Making SBOMs work for everyone

Paris - June 2023

APH10

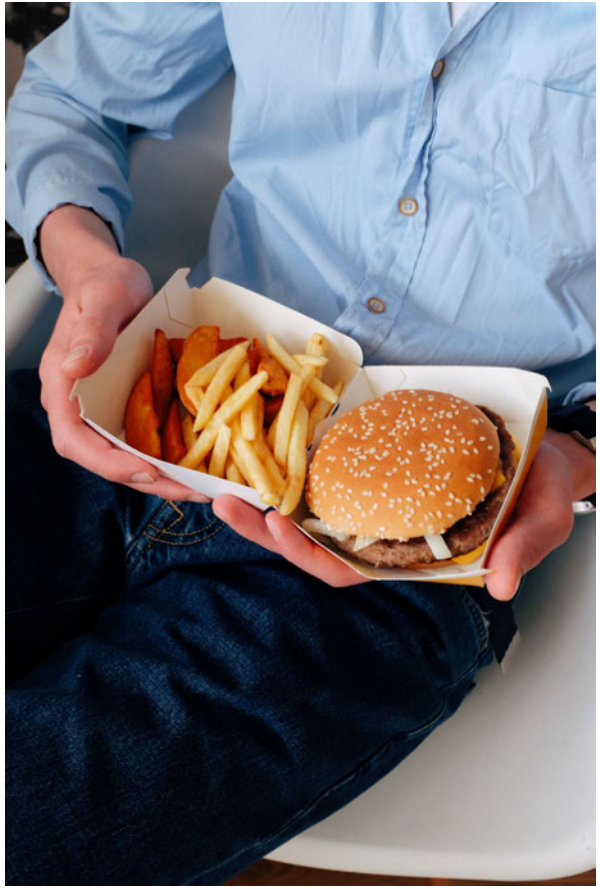
APH10

APH10

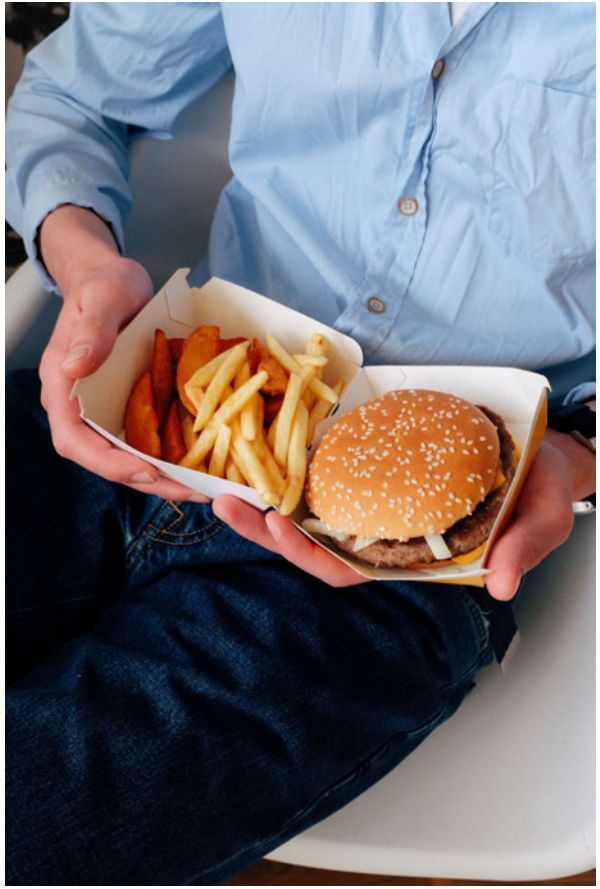
CoderDojo

STEM AMBASSADORS

APH10



APH10



APH10

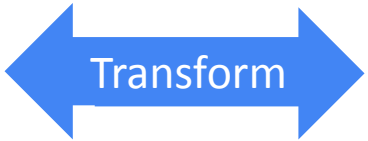
APH10

What is an SBOM?

- ➔ A SBOM is a **formal set of machine-readable metadata** describing your software application
- ➔ SBOMs are designed to be **shared within and across organizations**
- ➔ SBOMs form an important part of a software **risk strategy**

APH10

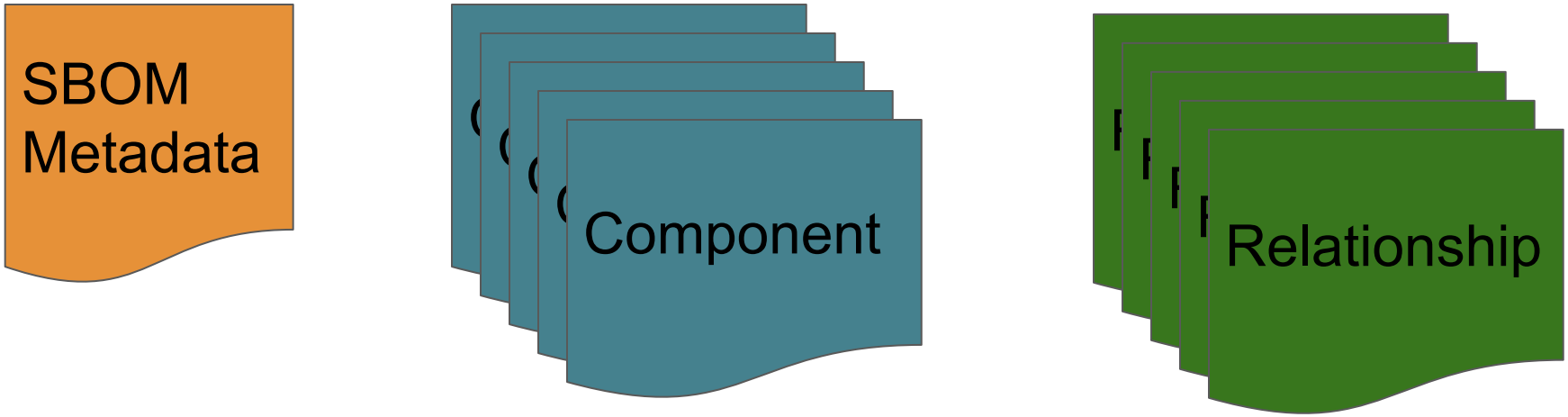
Two primary standards and formats….



