

# Making SBOMs work for everyone

Paris - June 2023



Log A Shell™











```
94     .image/gif;base64,R01GODlhAQABAIAAIFVpZG90AA==>
95     <div class="container">
96       <div class="carousel-caption">
97         <h1>One more for good measure.</h1>
98         <p>Cras justo odio, dapibus ac facilisis in, egestas eget quam. Donec id elit sed purus consectetur elit.
99         .</p>
100        <p><a class="btn btn-lg btn-primary" href="#" role="button">View gallery</a>
101        </div>
102        </div>
103        <a class="left carousel-control" href="#myCarousel" role="button" data-slide="prev">
104          <span class="glyphicon glyphicon-chevron-left" aria-hidden="true"/>
105          <span class="sr-only">Previous</span>
106        </a>
107        <a class="right carousel-control" href="#myCarousel" role="button" data-slide="next">
108          <span class="glyphicon glyphicon-chevron-right" aria-hidden="true"/>
109          <span class="sr-only">Next</span>
110        </a>
111      </div><!-- /.carousel -->
112    <!--Featured Content Section-->
113    <div class="container">
114      <div class="row">
115        <div class="col-md-4"></div>
116        <div class="col-md-4"><h2>FEATURED CONTENT </h2></div>
117        <div class="col-md-4"></div>
118      </div>
119    </div>
```



# 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**

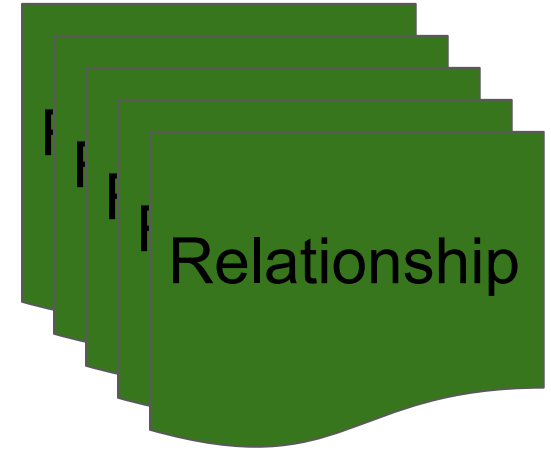
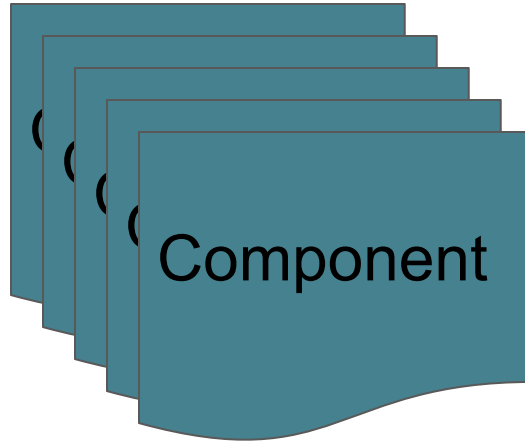
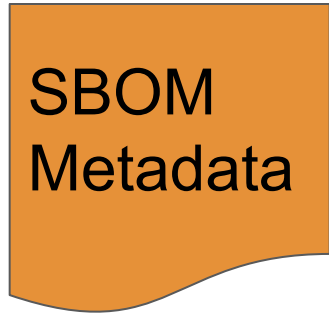
# Two primary standards and formats....



