CARAF 2.0

MAKING CARAF CLEAR & PRACTICAL

COMCAST

CARAF 1.0

Phase 1: Identify Threats	Update README.md	3 months ago
Phase 2: Inventory of Assets	Update README.md	2 months ago
Phase 3: Risk Estimation	Update README.md	2 months ago
Phase 4: Secure Assets	Update README.md	3 months ago
Phase 5: Organizational Roadmap	Update README.md	3 months ago
Use Cases	Update and rename Applications, Devices and Databases ...	4 months ago
CODE_OF_CONDUCT.md	Create CODE_OF_CONDUCT.md	5 months ago
Contributing.md	Update Contributing.md	4 months ago
LICENSE	Initial commit	5 months ago
Pull Request Template.md	Update Pull Request Template.md	4 months ago
README.md	Update README.md	3 months ago

COMCAST

CARAF 1.0 -> 2.0

CARAF did not have a clear structure

✓CARAF now has clearer separations & boundaries

CARAF was branded as a “knowledge base”

✓CARAF now is a practical risk assessment tool

CARAF had no PoC / tools

✓CARAF now has a calculator

COMCAST

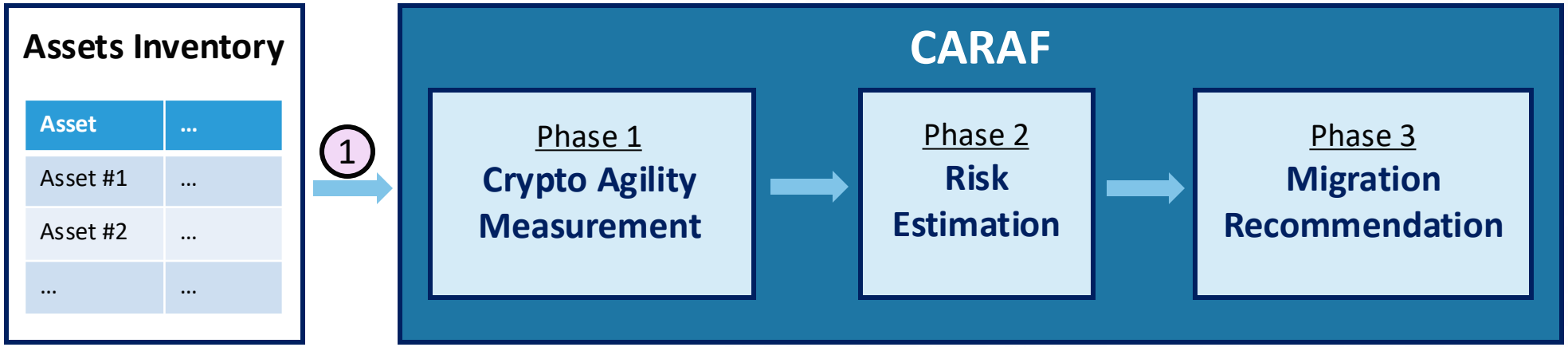
CARAF 2.0

Assets Inventory

Asset	…
Asset #1	…
Asset #2	…
…	…

COMCAST

CARAF 2.0



COMCAST

CARAF 2.0

Assets Inventory

Asset	...
Asset #1	...
Asset #2	...
...	...

1

Phase 1
Crypto Agility Measurement

Phase 1: Crypto Agility Measurement

This phase measures the crypto agility of the asset by asking the following binary and quantifiable questions.

Informational

- What is the lifespan of the asset (in years)? Value = X
- What is the time needed to migrate the asset (in years)? Value = Y; X and Y will be used in Phase 2.

Required to be crypto agile

- Is it owned by a third party? If no, +1.
- Is it configured/managed by a third party? If no, +1.
- Are there dependencies that also need to be updated in case of crypto migration? If no, +1.
- Does implementation of it include hardware components (e.g., HSM, ASIC, FPGA, hardware accelerators, etc.)? If no,
- Does updating the crypto require changes to the asset? If no, +1.

Good-to-have to be more crypto agile

- *Does it use certificates with lifespan beyond 2035? If no, +1.
- *Does it store secret keys? If no, +1.
- *Does it contain encrypted data with lifespan beyond 2035? If no, +1.
- *Is it capable of remote updates? If yes, +1.
- *Are there PQC implementations, tools, or services available to help with the migration? If yes, +1.
- *Is the asset capable of supporting the PQC key sizes and message sizes? If yes, +1.