https://spdx.org/

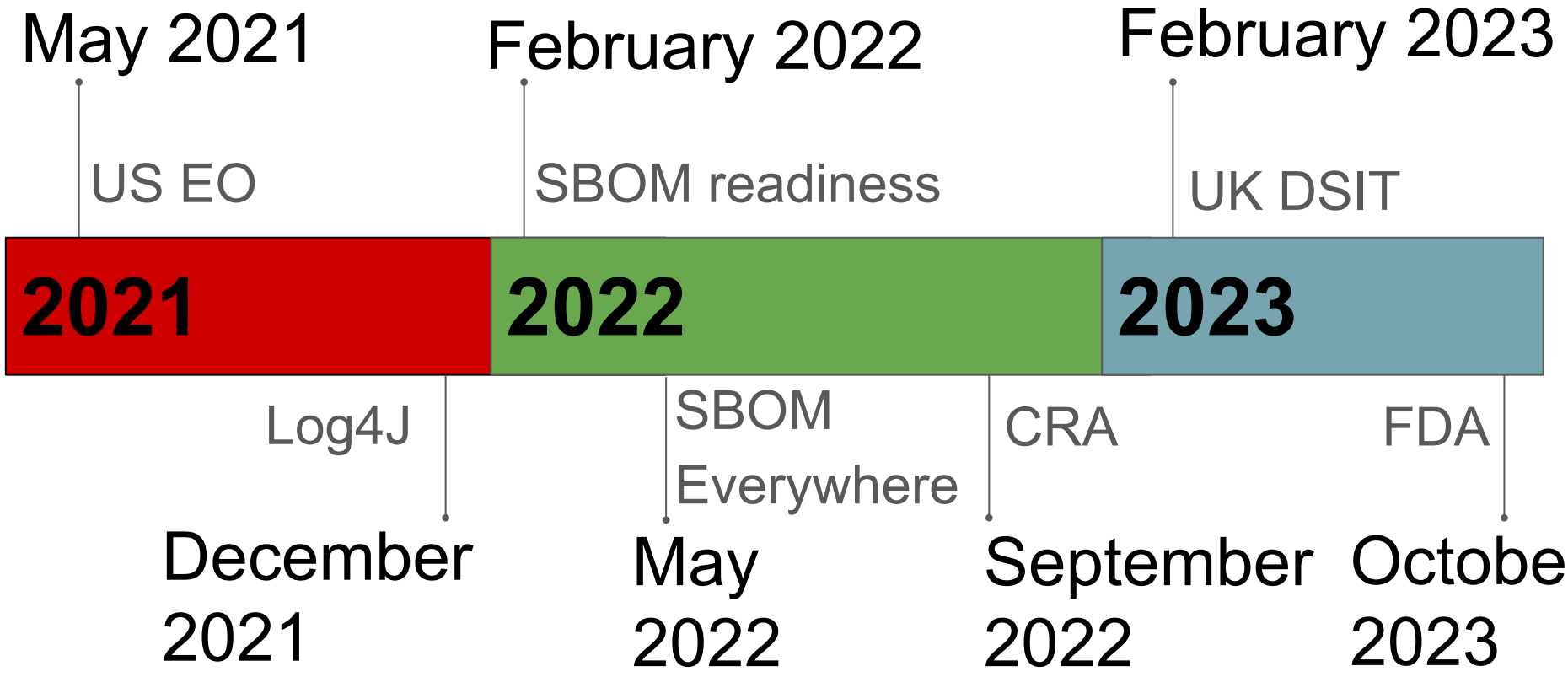
https://cyclonedx.org/

SBOM Content



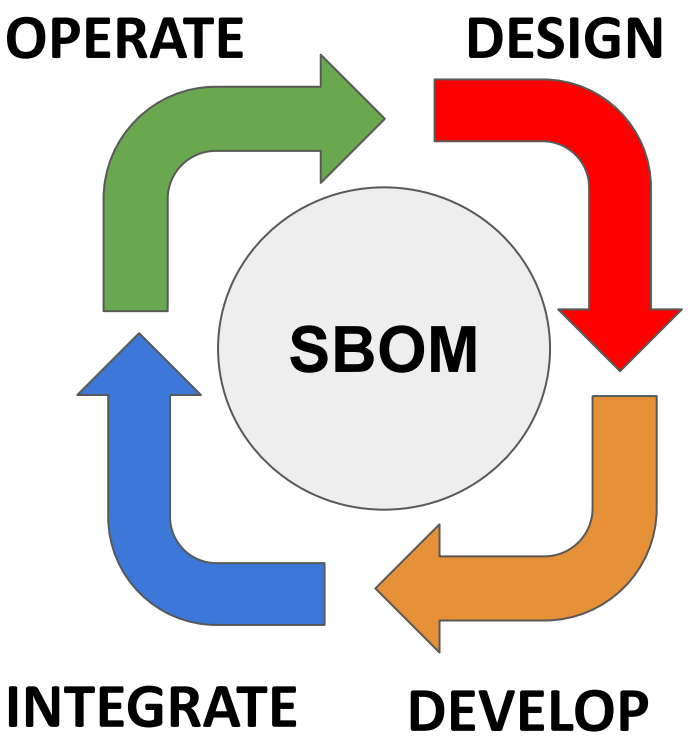
APH10

Increasing awareness of SBOMs



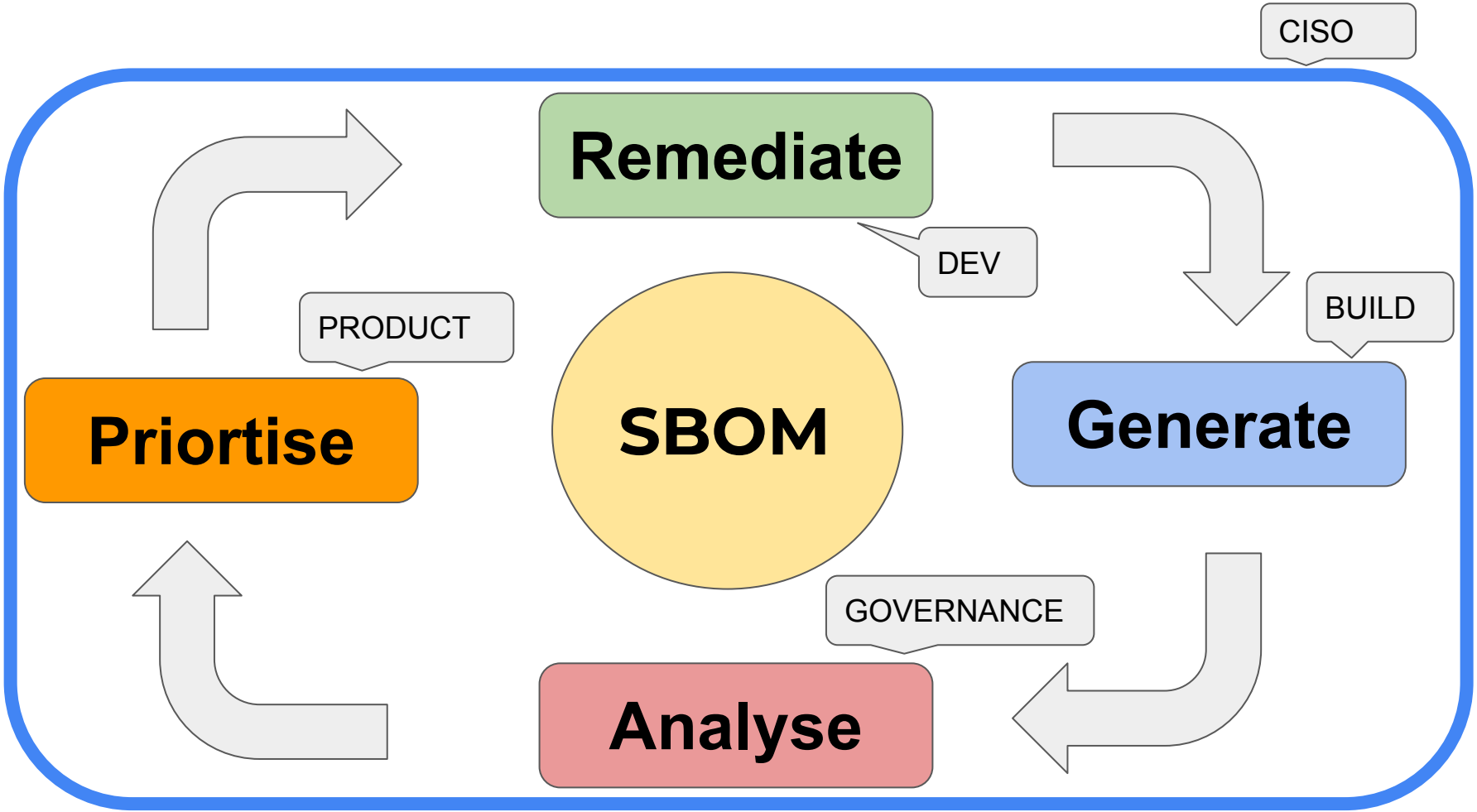
APH10

SBOMs are used throughout the lifecycle



