Introduction to the OSADL CRA Policy Template

Caren Kresse
Open Source Automation Development Lab (OSADL) eG

Yet another policy?!

- The OSADL Open Source Policy Template has proved helpful for establishing FOSS **compliance processes**.
- 1st approach: A **combined** FOSS and CRA policy.
- 2nd approach: A **separate** CRA policy with references to the FOSS policy, where appropriate.

1st approach: Combined FOSS and CRA policy

- Both are legal requirements relevant for software.
- Both concern procurement, own development and distribution of products (so processes and tools to manage these are required anyway).
- Many requirements are similar.
- And mainly: Because it makes sense to avoid parallel work!

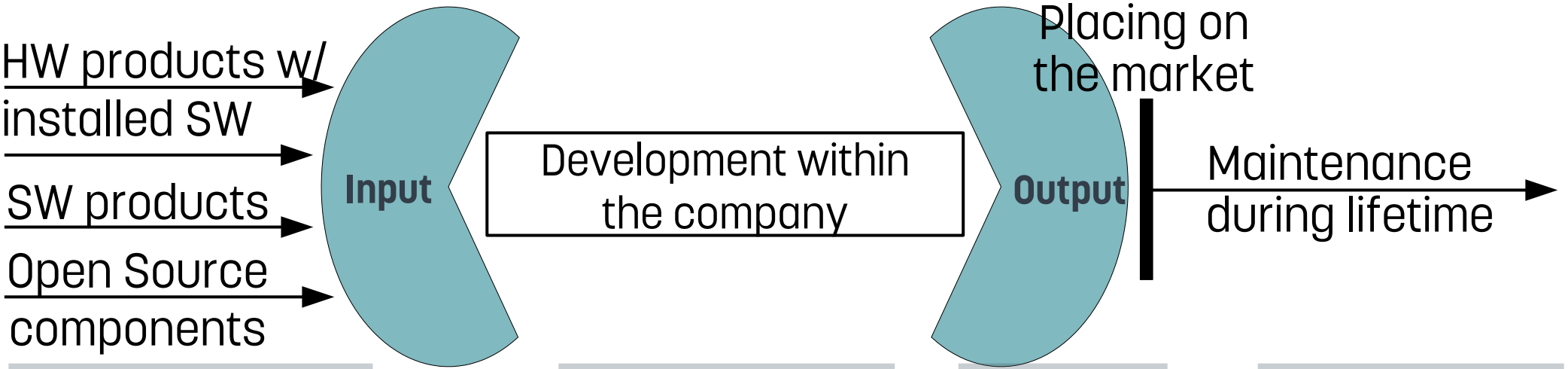
But:

- In some companies, the topics are taken care of by different departments,
- And mainly: The document would be very extensive.

2nd approach: Separate CRA policy

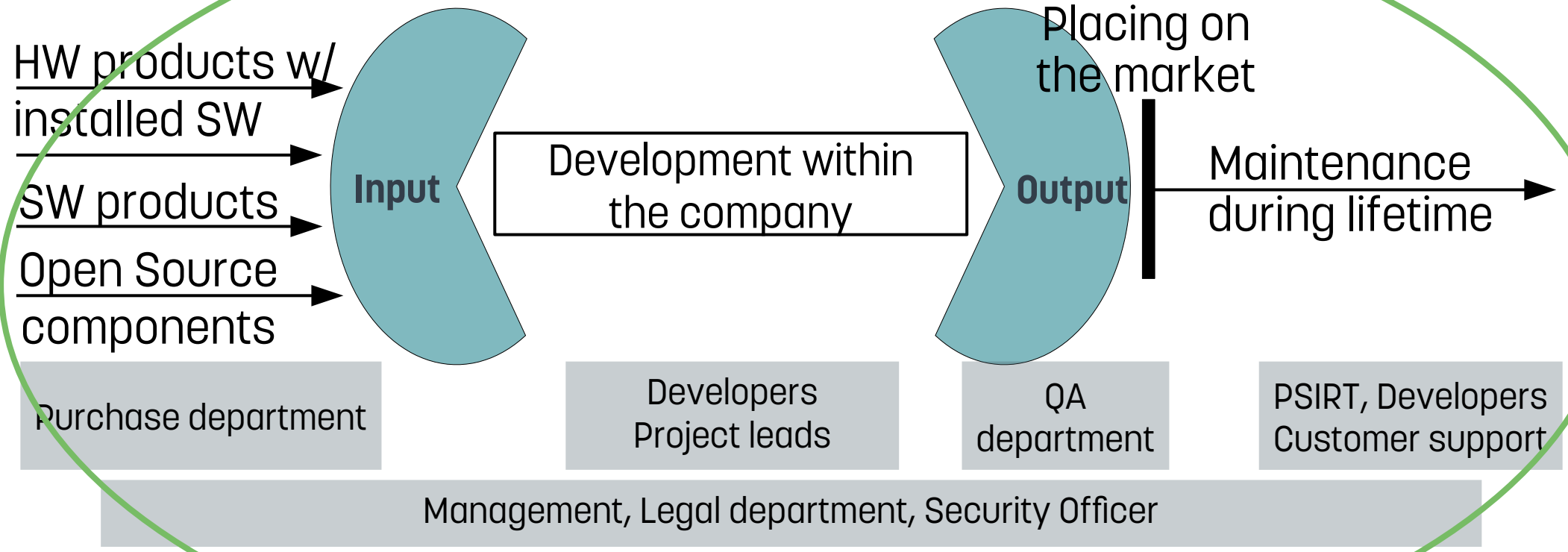
- Allows for a dedicated structure.
- Keeps both documents manageable in size.
- Allows for separate updates of the policy.
- Where appropriate, the FOSS policy can be referenced (and vice versa).

