

INTELLIGENCE FOR THE DIGITAL ECONOMY

# THE SOVEREIGN SHIELD

Bridging the Resilience Divide through RaaS & SupTech

## THE SYSTEMIC CRISIS

The 2024 fraud surge resulted in an unrecoverable loss of **1.3 Billion Birr**. This was not a failure of individual technology, but a systemic failure of **Response Velocity**. Our audit confirms that the Ethiopian financial grid is currently operating under a state of uncompensated risk.

**Biniyam Mosisa**

Senior Executive & Techno-Functional Architect

*Sourced from: TIMONA Intelligence (2026)*

[www.timona.org](http://www.timona.org)

## Contents

<b>1</b>	<b>The Resilience Divide: A National Security Risk</b>	<b>2</b>
1.1	The Staffing Bottleneck . . . . .	2
<b>2</b>	<b>Intelligence Silos: The Hidden Vulnerability</b>	<b>3</b>
<b>3</b>	<b>The 1.3 Billion Birr Cost of Inaction</b>	<b>3</b>
<b>4</b>	<b>The Solution: Regulator-as-a-Service (RaaS)</b>	<b>4</b>
<b>5</b>	<b>Implementation Roadmap: 2026–2030</b>	<b>4</b>
<b>6</b>	<b>Strategic Appendix</b>	<b>5</b>
6.1	Executive Glossary . . . . .	5
6.2	Key References . . . . .	5

### DOCUMENT CLASSIFICATION

**Status:** Final Report

**Classification:** Strategic Intelligence (Confidential)

**Distribution:** Board Level / National Bank of Ethiopia

**Primary Source:** TIMONA-2026-RS-001

# 1 The Resilience Divide: A National Security Risk

The TIMONA 2026 audit confirms a structural "Resilience Divide" where Group C institutions represent the primary point of systemic contagion.

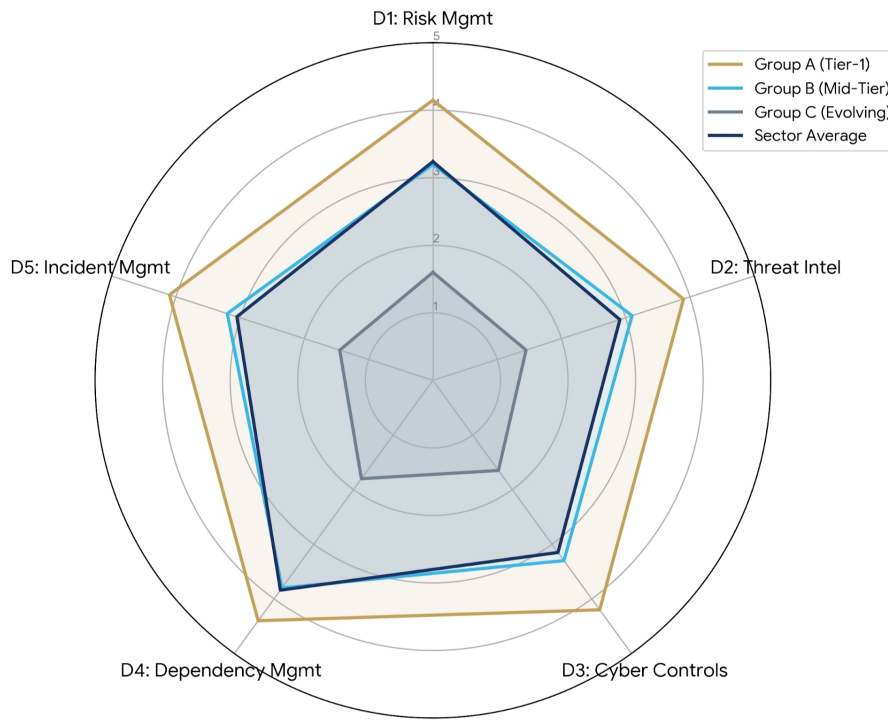


Figure 1: The Resilience Divide: Maturity Gap across the National Grid

## 1.1 The Staffing Bottleneck

Decentralized defense is physically impossible in the current market. As shown in Figure 10, 66.7% of the sector lacks the specialized staff required for independent 24/7 security.

