Crypto Agility Risk Assessment Framework (CARAF)

Framework & Knowledge Base

Comcast - SPIDER

May 2025

Crypto Agility Risk Assessment Framework (CARAF)

Published in 2019 as first paper on crypto agility risk assessment in preparation for the quantum threat

- Referenced by over a dozen research papers
- Referenced by WG in US, Canada, Asia
- Referenced by Forbes

Advent of post-quantum cryptography migration

- US National Security Memorandum 10 established the year 2035 for migration to PQC across federal systems
- National Cyber Security Centre in UK recommended assessment in the next 2-3 years.

CARAF Knowledge Base

Self-service library of information based on CARAF

- A standardized playbook for PQC migration from a risk assessment perspective
- Up-to-date guidance from standard bodies, industries and vendors
- Educational resources on PQC and crypto agility, including real-world applications

How does it benefit us?

- A resource as a reference for PQC migration process
- A hub to facilitate PQC migration knowledge sharing

CARAF Knowledge Base: Big Picture

CARAF conceptually proposes to

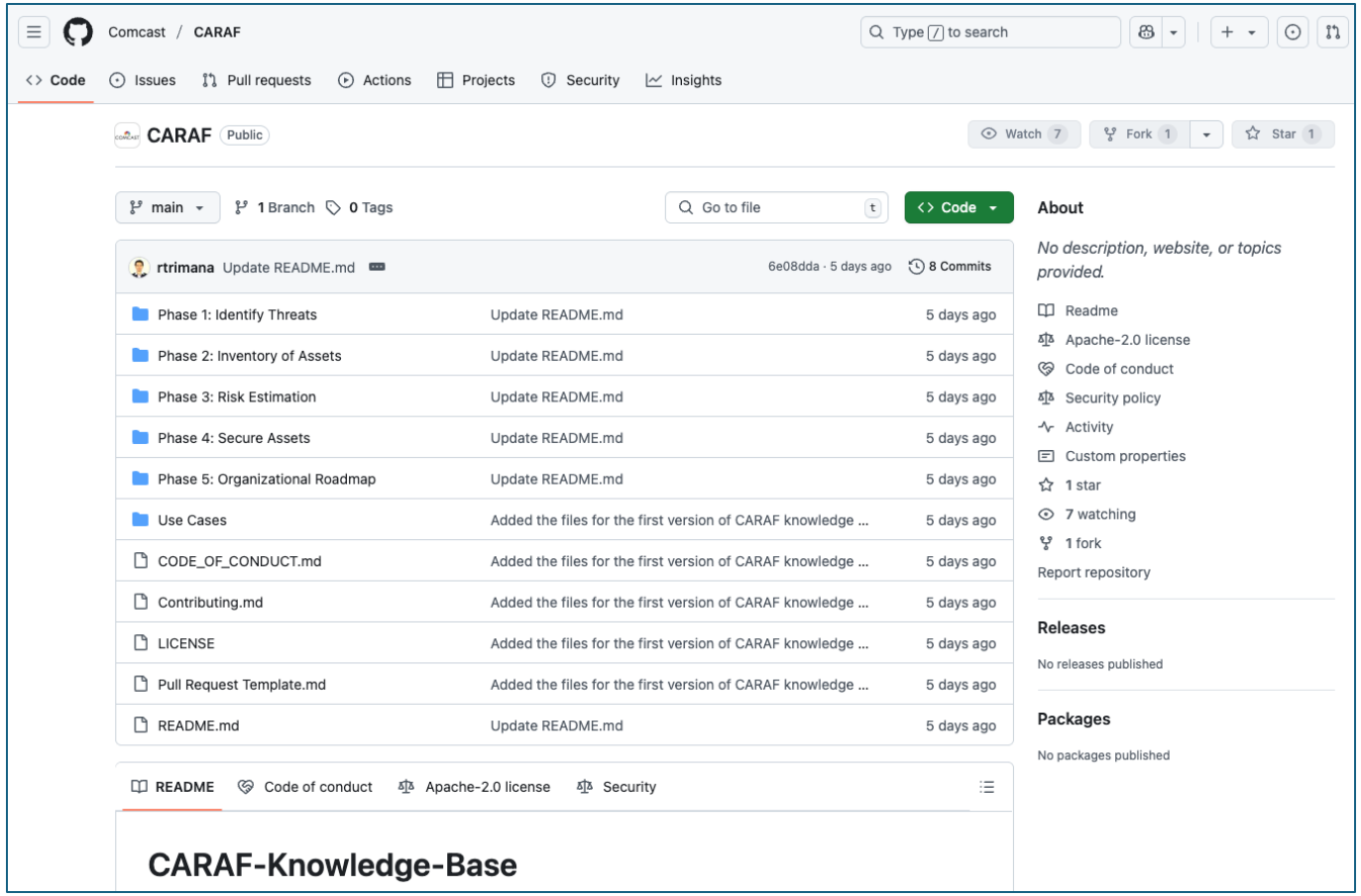
- Define Asset criteria
- Ask binary & quantifiable questions on a per asset basis
  - Measure crypto agility
- Estimate risk: high vs. low
- Three recommendations:
  - High risk + high agility = secure the asset
  - High risk + low agility = phase out the asset
  - Low risk + low/high agility = accept the risk
- Next steps: migration roadmap

CARAF Knowledge Base: Big Picture

CARAF conceptually proposes to

- Define Asset criteria → Phase 1: Identify Threats
- Ask binary & quantifiable questions on a per asset basis → Phase 2: Inventory of Assets
  - Measure crypto agility
- Estimate risk: high vs. low → Phase 3: Estimate Risk
- Three recommendations: → Phase 4: Secure Assets
  - High risk + high agility = secure the asset
  - High risk + low agility = phase out the asset
  - Low risk + low/high agility = accept the risk
- Next steps: migration roadmap → Phase 5: Organizational Roadmap

CARAF Knowledge Base



https://github.com/Comcast/CARAF