Government of Saint Lucia
Division of Public Sector Modernization

DFS Security IMPLEMENTATION

and Testing Update

Presented By

Ms. Nykole Edward

September 8th 2026

DFS KNOWLEDGE TRANSFER PHASES

Phase 1

- Identify Lab team
- Procure/identify equipment
- Configure infrastructure
- Establish secure testing environment

Phase 2

- ITU knowledge transfer
- Android/iOS security testing
- Tools deployment
- Testing methodology development

Phase 3

- Select DFS applications
- Conduct vulnerability assessments
- Document findings
- Produce security reports

Phase 4

- Follow up with providers
- Remediation and retesting
- Policy/regulatory integration
- Continuous testing
- Regional knowledge sharing

DFS SECURITY LAB SCOPE

The project evolved from lab setup
(Phase 1)
→ app testing and tool deployment

(Phase 2)
→ advanced security and training

(Phase 3)
→ oversight and regional integration

(Phase 4)
Covers infrastructure readiness, vulnerability testing of DFS apps, regulatory coordination, and capacity building in cybersecurity testing for digital financial services.

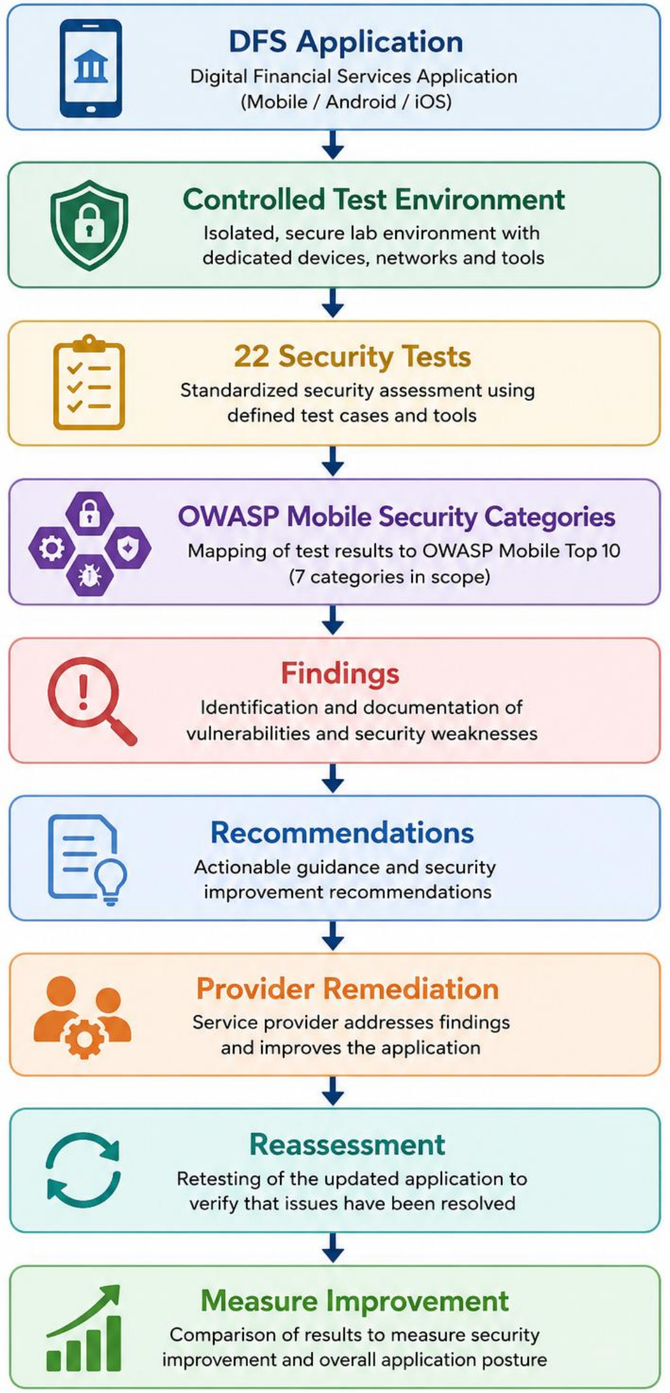
What has been Implemented?