CRA compliance policy: Structure

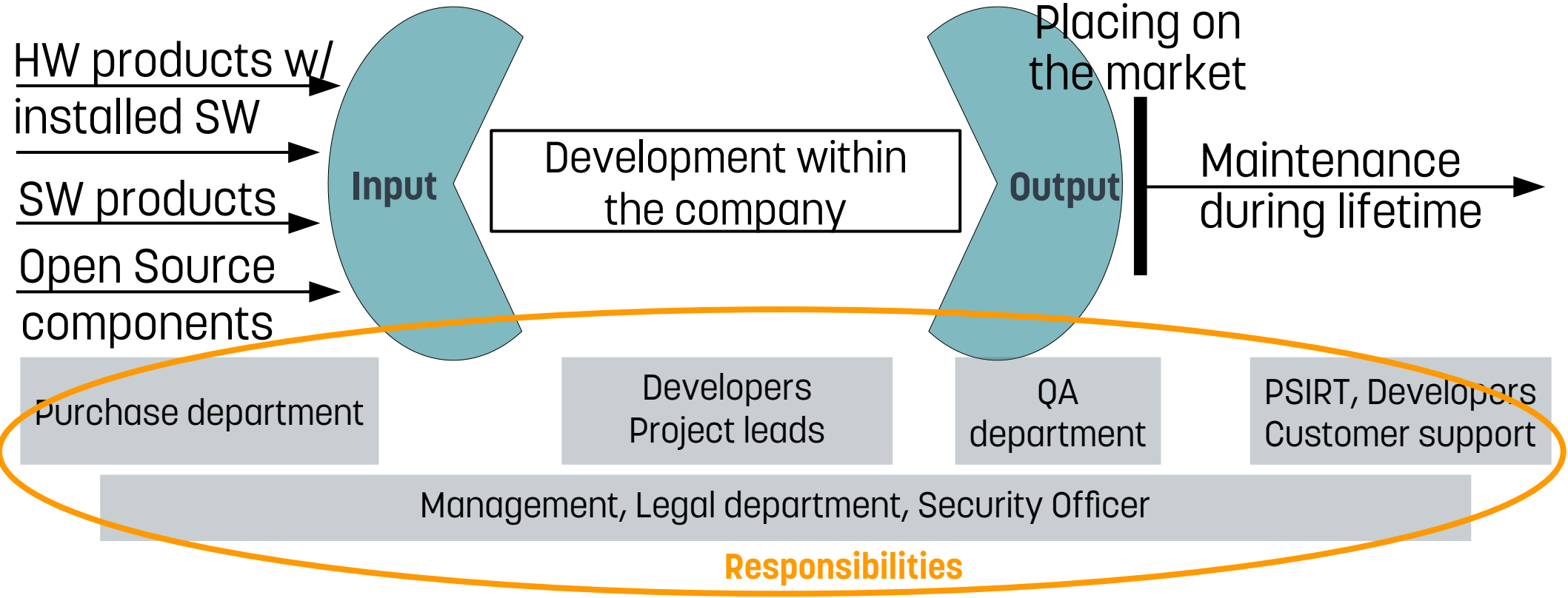


Scope

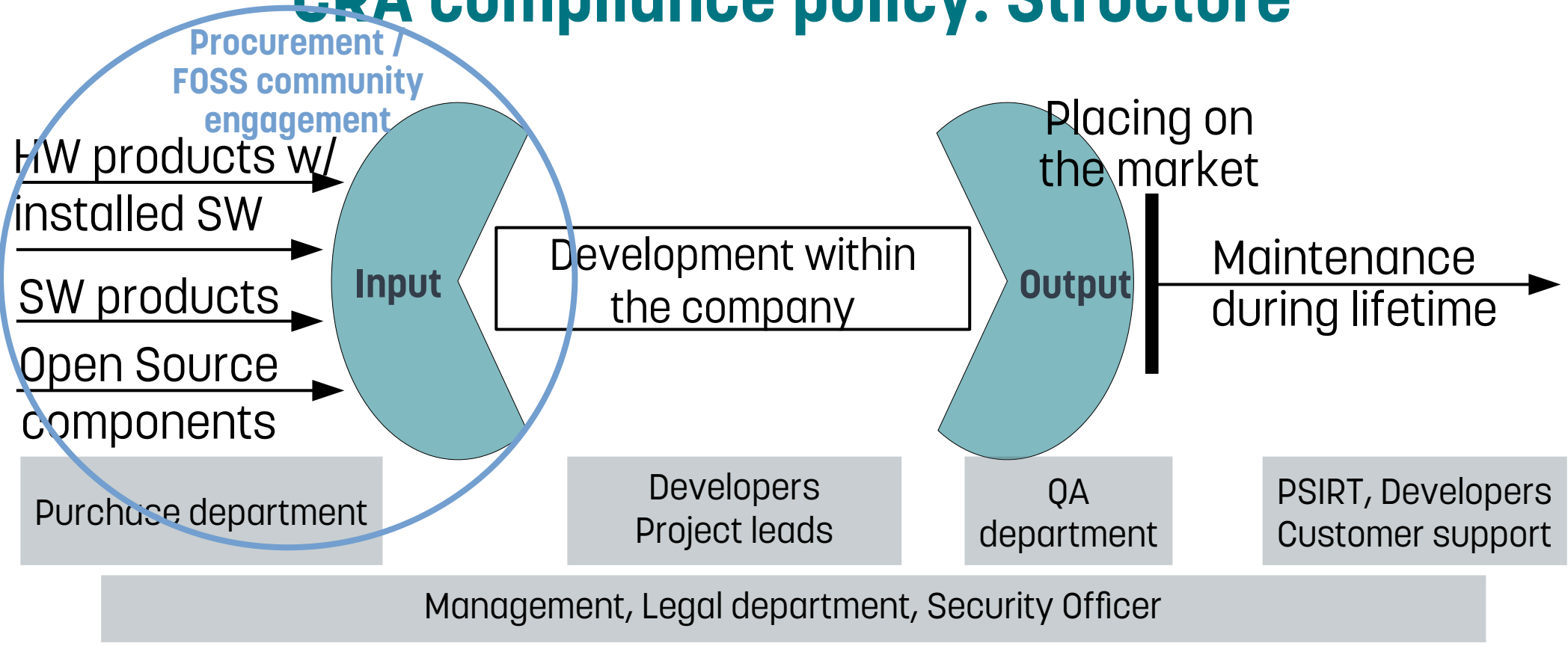
CRA compliance policy: Structure



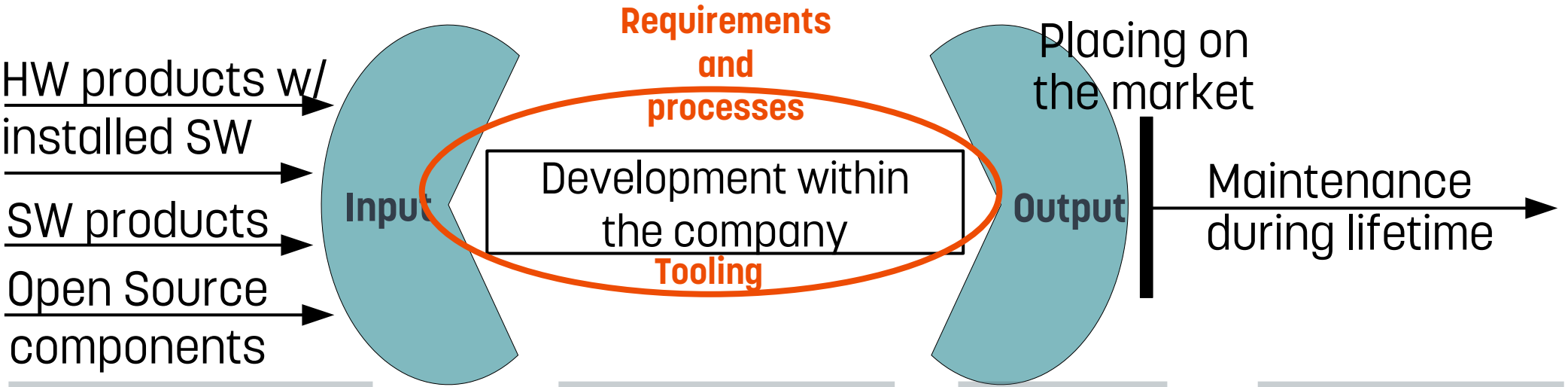
CRA compliance policy: Structure



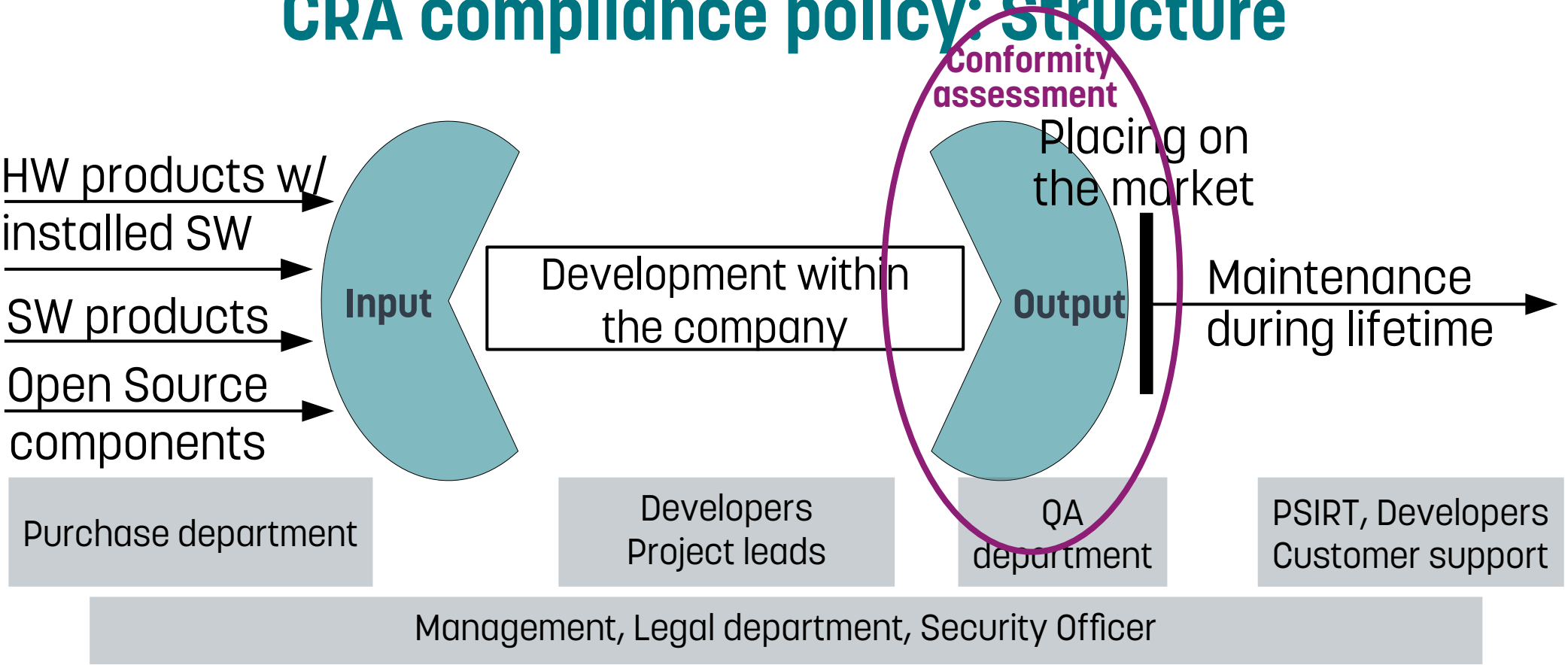
CRA compliance policy: Structure



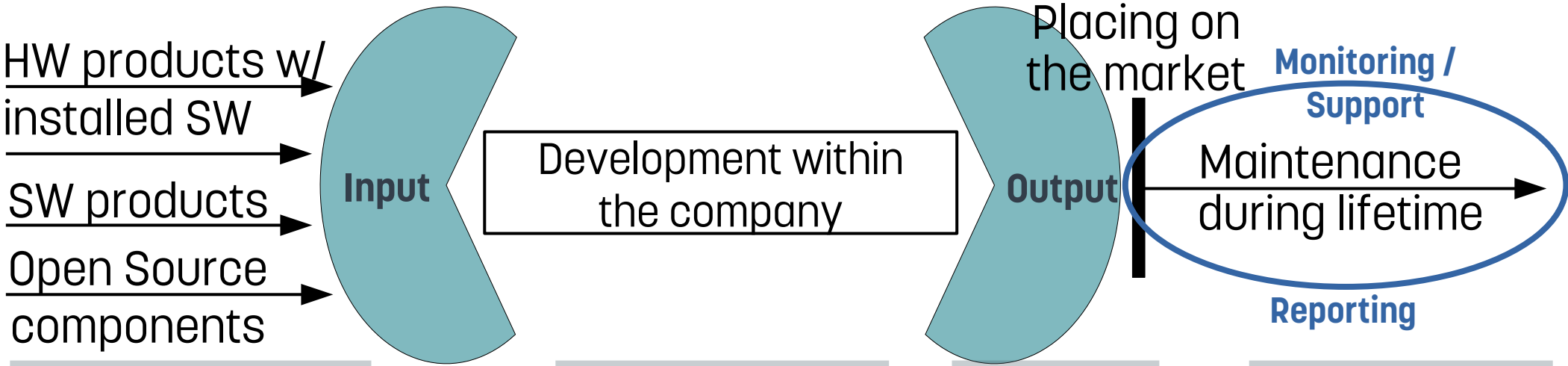
CRA compliance policy: Structure

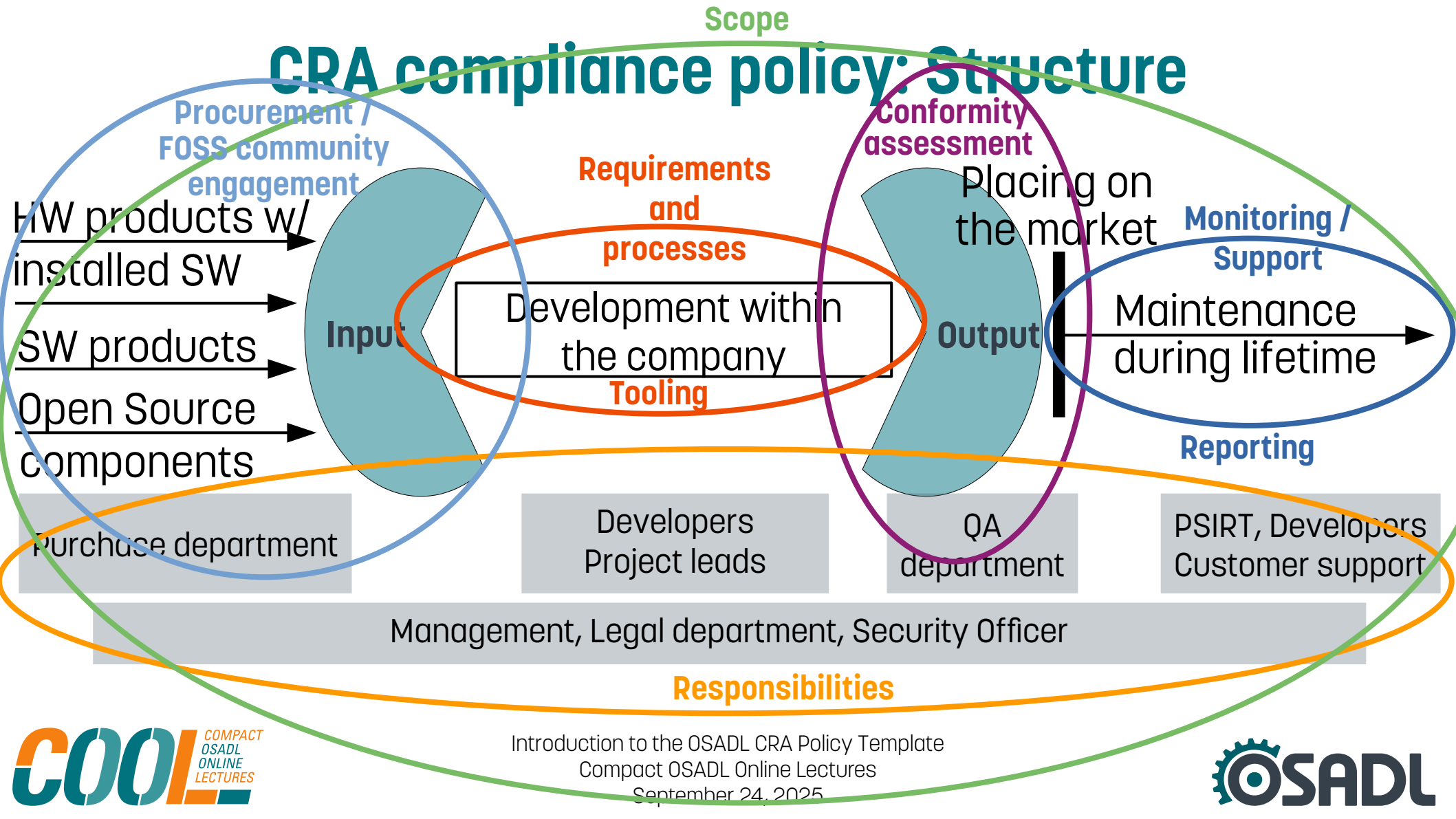


CRA compliance policy: Structure



CRA compliance policy: Structure




Scope
CRA compliance policy: Structure
Procurement / FOSS community engagement
Conformity assessment
Requirements and processes
Monitoring / Support
HW products w/ installed SW
SW products
Open Source components
Input
Development within the company
Tooling
Output
Placing on the market
Maintenance during lifetime
Reporting
Purchase department
Developers Project leads
QA department
PSIRT, Developers Customer support
Management, Legal department, Security Officer
Responsibilities

CRA compliance policy: Content (1)

- Scope:
  - Timeline for obligations to come into force
  - Classification of product criticality
  - Types of products (embedded, PC, Cloud services, ...) and addressees (manufacturers, importers, distributors)
  - Stages of a product's development and lifetime

CRA compliance policy: Content (1)

- Scope:
  - Timeline for obligations to come into force
  - Classification of product criticality
  - Types of products (embedded, PC, Cloud services, ...) and addressees (manufacturers, importers, distributors)
  - Stages of a product's development and lifetime

- Allocation of responsibilities:
  - Decisions of management & legal department
  - Project leads ad developers to implement security standards and update mechanism
  - Security officer as contact person for vulnerability reports
  - PSIRT (Product Security Incident Response Team) to react to reports of actively exploited vulnerabilities

CRA compliance policy: Content (2)