Next, sum up the values from all questions for a combined crypto agility score ranging from 0 to 11. For the asset, if the an of the questions in the *Required* section, it will be difficult to update the crypto component without significantly affecting t asset. On the other hand, the questions in *Good-to-have* section does affect crypto agility, but may or may not be applica the type of asset. The final score determines the crypto agility as given below:

- *Low Agility*: range from 0 to 5.
- *High Agility*: range from 6 to 11.

Once a crypto agility score is calculated for each asset, please proceed to Phase 2.

Informational

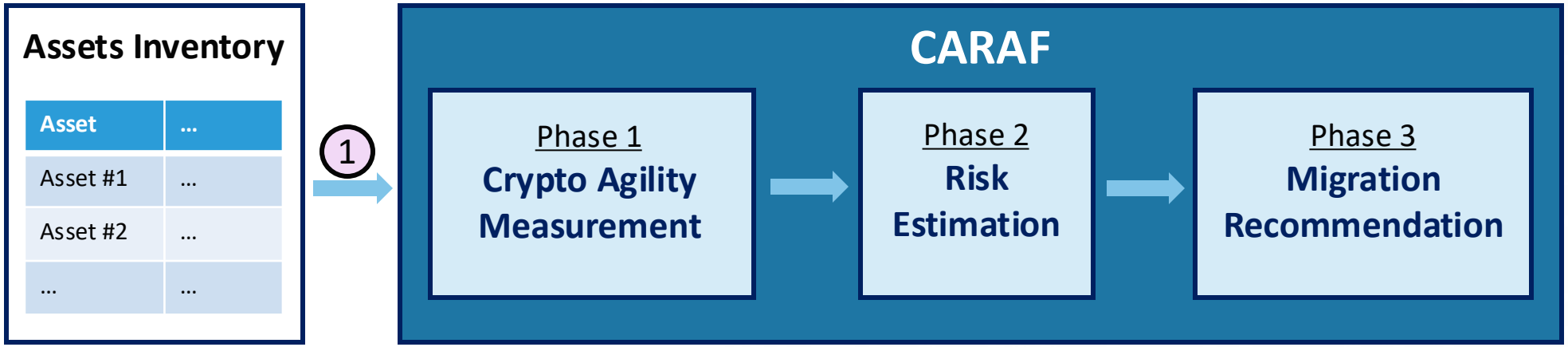
Required

Good-to-have

Crypto Agility

COMCAST

CARAF 2.0



COMCAST

CARAF 2.0

Phase 2: Risk Estimation

This phase estimates the risk level of the asset, representing the value and importance of the asset to be secured with PQC algorithms. Here, we calculate the risk level by considering time and cost.

Time to exposure

Mosca's theorem is used as reference:

- Lifespan of the asset is X from Phase 1.
- Time needed for migration is Y from Phase 1.
- Time before threat results in a compromise (now - 2035) is Z.
- Calculate the value of $Z - (X + Y)$.
  - If the result is positive, your asset will be *phased out* before PQC migration is required.
  - If the result is negative, your asset will be *vulnerable* for $Z - (X + Y)$ number

Cost to migrate

The evaluation will be based on the following factors:

1. Will performance overhead be critical to the function of the asset? For example, the answer may be yes for streaming application, or no for databases accessed once per month.
2. Will there be a significant cost for updating to the new algorithms each time? For example, the answer m e yes if asset is implemented in hardware, or no if asset is implemented in software.
3. *Is decrypting then re-encrypting the asset needed (e.g., long-lived data)?
4. *Will there be a cost to migrate to PQC (i.e., additional internal resources dedicat The questions with * are a one-time cost.

