Defining and Measuring Crypto Agility through KPIs

Ian Deakin Principal Technologist , ATIS

ideakin@atis.org

April 17th, 2025

atis

Overview of Cryptography Agility

Definition

Cryptographic Agility (CAg) refers to the ability to swiftly adapt and change cryptographic algorithms, protocols, and mechanisms.

Key Components

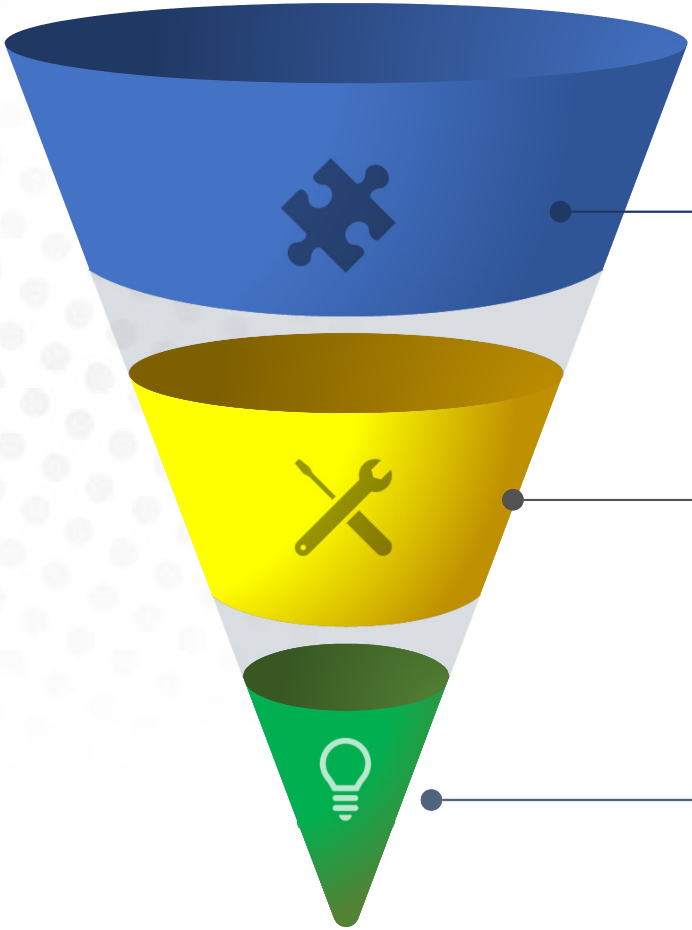
Incorporates robust key management, flexible cryptographic implementations, and continuous monitoring of cryptographic vulnerabilities.

Benefits

Empowers organizations to proactively address evolving threats, maintain compliance, and ensure the integrity, confidentiality, and availability of sensitive information.

Crypto agility goes beyond product implementation, it also relies on organizational readiness.

Cryptographic Agility KPIs



Explanation of KPIs

KPIs, or Key Performance Indicators, are quantifiable measures used to assess the effectiveness and progress of an organization in achieving specific goals.

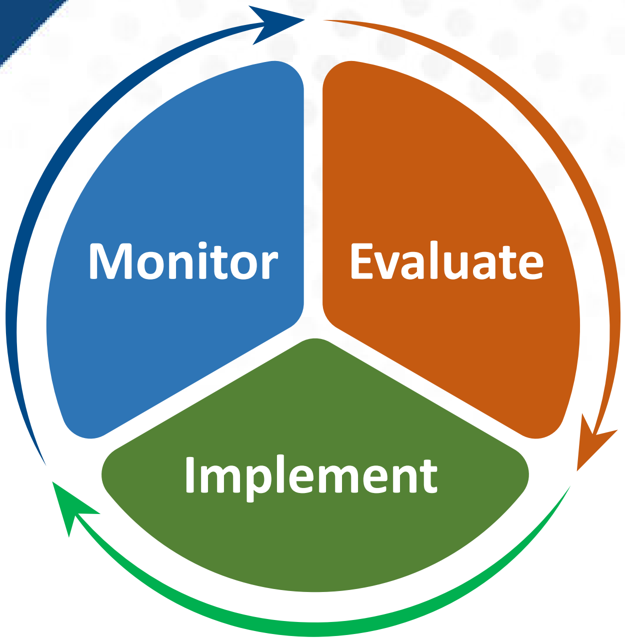
Specific KPIs

Includes organization process, algorithm vulnerability assessments, time-to-update metrics, incident response effectiveness……

Role of KPIs

Provides organizations with insights into their cryptographic resilience, helping to prioritize improvements and make informed decisions.

Crypto Agility KPIs in Risk Management



Quantum Resistance:

Regular monitoring of KPIs ensures timely adjustments to security measures as quantum technology advances.