- Procurement
  - Requiring CRA compliance from suppliers
  - Evaluating quality (e.g. “security by design”)
  - Agreeing on support time
  - Setting up an approval process for FOSS and proprietary software

CRA compliance policy: Content (2)

- Procurement
  - Requiring CRA compliance from suppliers
  - Evaluating quality (e.g. “security by design”)
  - Agreeing on support time
  - Setting up an approval process for FOSS and proprietary software
- FOSS community engagement
  - CRA requirements do not apply to FOSS stewards, but to manufacturers using FOSS
  - Establishing a relationship with maintainers of critical FOSS components
  - Collaborating with community to create required materials
  - Reporting vulnerabilities to FOSS projects

CRA compliance policy: Content (3)

- Requirements and processes:
  - Product classification
  - SBOM creation
  - Detecting & classifying vulnerabilities
  - Secure programming, pen testing and other security measures
  - Documentation requirements

CRA compliance policy: Content (3)

- Requirements and processes:
  - Product classification
  - SBOM creation
  - Detecting & classifying vulnerabilities
  - Secure programming, pen testing and other security measures
  - Documentation requirements
- Tooling
  - FOSS or proprietary
  - One-stop-for-all or diverse tooling landscape

CRA compliance policy: Content (4)

- Conformity assessment
  - Self-certification or third-party (depending on classification of criticality)
  - Documentation

CRA compliance policy: Content (4)

- Conformity assessment
  - Self-certification or third-party (depending on classification of criticality)
  - Documentation
- Monitoring
  - Selecting and monitoring sources for vulnerability reports
  - Process for intake and analysis of reports
- Support
  - Release and update strategy to remediate vulnerabilities
- Reporting obligations
  - For actively exploited vulnerabilities
  - To authorities, users and FOSS projects within certain time limits

CRA compliance policy: Content (4)

- Conformity assessment
  - Self-certification or third-party (depending on classification of criticality)
  - Documentation
- Monitoring
  - Selecting and monitoring sources for vulnerability reports
  - Process for intake and analysis of reports
- Support
  - Release and update strategy to remediate vulnerabilities
- Reporting obligations
  - For actively exploited vulnerabilities
  - To authorities, users and FOSS projects within certain time limits
- Enforcement

Outlook

- The OSADL CRA Policy Template is work in progress.
- OSADL members will be notified when a first version is available.
- Beta testers may sign up for pre-release versions by contacting office@osadl.org.

Combined CRA and FOSS compliance approval process for FOSS* components

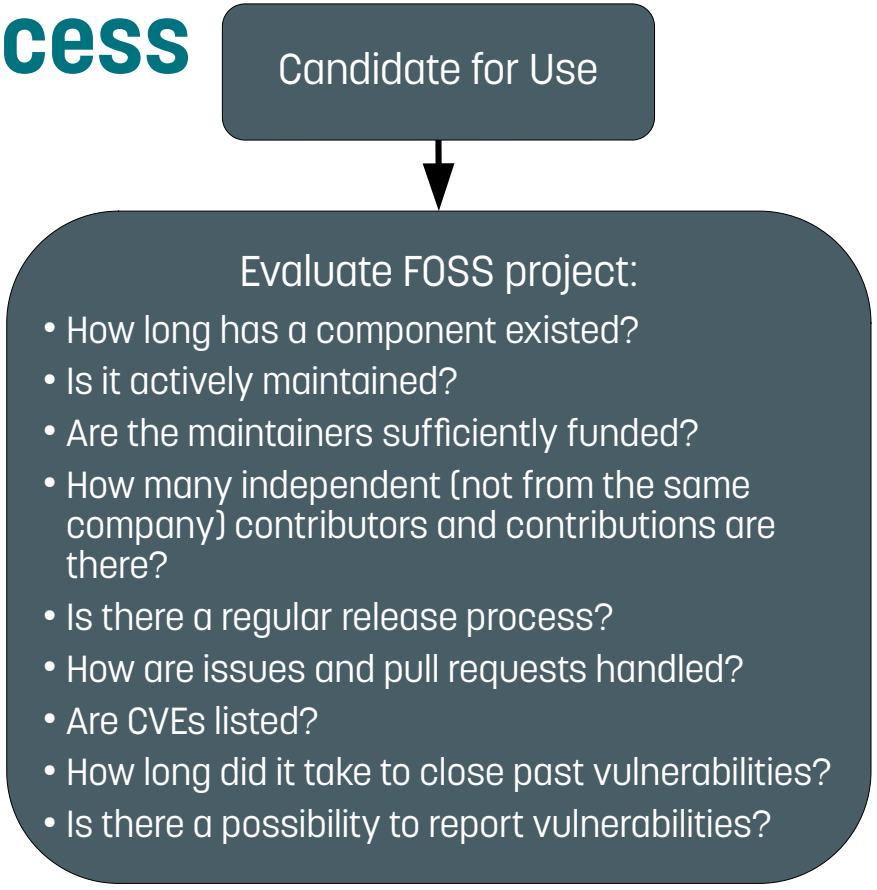
*Can partly also be applied for proprietary components