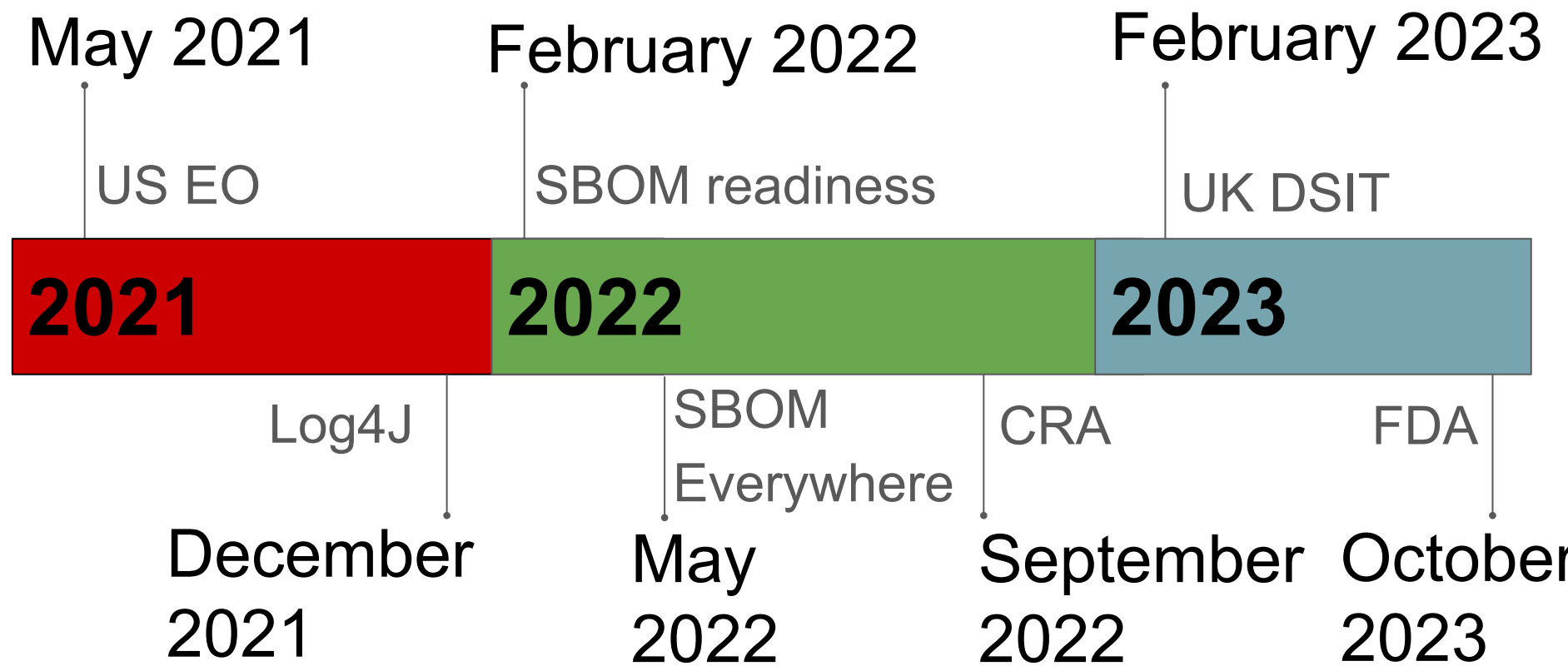
<https://spdx.org/>

<https://cyclonedx.org/>

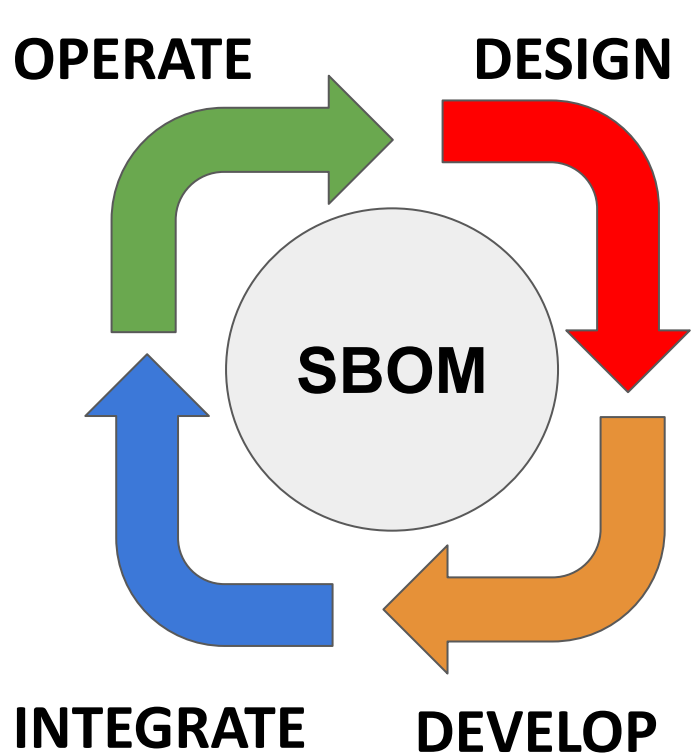
# SBOM Content



# Increasing awareness of SBOMs

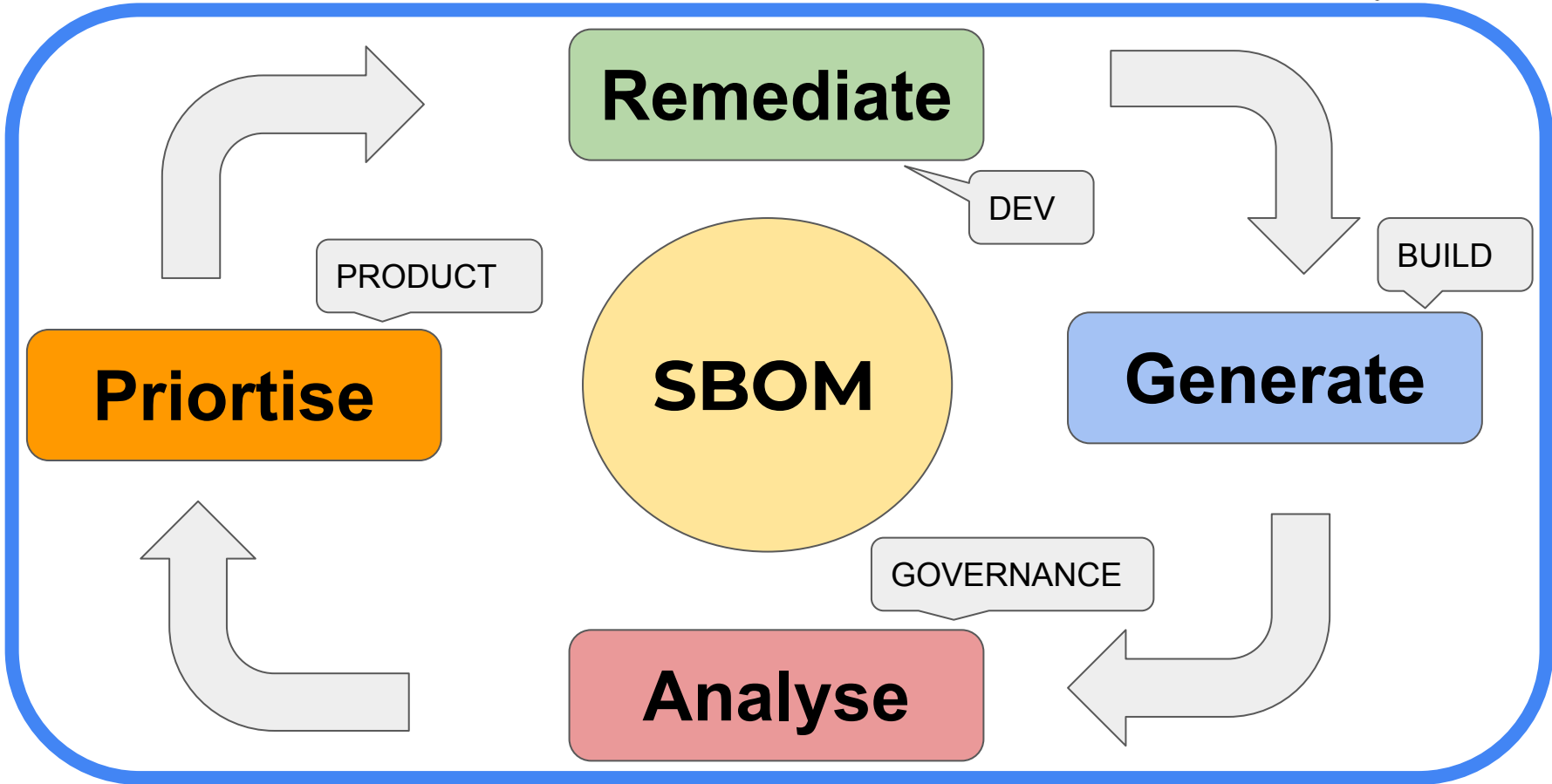


# SBOMs are used throughout the lifecycle



- **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**

CISO







**SBOM**

The diagram consists of a large blue rounded rectangle containing two elements: a yellow circle on the left and a light blue rounded rectangle on the right. The yellow circle contains the text 'SBOM' and the light blue rounded rectangle contains the text 'License'.