Cryptographic Evolution:

KPIs serve as early indicators for necessary updates or changes due to ongoing research and emerging vulnerabilities.

Compliance with Standards:

Consistent KPI tracking helps demonstrate adherence to evolving cryptographic standards, maintaining legal and trust requirements

Crypto Agility KPIs Context

1. **Organizational Capability KPIs**
   - Cryptographic Inventory Completeness (%)
   - Time to Implement New Cryptographic Standards (days/weeks)
   - Training Coverage on Crypto Agility (%)
2. **Technological Capability KPIs**
   - Crypto Modularity Score (%)
   - Interoperability Readiness Index
   - Automated Cryptographic Update Rate (%)
3. **Risk and Security KPIs**
   - Time to Mitigate Cryptographic Vulnerabilities (days/weeks)
   - Compliance Readiness Score (%)
   - Percentage of Encrypted Data Using Future-Proof Algorithms (%)

Crypto Agility KPI Scorecard

Example : 3GPP 5G Architecture Risk Assessment

	KPI	METRIC	COMMENT
ORGANIZATIONAL & OPERATIONAL	Cycle Time for Algorithm Implementation	3	Time consuming process due to defining new standards
	Stakeholder Education and Engagement	8	Stakeholders are well informed
	Cost of Implementation	2	Cost is high for compliance with standards
	Risk of Implementation	5	Modrate, but essential for long term security
	Resource Utilization Ratio	6	Efficent use of resources to implement QRC effectivly
	Implementation Readiness Assessment	6	Solid understanding, standards may delay rediness
	Algorithm Replacement Frequency	2	Low, due to duration of standards process
	Compliance with Evolving Standards	7	Committed, ensuring interoperability and security
PRODUCT HARDWARE	Algorithm Swap Time	6	Reasonable, considering the adherence to 3GPP standards
	Patch Deployment Efficiency	5	Patch deployment might take longer due to the need for compliance with evolving 3GPP standards.
	Compatibility with Multiple Algorithms	7	Good compatibility with various cryptographic algorithms, aligning with 3GPP standards.
	Crypto Module Update Frequency	0	Low, not possible to change as the cypto fuctions are designed into the hardware
	Incident Response for Crypto Vulnerabilities	6	Incident response protocols are effective, but may require adjustment to accommodate the implementation of QRC
PRODUCT SOFTWARE	Compatibility with Quantum-Resistant Algorithms	3	Might be challenging due to the evolving nature of 3GPP standards.
	Firmware Update Turnaround	5	Firmware updates may take longer to ensure compliance with 3GPP standards
	Retrofitting Feasibility	4	feasible, but the extended standardization process may affect its practicality.
	Hardware Replacement Cycle for Cryptographic Enhancements	6	Cycle may be extended due to the need for aligning with 3GPP standards
	Resistance to Side-Channel Attacks	9	Strong resistance to side-channel attacks, providing a robust security foundation.

CAg KPI

Benefits of using Crypto Agility KPIs

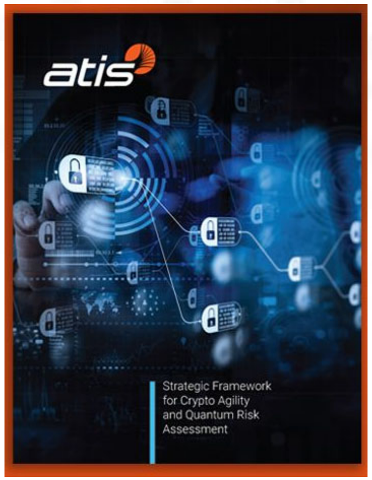
Enhanced Risk Management:
Organizational Level: Crypto agility KPIs provide a systematic way to assess and manage risks at the organizational level.

Trust and Transparency with Stakeholders:
Third-Party Stakeholders: Consistent monitoring and reporting of crypto agility KPIs establish trust with clients, partners, and regulatory bodies.

Operational Efficiency and Product Security:
Product Level: By tracking crypto agility KPIs, organizations ensure the resilience of their products and services.

Standardizing Crypto Agility KPIs Next Steps

These steps will not only contribute to a standardized shared language for the ICT industry, but also enhance the effectiveness of crypto agility communication across diverse stakeholders.



- **Strategic Framework Development:** Utilize the ATIS strategic framework to promote standardization of Crypto Agility KPIs.
- **Industry Collaboration:** Engage with industry experts to progress Crypto Agility KPIs into standardized metrics.
- **Continuous Refinement:** Foster ongoing collaboration and refinement of Crypto Agility KPIs, aligning with emerging best practices.

ADVANCING INDUSTRY TRANSFORMATION

WWW.ATIS.ORG