COOL COMPACT OSADL ONLINE LECTURES

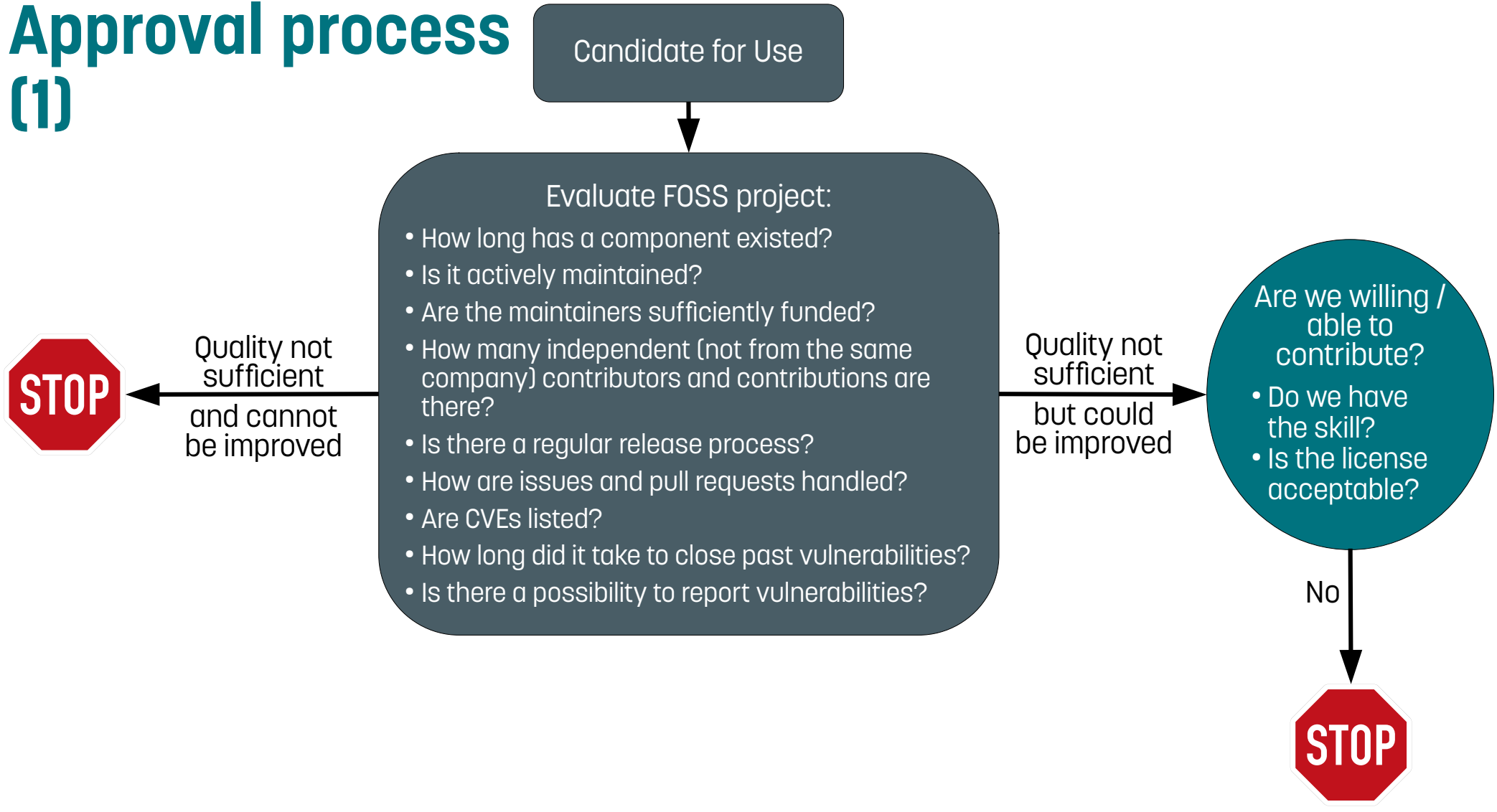
Introduction to the OSADL CRA Policy Template
Compact OSADL Online Lectures
September 24, 2025

OSADL

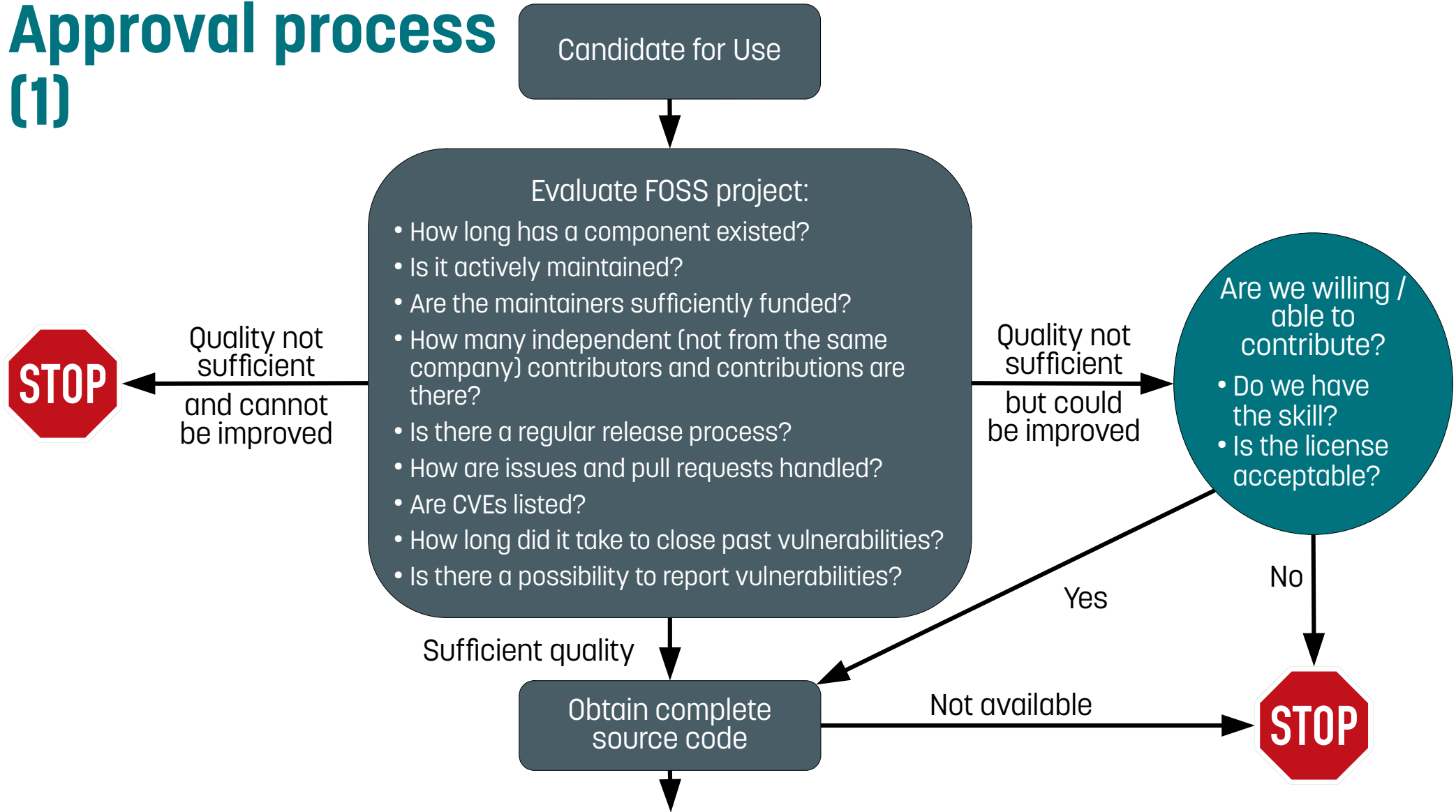
Approval process (1)