Based on the answers to the above questions, there are two levels of risk estimate:

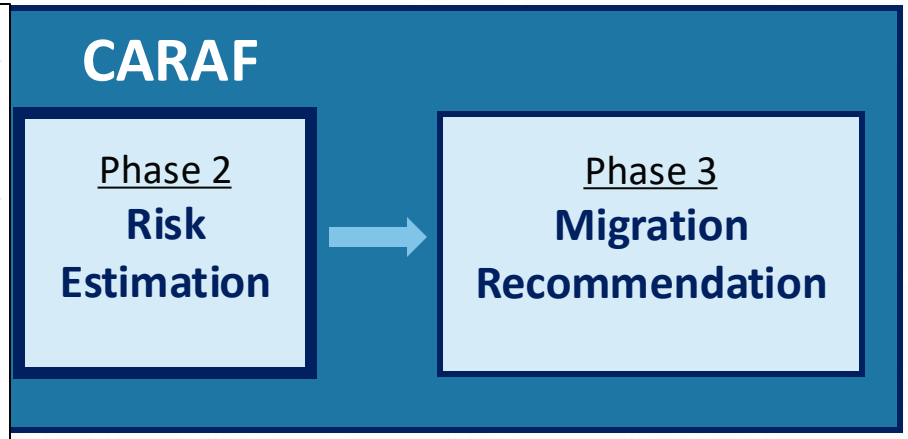
- *High risk*: If your asset will be *vulnerable* timeline-wise and you answered yes to it
- *Low risk*: Otherwise, risk = low.

Once the risk level is determined for each asset, proceed to Phase 3.