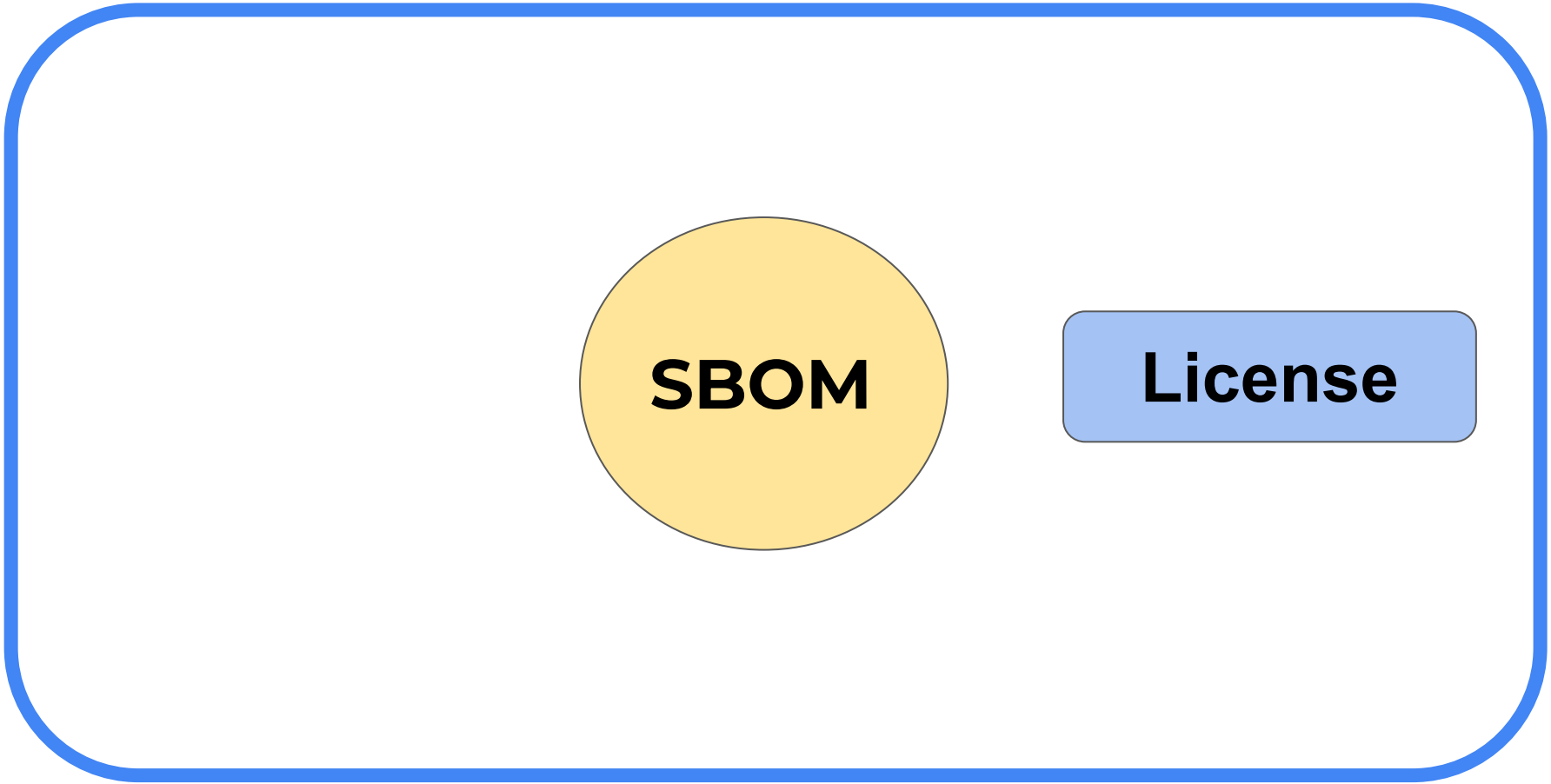
- 3rd party component selection
- Source files in build
- Applications built
- Component dependencies
- Build composition
- Build integrity
- License Compliance
- Change Management
- Vulnerability Monitoring
- Obsolete software detection