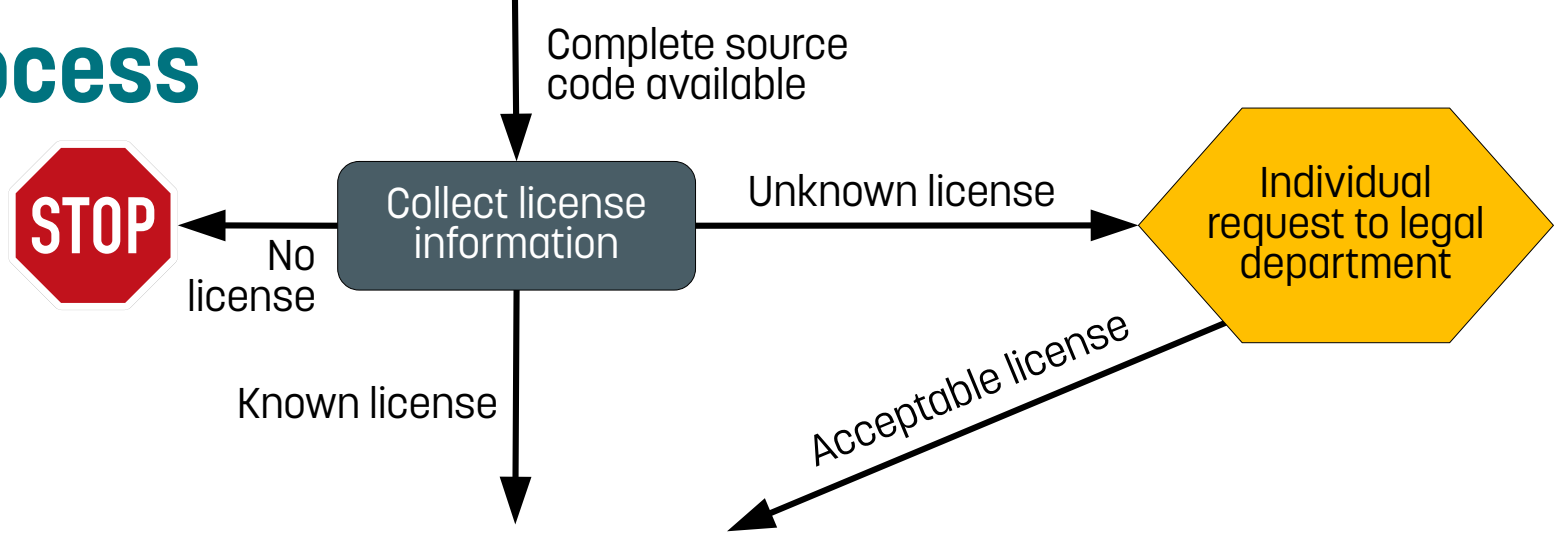
Approval process (1)



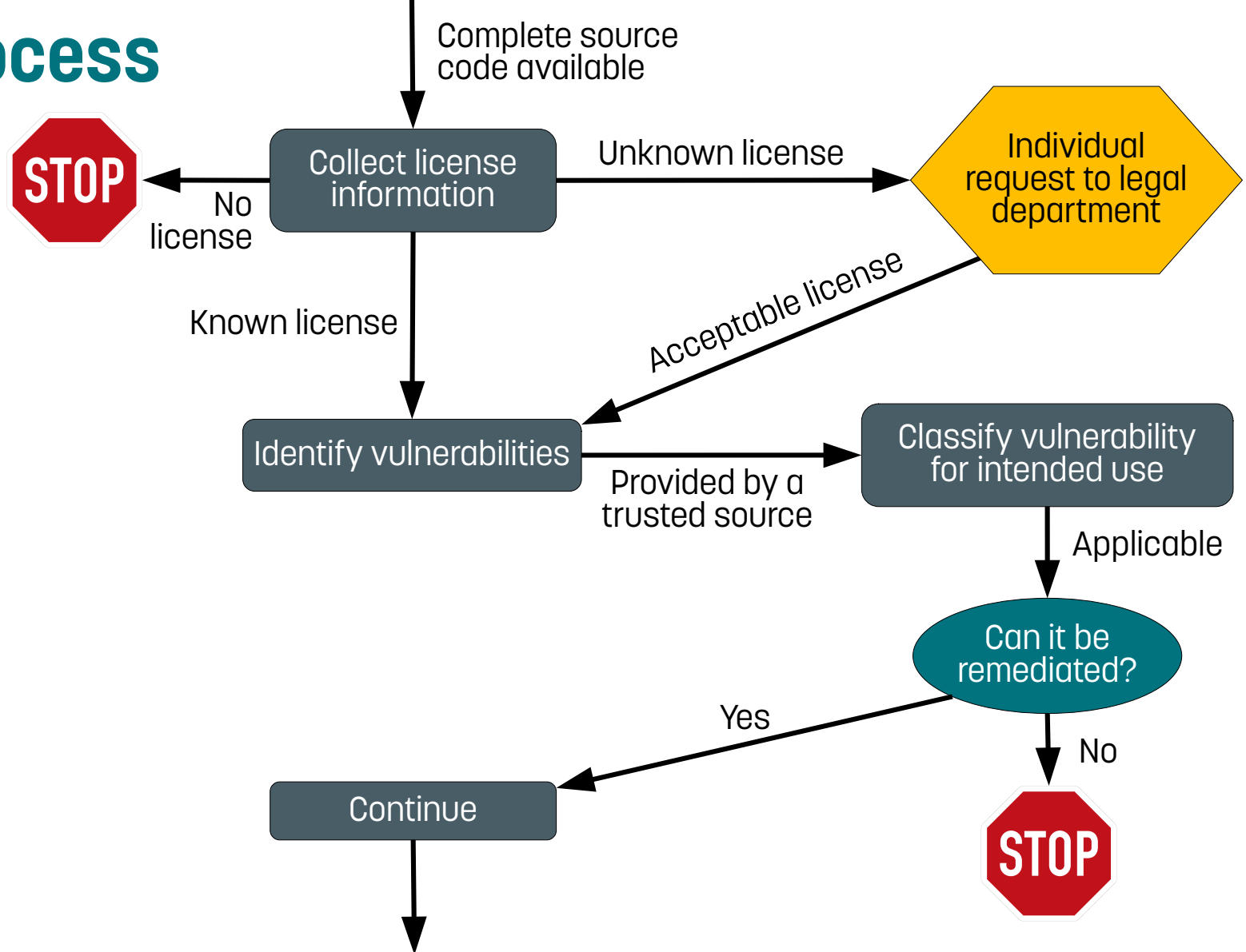
Approval process (1)