Time to exposure: Mosca Theorem

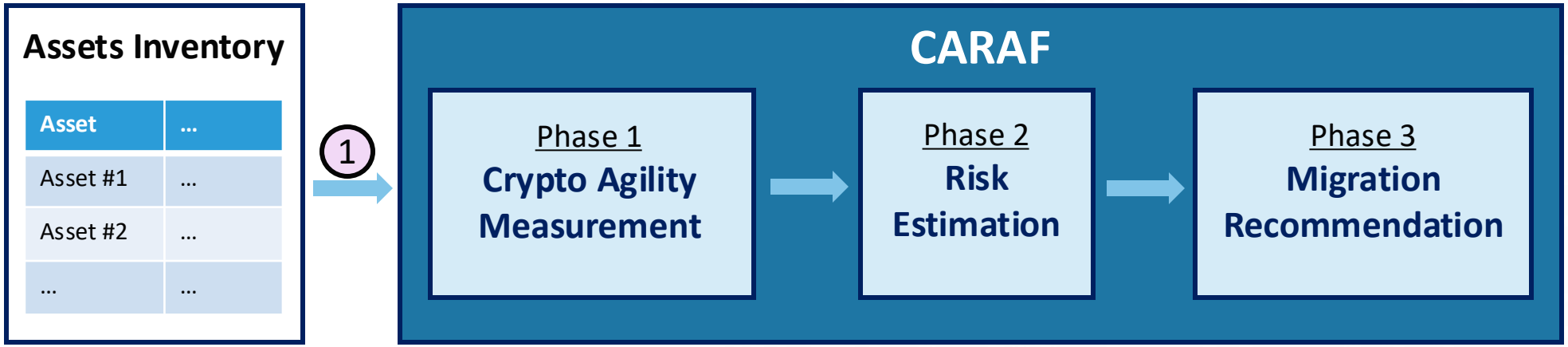
Cost to migrate

Risk Level



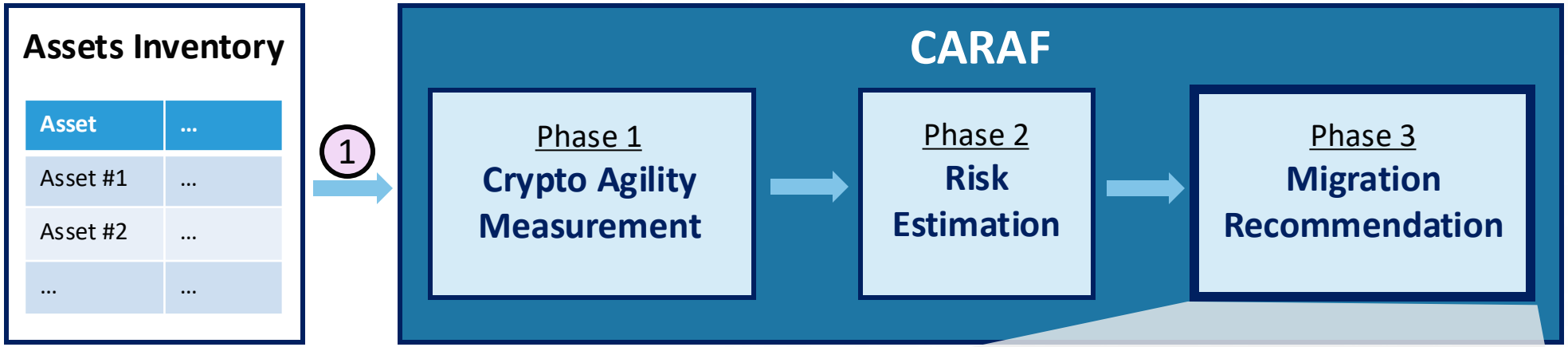
COMCAST

CARAF 2.0



COMCAST

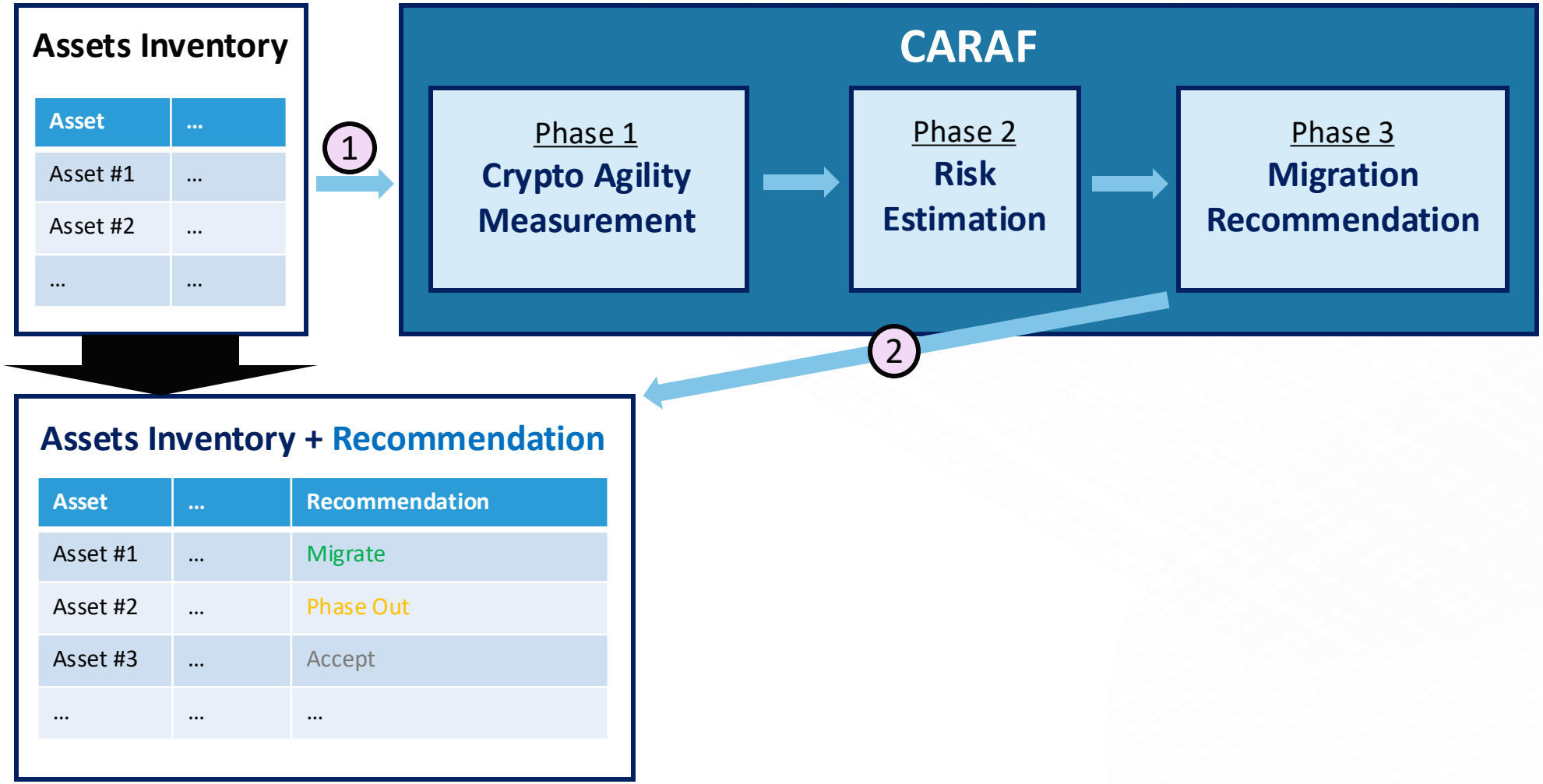
CARAF 2.0



Crypto Agility	Risk Level	Recommendation
High	High	Migrate
Low	High	Phase Out
Low/High	Low	Accept