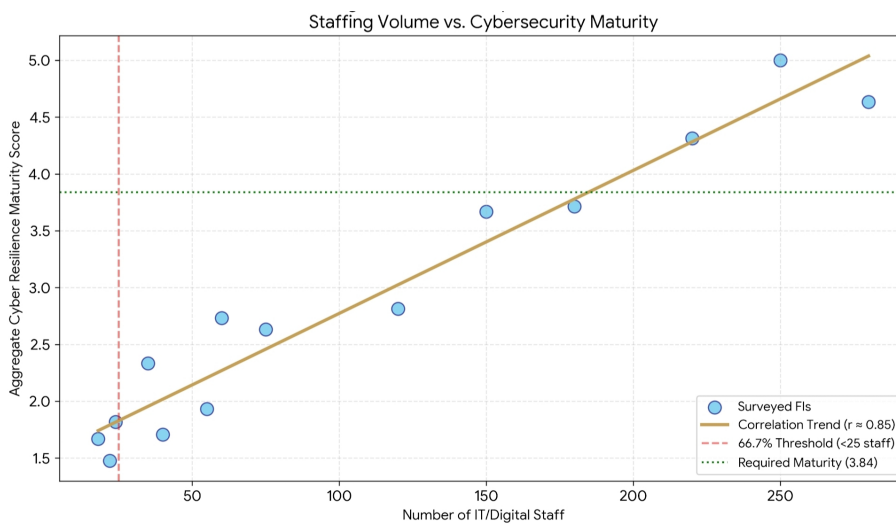


Figure 2: The Staffing Deficit: Specialized Talent vs. Institutional Need

## 2 Intelligence Silos: The Hidden Vulnerability

Beyond staffing and recovery, the "Middle Ground" of defense is crippled by **Threat Intelligence Silos**. Figure 7 illustrates that 85% of critical fraud indicators remain trapped within Tier-1 banks.

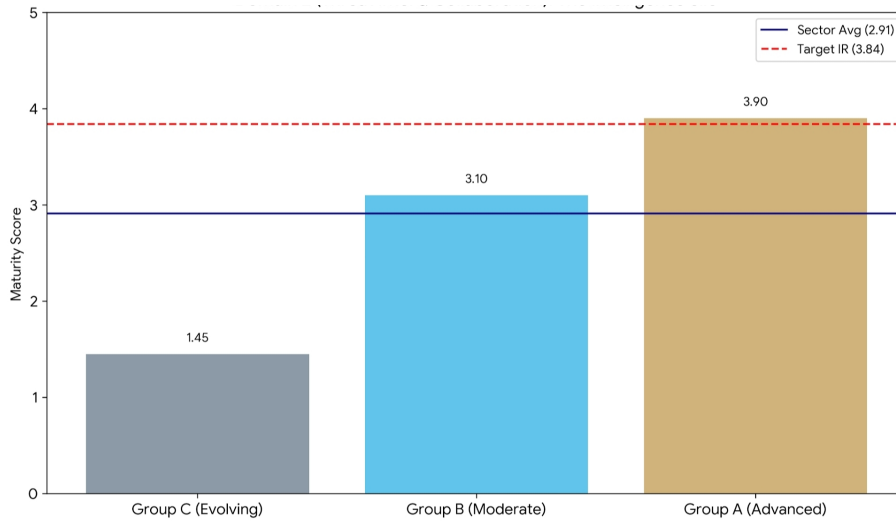


Figure 3: **Domain 2: The Intelligence Silo Effect.** Localized visibility prevents systemic inoculation across the national payment grid.

Without a shared ecosystem—specifically a **SupTech Data-Lake**—the National Bank of Ethiopia (NBE) remains blind to cross-institutional attack patterns until the financial damage is already irreversible.

## 3 The 1.3 Billion Birr Cost of Inaction

The "Golden Hour" of containment was missed during the 2024 surge because smaller institutions lacked real-time visibility. Figure 13 visualizes the **Recovery Gap** that cost the economy 1.3 Billion Birr.

