-agency coordination (central bank ↔ telecoms regulator)

CRITICAL GAP

CONSUMER LEVEL

End Users — The Weakest Link

- Low digital & financial literacy → phishing & social engineering
- Complex DFS products poorly understood by users
- SIM swap fraud and agent-level impersonation rising
- Weak or inaccessible grievance and recourse mechanisms
- Women, rural & elderly users disproportionately exposed

SYSTEMIC

→ These gaps compound each other: under-regulated providers serve under-protected consumers with little recourse. The ITU CSRA Toolkit addresses all three layers.

Four Pillars of UNCDF's DFS Resilience Work

Q1 | How development partners operationalize tools like the ITU CSRA Toolkit — with results

01 CONSUMER PROTECTION

Regulatory Frameworks & User Rights

UNCDF/development agencies could co-designs DFS consumer protection regulations, disclosure standards and complaint mechanisms with regulators. In Ethiopia, joint work with NBE produced consumer protection awareness campaign that can be directly supplemented by ITU Toolkit incident awareness requirements. This can further be used in the engagement with FSPs.

02 PRODUCT DEVELOPMENT SUPPORT

Security-by-Design for FSPs

Embedding cybersecurity requirements into FSP technical assistance — mobile wallet architecture, agent network risk controls, and vendor management.

03 AWARENESS & CAPACITY BUILDING

Regulator & Provider Cyber Literacy

UNCDF–ITU joint programmes brought NBE and ECA staff to ITU DFS Security Lab forums, building hands-on familiarity with CSRA Toolkit methodology. This can be extended into a training-of-trainers model extending reach to compliance and supervisory staff at the regulators with its spill over impact and engagement with FSPs.

04 ECOSYSTEM SUPPORT — MSD APPROACH

Market Systems Change for Resilience

UNCDF's Market Systems Development approach targets the full ecosystem — not individual actors. Convening FSPs, regulators, telecoms and working with institutions to reach consumer groups while allowing the market to work.

Making Cyber Resilience Stick: Three Design Principles

Q2 | Sustaining improvements in smaller providers and supervisory authorities over time

01

Embed in Regulation

From voluntary guidance to mandatory supervision

- ITU CSRA Toolkit → NBE/ECA supervisory integration, Ethiopia
- DFS licensing criteria updated to include cyber risk self-assessment
- ECA cyber audit checklist developed using toolkit methodology

02

Peer Learning & South–South Exchange

Communities of practice — not one-off workshops

Knowledge walks out when staff rotate. UNCDF facilitates standing regulatory communities of practice across DFS markets, sharing incident case studies, supervisory playbooks and toolkit implementation lessons across borders.

- East & West Africa regulator peer cohort — cross-country exchange
- ITU DFS Security Lab as permanent knowledge-sharing infrastructure
- Joint Ethiopia–Kenya/ other country supervisory exercise on DFS incident simulation

03

Proportionality & Sustained TA

Tiered frameworks + blended finance for smaller providers

Smaller FSPs and agent networks cannot absorb compliance costs designed for large MNOs. Promote use of tiered cyber compliance frameworks calibrated to provider size and risk profile, paired with long-term embedded TA and blended finance instruments — guarantees and concessional loans — so FSPs can fund security upgrades without it becoming a barrier to financial inclusion.

- Tiered cyber compliance pilot: agents vs. e-money issuers vs. MNOs
- UNCDF guarantees linked to FSP security upgrade investment plans
- Regular TA model — not a one-off workshop.

Potential model for practice (The three M's)
Mandate (Regulation) + Memory (Peer Exchange) + Means (Proportionate TA & Finance).
All three must be active simultaneously.

The Ask: Three Commitments for Resilient DFS Markets

Test and Replicate the Model

Commitment solicitation from regulators and industry actors while adopting it in more additional DFS markets within 24 months.

Fund Sustained TA, Not Workshops

Development organizations need to move beyond one-off trainings. Fund 3–5 year embedded technical assistance paired with blended finance instruments so smaller FSPs can invest in cyber resilience upgrades.

Launch a DFS Cyber CoP for Africa

Establish a DFS Cyber Resilience Community of Practice under ITU–UNCDF stewardship — a permanent platform for regulators, FSPs and development partners to share threats, tools, and supervisory playbooks.

Note: Any and all contents presented here do not reflect the position of UNCDF rather the author and presenter.

Thank you!

For more information: Endashaw Tesfaye
DFS specialist
Endashaw.Tesfaye@uncdf.org
www.uncdf.org