APH10

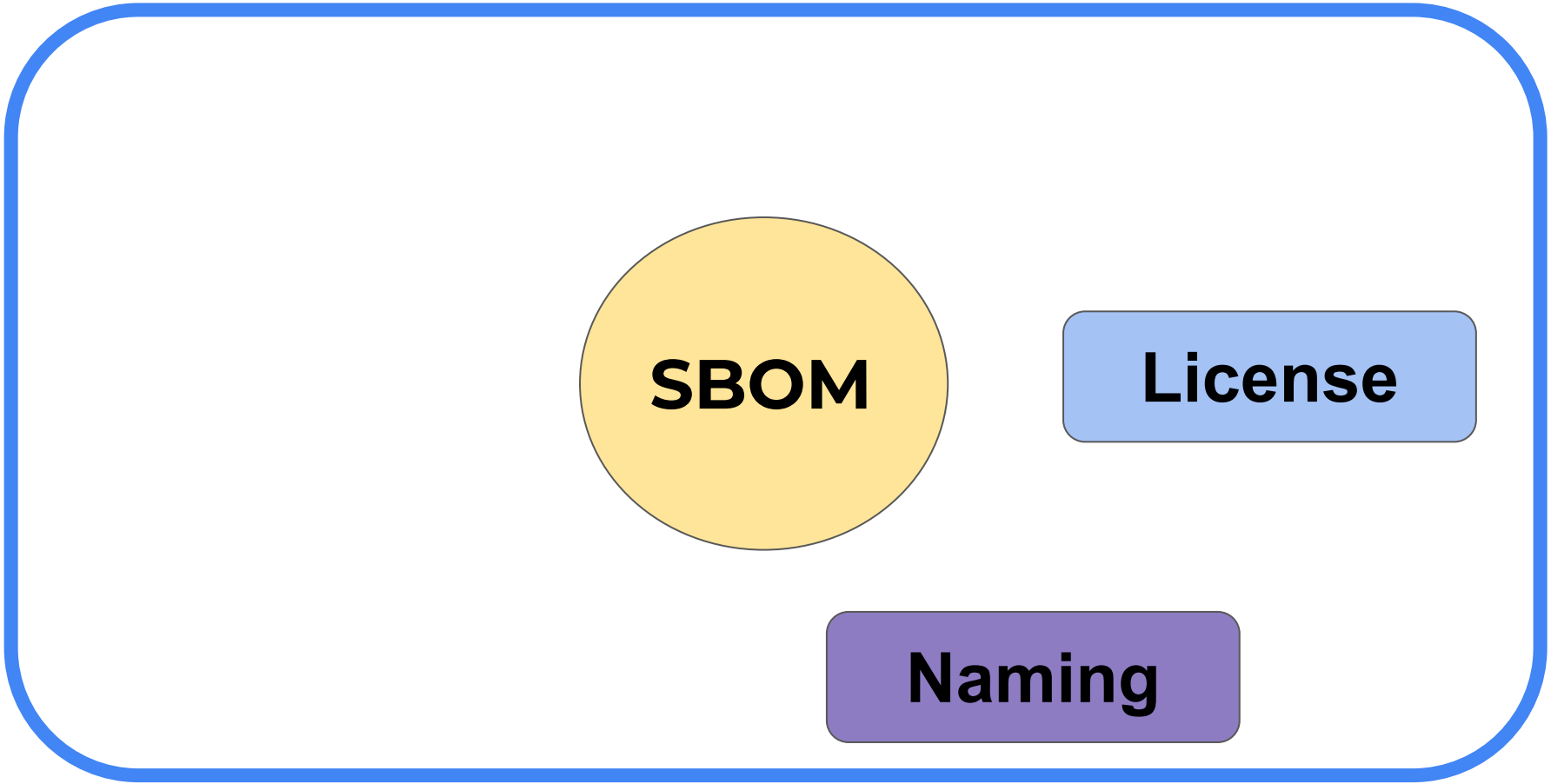


APH10

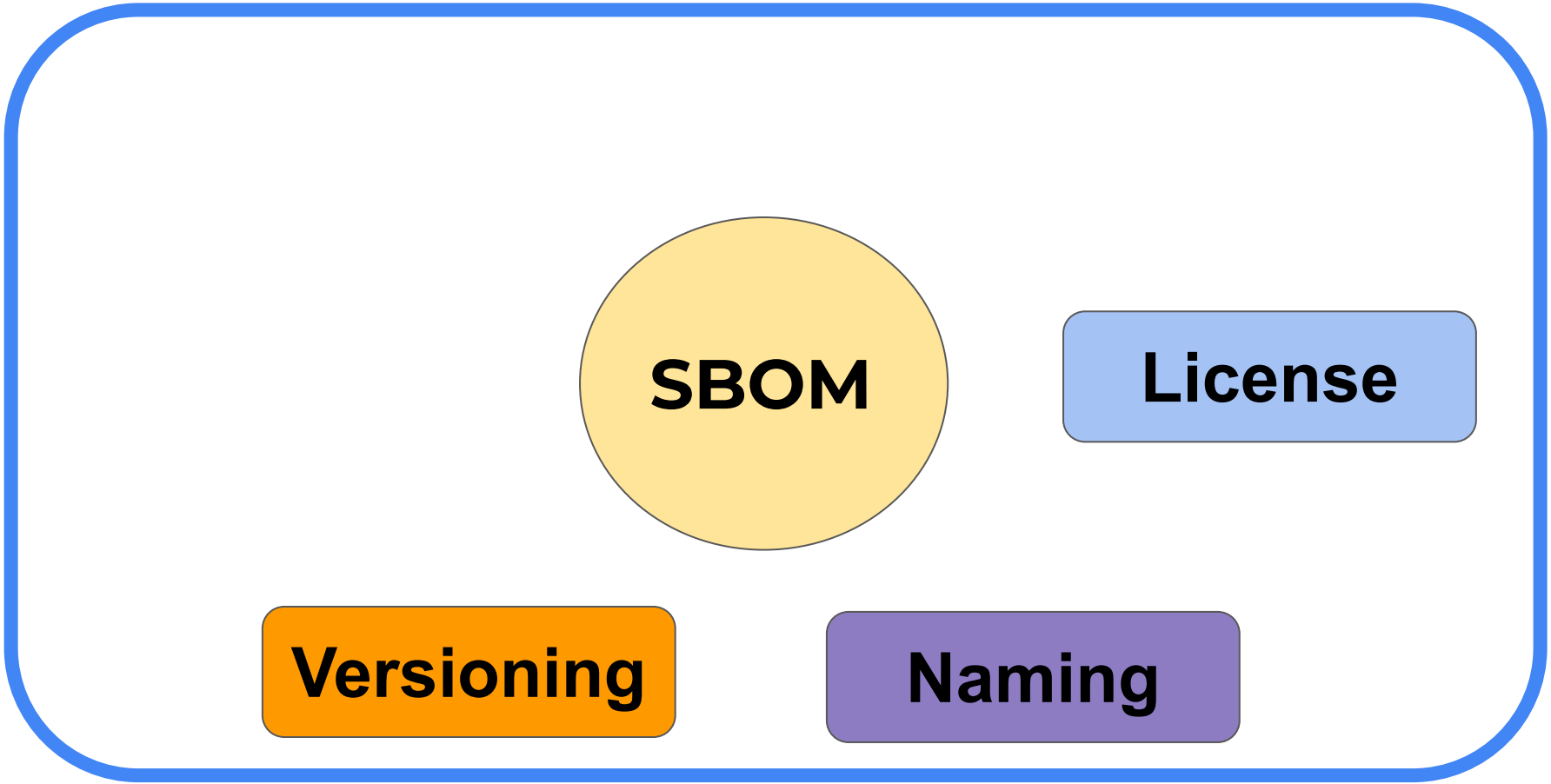
APH10



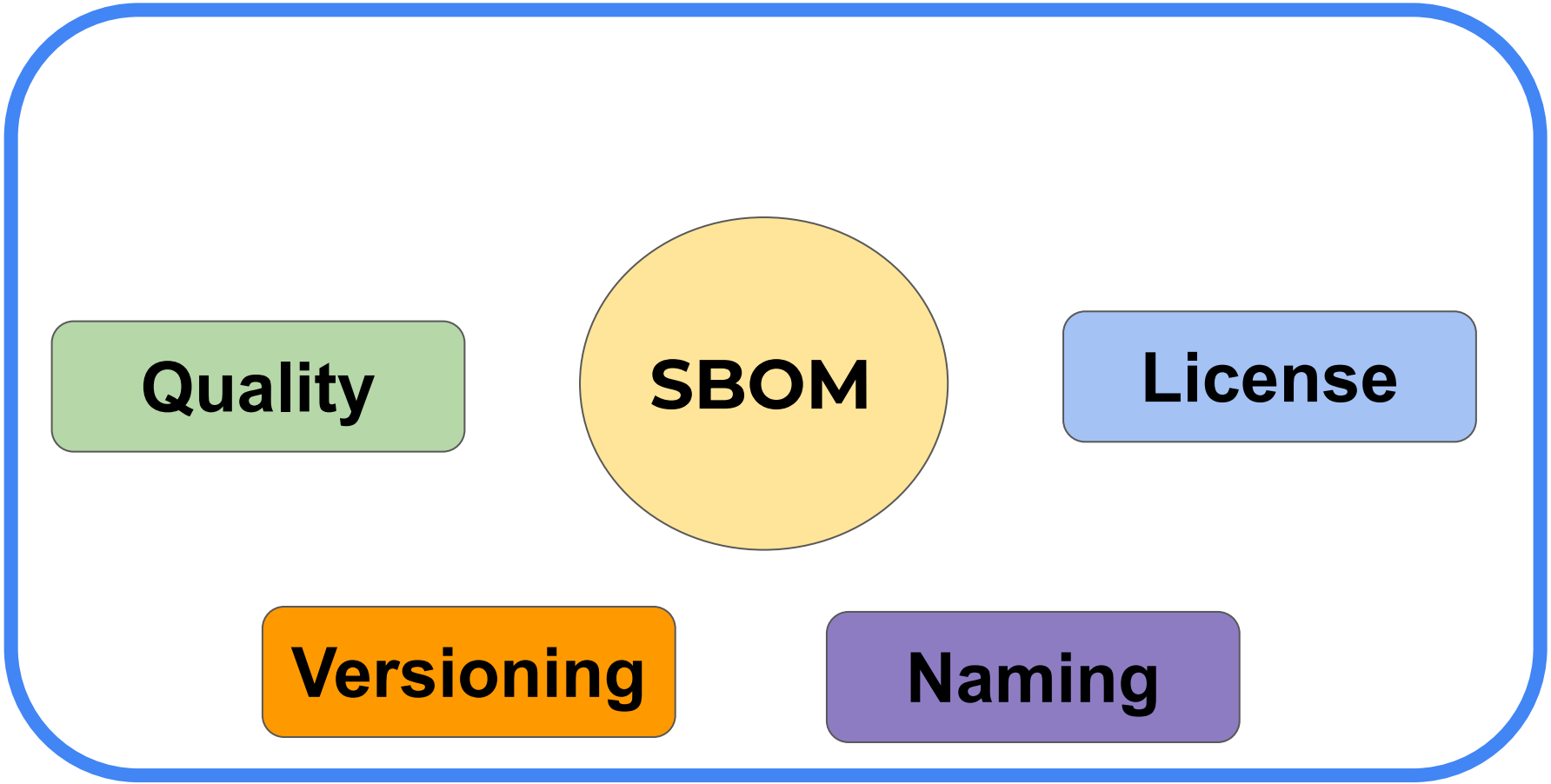
APH10



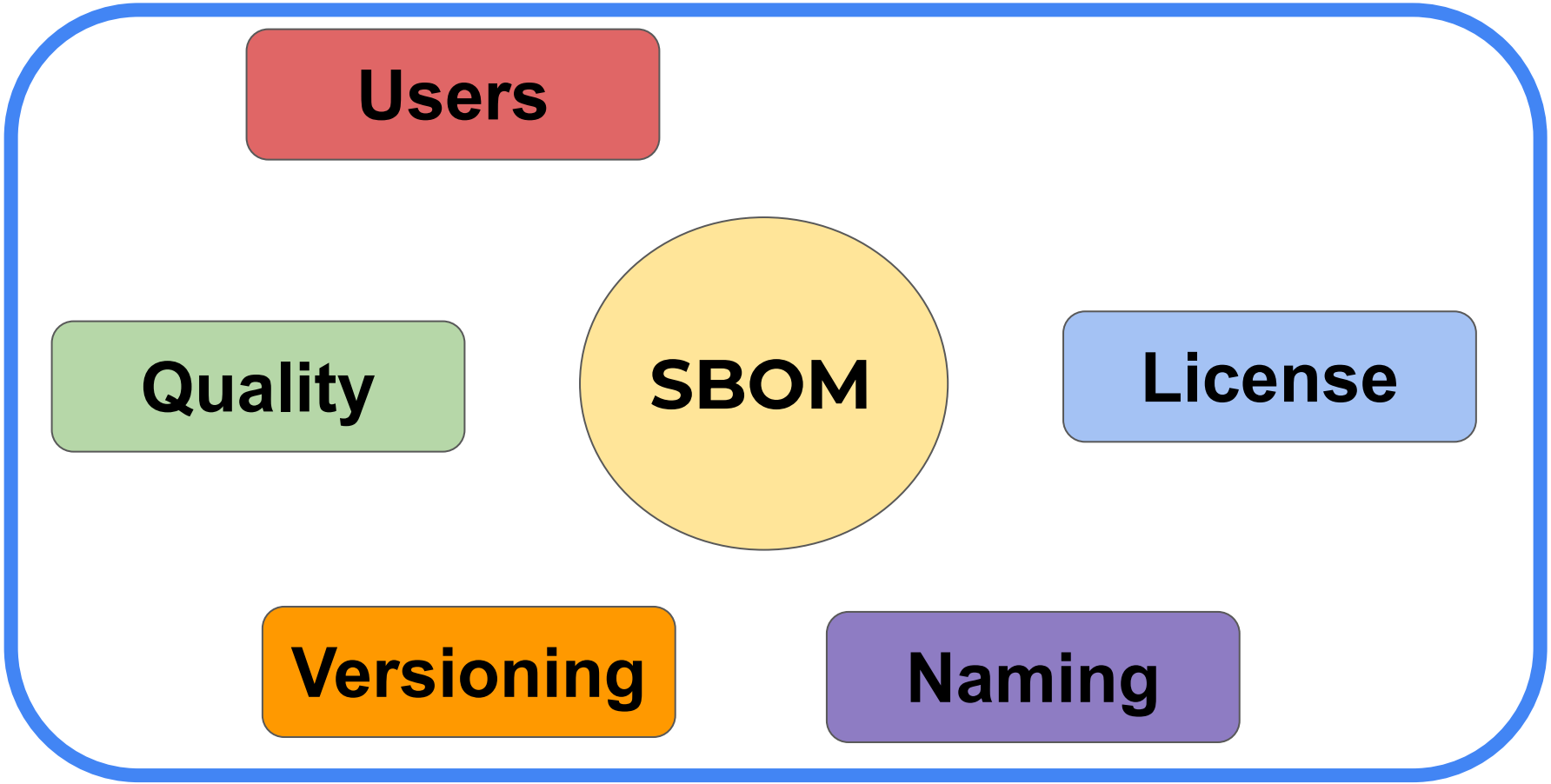
APH10



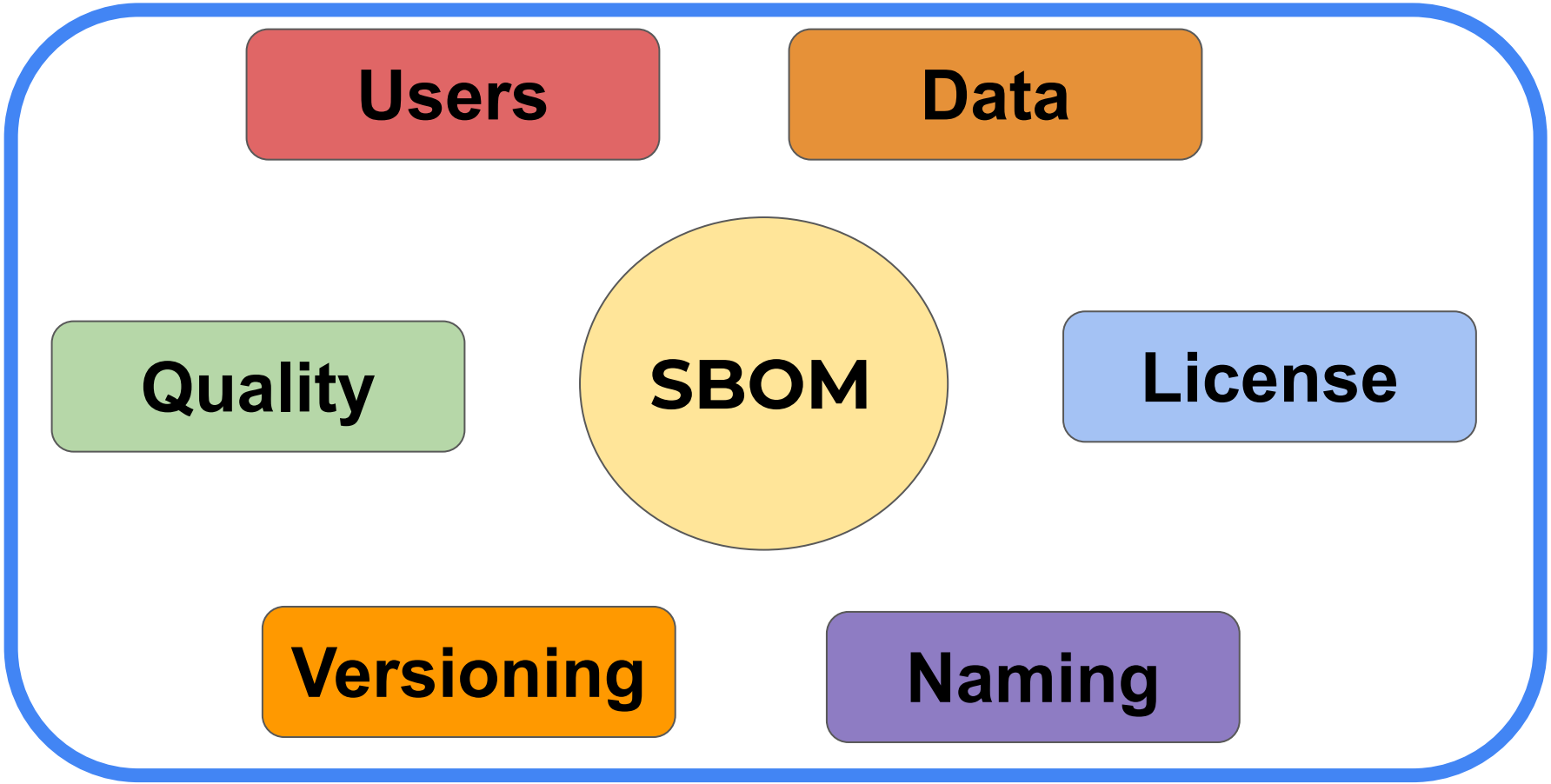
APH10



APH10



APH10

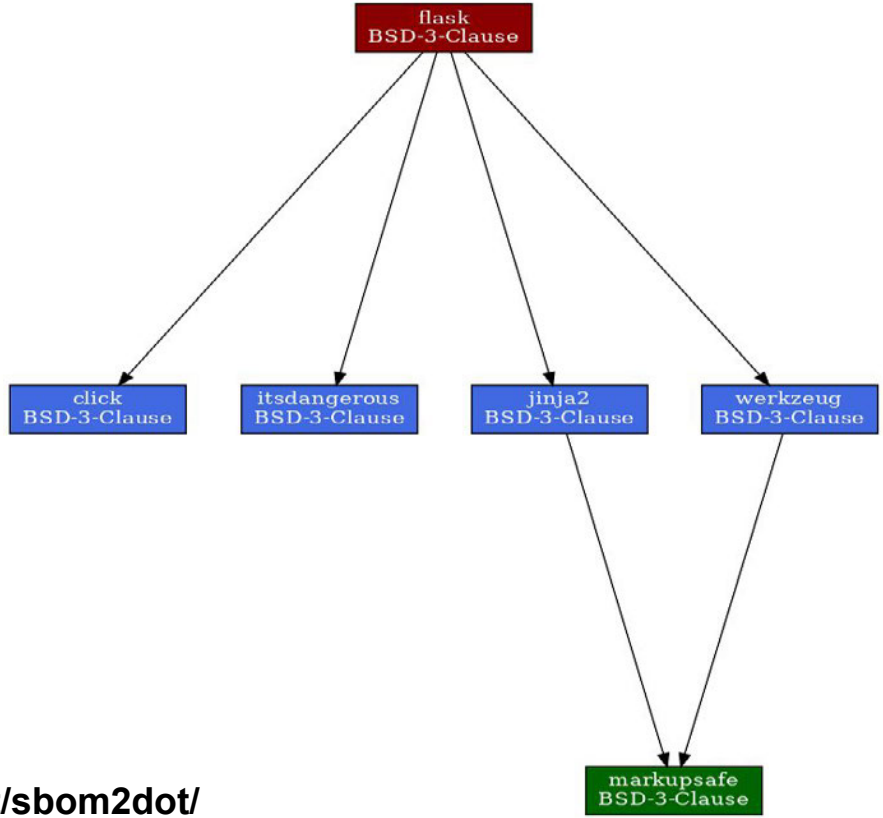


APH10

```
┌─────────────────┐
| Package Summary |
└─────────────────┘
[ ] License included for package attrs: MISSING
[ ] License included for package idna: MISSING
[ ] OSI Approved license for defusedxml: MISSING
[ ] Using latest version of package httplib2: Version is 0.20.4; latest is 0.22.0