COMCAST

CARAF 2.0



COMCAST

CARAF 2.0

Assets Inventory

Asset	...
Asset #1	...
Asset #2	...
...	...

1

CARAF

Phase 1
Crypto Agility Measurement

Phase 2
Risk Estimation

Phase 3
Migration Recommendation

2

Assets Inventory + Recommendation

Asset	...	Recommendation
Asset #1	...	Migrate
Asset #2	...	Phase Out
Asset #3	...	Accept
...	...	...

3

Migrate / Phase Out Recommendation

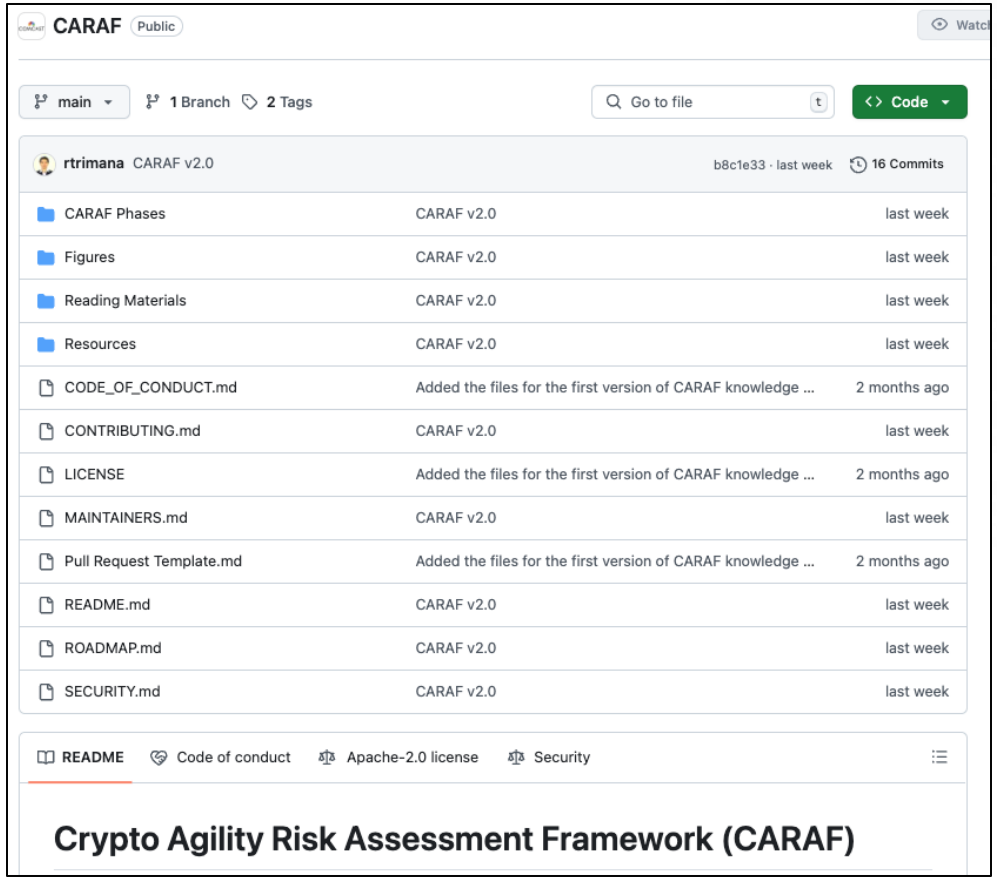
Option 1: Asset migration for first-party asset
Option 2: Vendor Risk Assessment (VRA) for third-party asset & work with third party for migration

Accept Recommendation

No action on the asset

COMCAST

CARAF REPO & DEMO



https://github.com/Comcast/CARAF

COMCAST

COMCAST