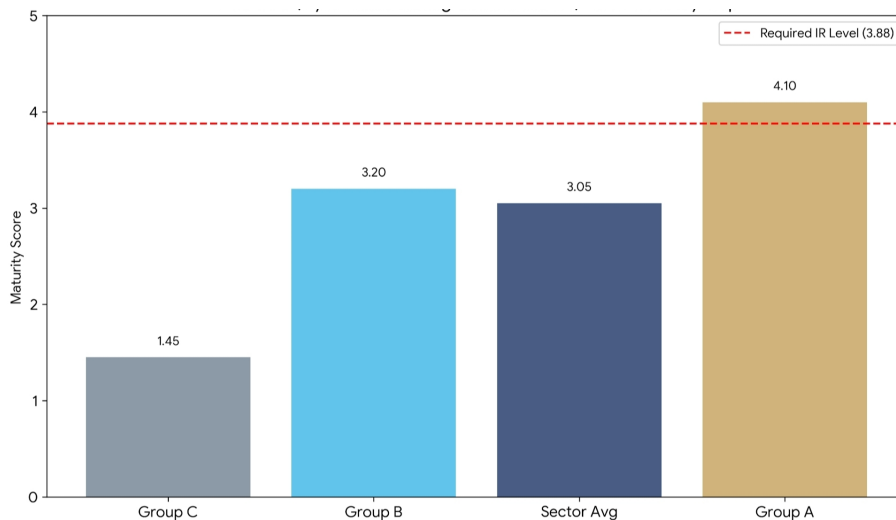


Figure 4: **The Recovery Gap: Containment Timelines vs. Systemic Loss**

## 4 The Solution: Regulator-as-a-Service (RaaS)

The **Sovereign Shield** model centralizes high-cost technical burdens within the NBE, providing a "Public Utility" security model.

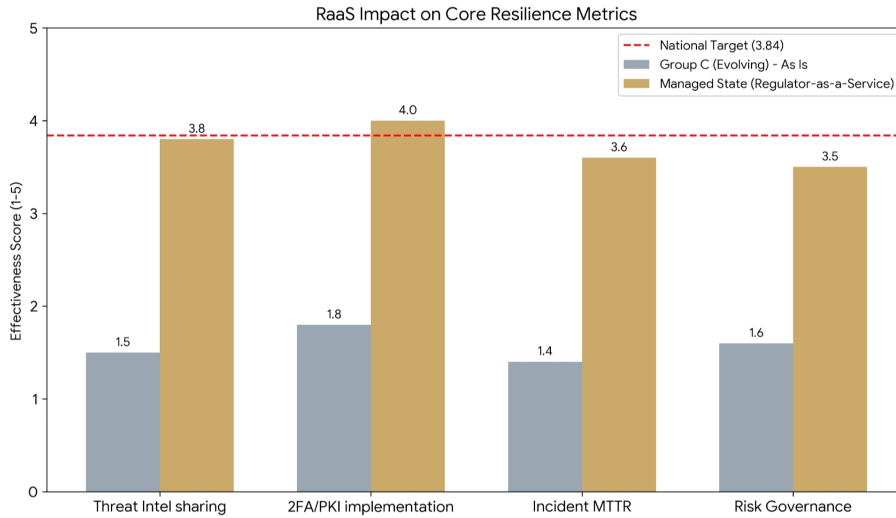


Figure 5: The Sovereign Shield (RaaS) Architecture: Centralized Defense

## 5 Implementation Roadmap: 2026–2030



Figure 6: 2026–2030 Strategic Implementation Timeline

## 6 Strategic Appendix

### 6.1 Executive Glossary

**RaaS:** Regulator-as-a-Service; a model where the NBE provides shared security infrastructure to lower institutional risk.

**SupTech Data-Lake:** A centralized repository for real-time financial telemetry and AI-driven fraud detection.

**Sovereign Shield:** The unified national cybersecurity framework for Ethiopia.

### 6.2 Key References

- **TIMONA Intelligence (2026).** *The Resilience Divide: A National Audit.*
- **National Bank of Ethiopia (2030).** *National Digital Payments Strategy.*
- **Mosisa, B. (2025).** *Assessment of Cybersecurity in Ethiopian Financial Institutions (AAU Thesis).*

**Contact for Strategic Consultation:**  
hub@timona.org — www.timona.org