[ ] License included for package pyparsing: MISSING
[ ] Using latest version of package rsa: Version is 4.7.2; latest is 4.9
[ ] Using latest version of package pyopenssl: Version is 23.1.1; latest is 23.2.0
[ ] OSI Approved license for cryptography: MISSING
[ ] Using latest version of package google-auth: Version is 2.18.1; latest is 2.19.1
[ ] Using latest version of package cachetools: Version is 5.3.0; latest is 5.3.1
[ ] Using latest version of package urllib3: Version is 1.26.15; latest is 2.0.2
[ ] OSI Approved license for packaging: MISSING
[ ] Using latest version of package packaging: Version is 21.3; latest is 23.1
[ ] Using latest version of package requests: Version is 2.30.0; latest is 2.31.0
[ ] Using latest version of package rich: Version is 13.3.5; latest is 13.4.1
[ ] NTIA compliant: FAILED
```

https://pypi.org/project/sbomaudit/

APH10



https://pypi.org/project/sbom2dot/

APH10

SBOM Summary

Item	Details
SBOM File	/tmp/click.json
SBOM Type	cyclonedx
Version	1.4
Name	Python-click
Creator	tool:sbom4python
Created	2023-03-02T11:58:30Z
Files	0
Packages	1
Relationships	1

Package Summary

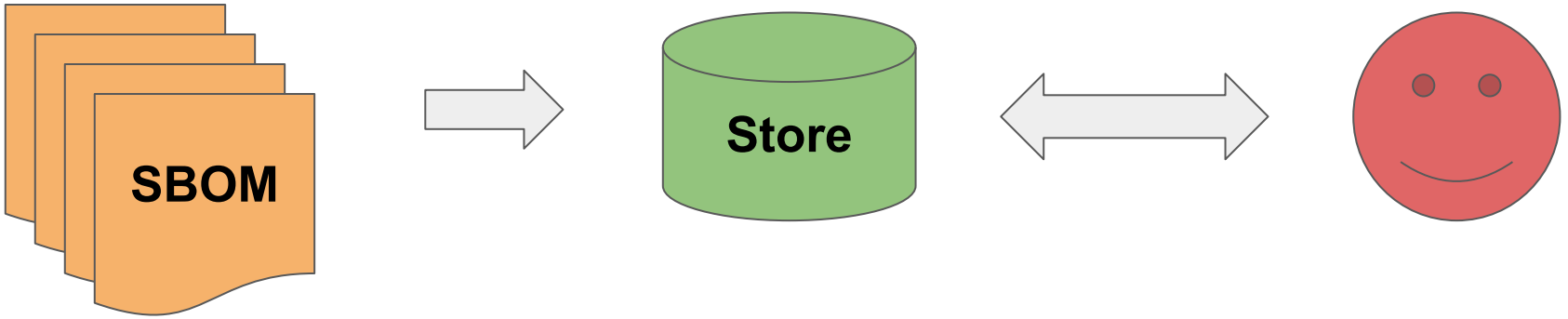
Name	Version	Supplier	License
click	8.1.2	Armin Ronacher	BSD-3-Clause

License Summary

License	Count
BSD-3-Clause	1

https://pypi.org/project/sbom2doc/

APH10




```
sbom-manager --module pyyaml
SBOM                    Project          Description     Product  Version   License
=============================================================================
matcha-ml.spdx          Matcha-ML        Release 2.3     pyyaml   5.4.1     MIT
cve-bin-tool-py3....    Release_3.2.1    Not specified   pyyaml   6.0       MIT
sbom4python.spdx        sbom4python      Release 0.8.0   pyyaml   6.0       MIT

sbom-manager --module log4j
No data found
```

https://pypi.org/project/sbom-manager/

APH10

SBOMs provide an important part of the **secure software development lifecycle**

SBOMs provide enhanced **transparency** and **dependency management**

SBOMs provide a key role to supporting better **risk management**

APH10

SBOMs are only as good as the data which is provided. Everyone is responsible for improving this data.

APH10

info@aph10.com

https://www.linkedin.com/in/anthonypharrison/

https://www.linkedin.com/company/aph10/

https://github.com/anthonyharrison

APH10