**License**



The diagram consists of three main elements: a yellow circle containing the text 'SBOM', a light blue rounded rectangle containing the text 'License', and a purple rounded rectangle containing the text 'Naming'. These elements are arranged within a larger blue rounded rectangle. 'SBOM' is positioned on the left, 'License' is on the right, and 'Naming' is centered below the other two.

**SBOM**

**License**

**Naming**

The diagram features a central yellow circle labeled 'SBOM'. To its right is a light blue rounded rectangle labeled 'License'. Below the 'SBOM' circle are two rounded rectangles: an orange one labeled 'Versioning' on the left and a purple one labeled 'Naming' on the right. All elements are contained within a blue rounded rectangular border.

**SBOM**

**License**

**Versioning**

**Naming**

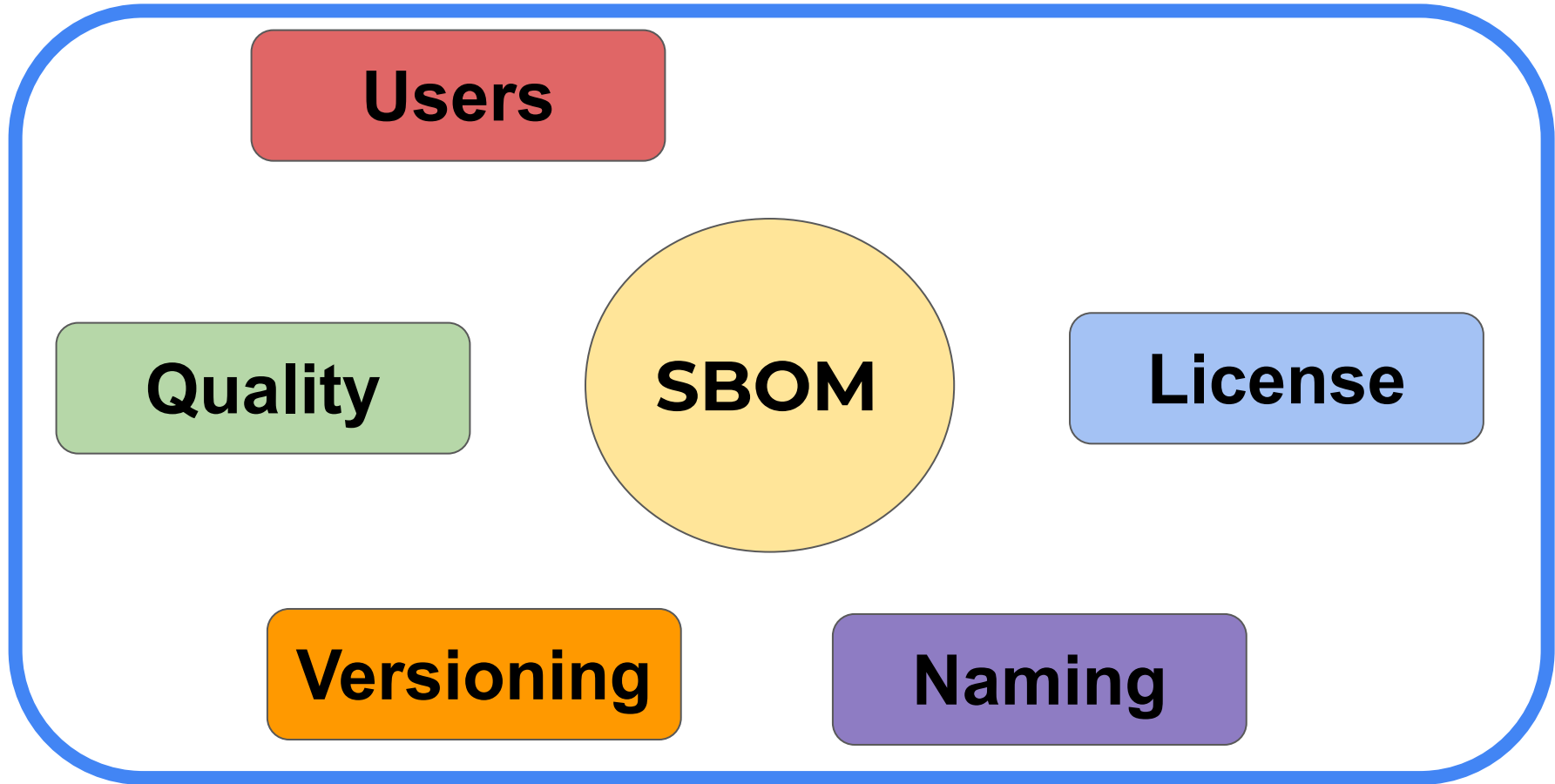
**Quality**

**SBOM**

**License**

**Versioning**

**Naming**



**Users**

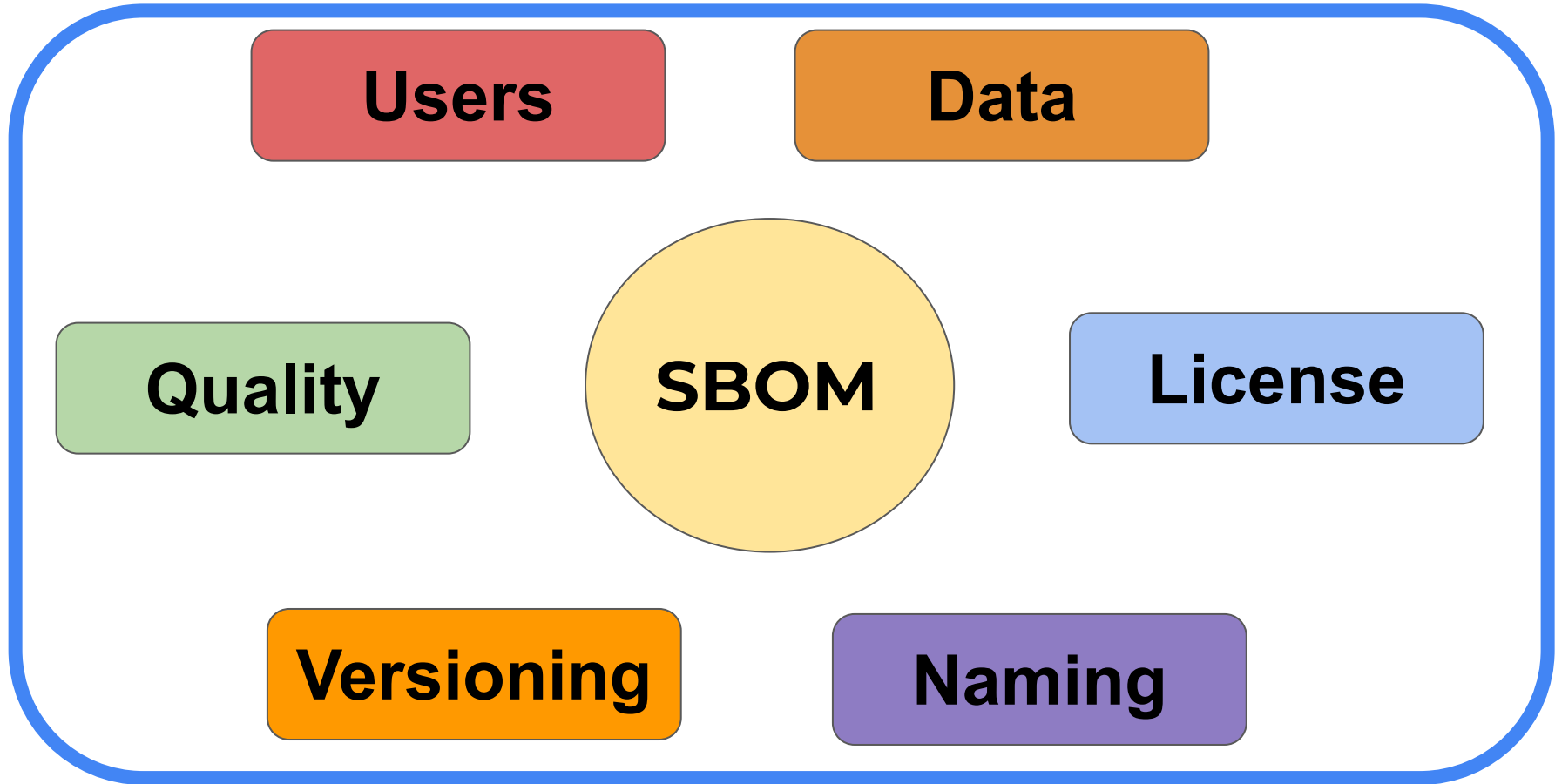
**Quality**

**SBOM**

**License**

**Versioning**

**Naming**



**Users**

**Data**

**Quality**

**SBOM**

**License**

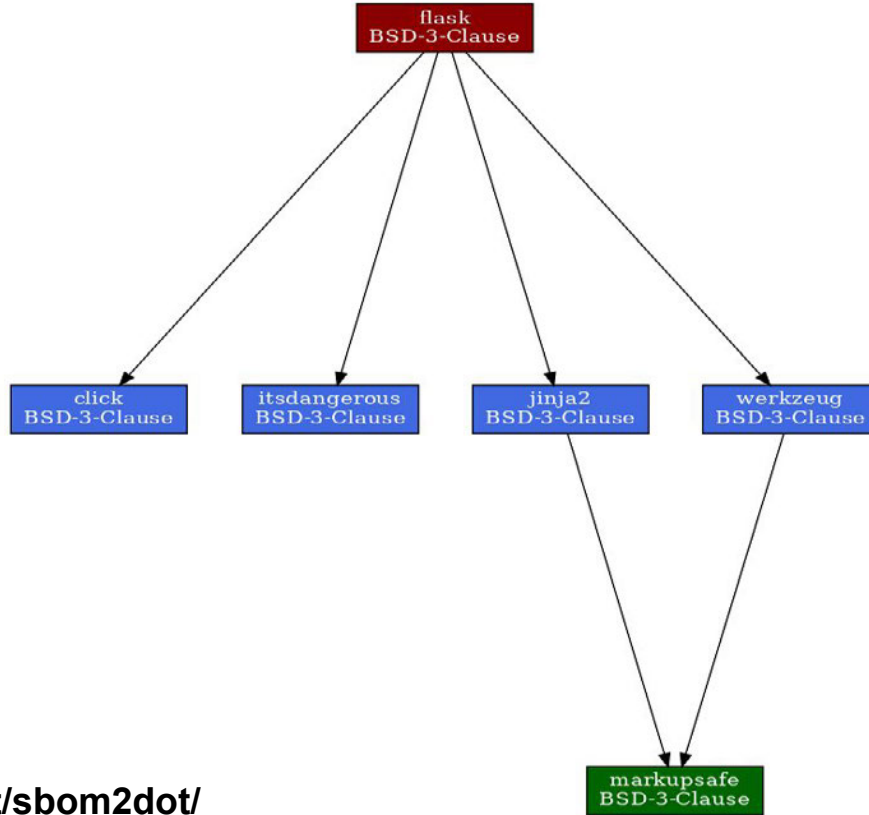
**Versioning**

**Naming**

## 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/>



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

**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**

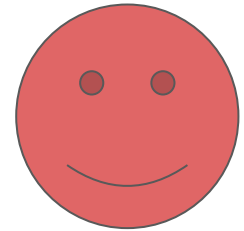
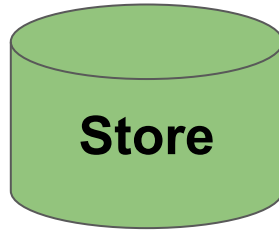
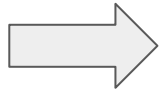
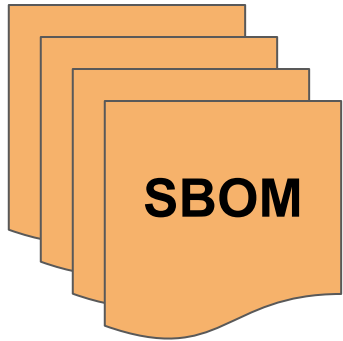
Name	Version	Supplier	License
click	8.1.2	Armin Ronacher	BSD-3-Clause

**License Summary**

License	Count
BSD-3-Clause	1

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





```
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/>

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**

SBOMs are only as good as the data which is provided.

**Everyone** is responsible for improving this data.

[info@aph10.com](mailto:info@aph10.com)

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

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

<https://github.com/anthonyharrison>