Area	Status
DFS Security Lab established	✅ Completed
Lab team identified	✅ Completed
Dedicated testing environment	✅ Implemented
Testing tools deployed	✅ Implemented
Testing methodology developed	✅ Completed
ITU technical knowledge transfer	✅ Completed/Ongoing
DFS application testing	✅ Started
Security reports produced	✅ Completed
Provider remediation	🟡 Ongoing
Reassessment	🟡 Pending
Updated OWASP methodology	🔵 Next phase
Formalized remediation tracking	🔵 Recommended

Division of Public Sector Modernization

TESTING METHODOLOGY

The goal of the tests is to efficiently evaluate the security of Digital Financial Services apps using a practical, standardized approach



RESULTS OVERVIEW

Storage	T2.2 Auto generated screenshot should not contain sensitive information	Fail
	T2.3 Determine whether sensitive data is shared with third parties	Fail
	T2.4 Finding sensitive data in the keyboard cache	Fail
Communication	T3.2 Application should detect Machine-in-the-Middle attacks with untrusted certificates	Fail
	T3.4 App manifest should not allow cleartext traffic	Fail
M4 Insecure	T4.1 Authentication required before accessing sensitive information	Fail
	T4.3 If a fingerprint is added, existing authentication with fingerprints should be disabled	Fail
	T4.4 Sensitive requests cannot be replayed	Fail
M8: Code Tampering	T8.1 The application should refuse to run on a jailbroken device	Fail
M9: Reverse Engineering	T9.1 Debug symbols should be removed from native binaries	Fail

Challenges of The DFS Lab

The DFS Lab report highlights the region’s progress in digital financial security testing while identifying gaps in technical expertise, coordination, and regulatory enforcement. It calls for dedicated resources, ongoing training, and stronger policies to ensure safe and reliable financial technology adoption.

- EXPERIENCE
- OBSERVATIONS
- CHALLENGES
- RECOMMENDATIONS

Division of Public Sector Modernization

DFS SECURITY LAB – 12 MONTH ROADMAP

Building a Sustainable National Capability for DFS Security Assurance

This roadmap outlines our plan to strengthen the security of Digital Financial Services in Saint Lucia through continuous testing, collaboration and capacity building.

OUR MISSION

Protect consumers, strengthen trust and build a resilient digital financial ecosystem.

OUR APPROACH

Test. Identify. Report. Remediate. Reassess. Improve.

OUR GOAL

A secure, trusted and resilient DFS environment for Saint Lucia.

OUR PARTNERS

DPSM, FSRA, DFS Providers, ITU and other national & regional stakeholders.

12 MONTH ROADMAP OVERVIEW

Q1 (Months 1–3) IMMEDIATE FOUNDATION & COMPLETION

Key Focus

- Complete current provider remediation cycle
- Conduct reassessment of updated application
- Document lessons learned
- Standardize testing environments
- Establish secure findings repository
- Strengthen provider engagement process

Q2 (Months 4–6) NEAR TERM EXPANSION & STANDARDIZATION

Key Focus

- Update methodology to OWASP Mobile Top 10 – 2024
- Expand testing to additional DFS applications
- Formalize vulnerability tracking and remediation process
- Increase hands-on training for lab team
- Begin addressing USSD testing dependencies
- Strengthen coordination with regulators

Q3 (Months 7–9) CAPABILITY MATURATION & INTEGRATION

Key Focus

- Institutionalize remediation and retesting process
- Strengthen reporting templates and scoring metrics
- Expand iOS and Android testing coverage
- Begin USSD security assessments (when dependencies resolved)
- Develop national DFS security baseline
- Enhance internal policies and procedures

Q4 (Months 10–12) SUSTAINABILITY & CONTINUOUS IMPROVEMENT

Key Focus

- Establish recurring assessment cycle
- Continuous monitoring of emerging threats and vulnerabilities
- Regional knowledge sharing and collaboration
- Strengthen policy and regulatory integration
- Evaluate performance against KPIs
- Plan for continuous capacity building

Division of Public Sector Modernization

THANK YOU

For Your Attention