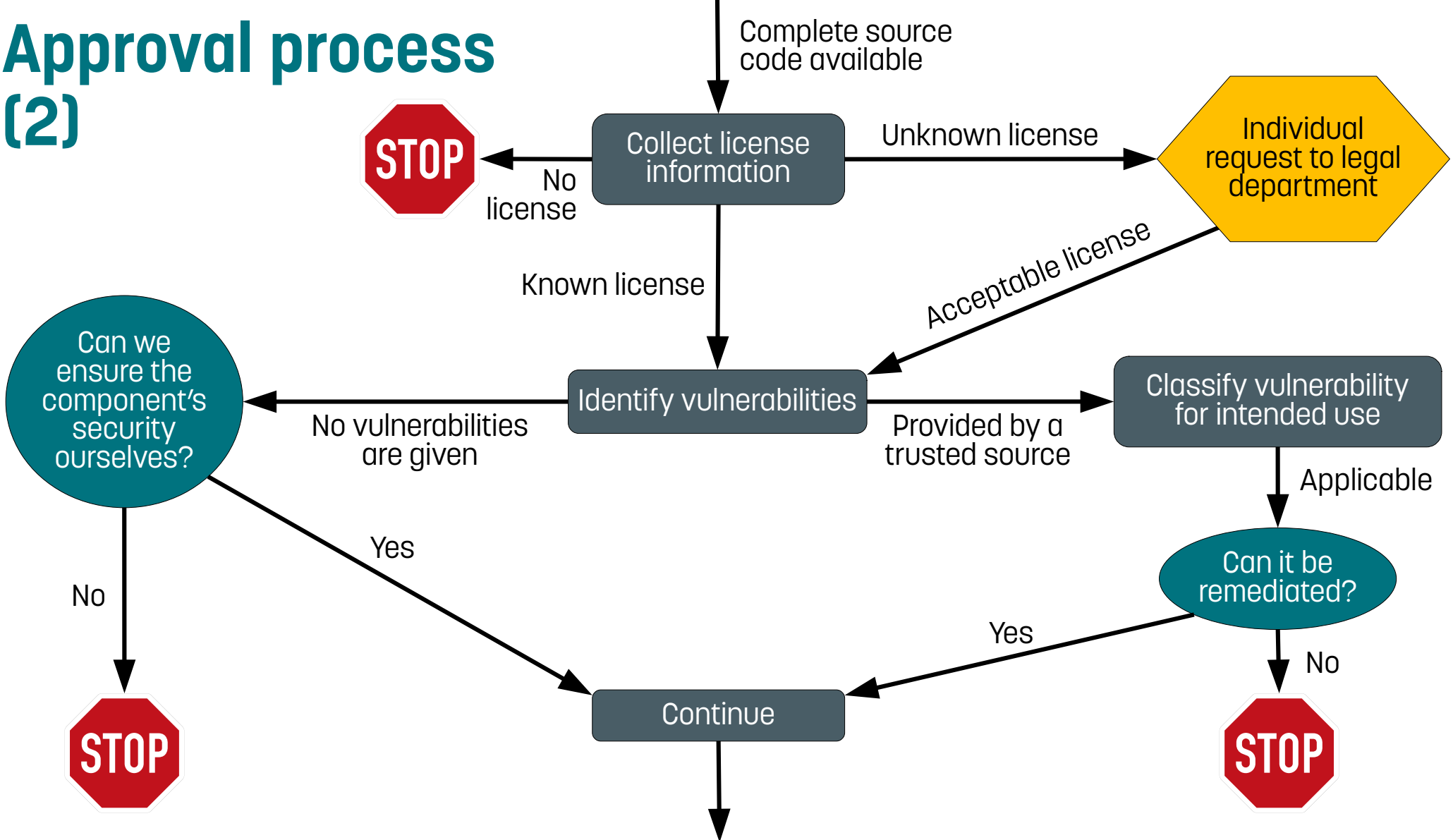
Approval process (2)



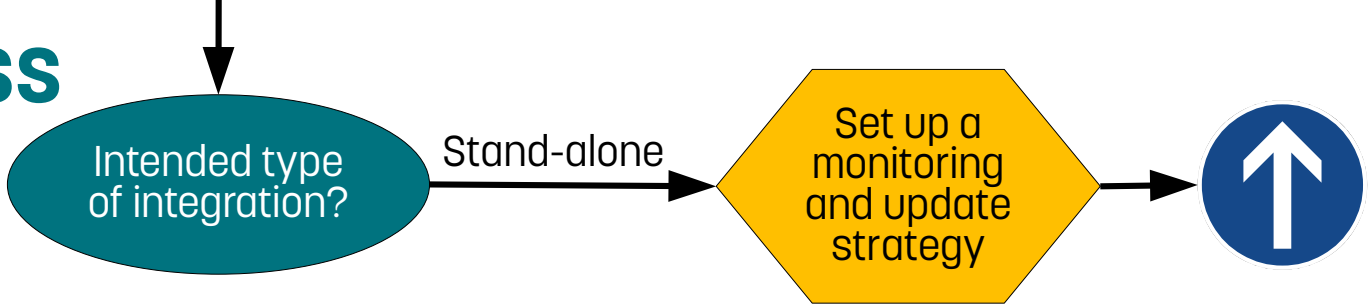
Approval process (2)



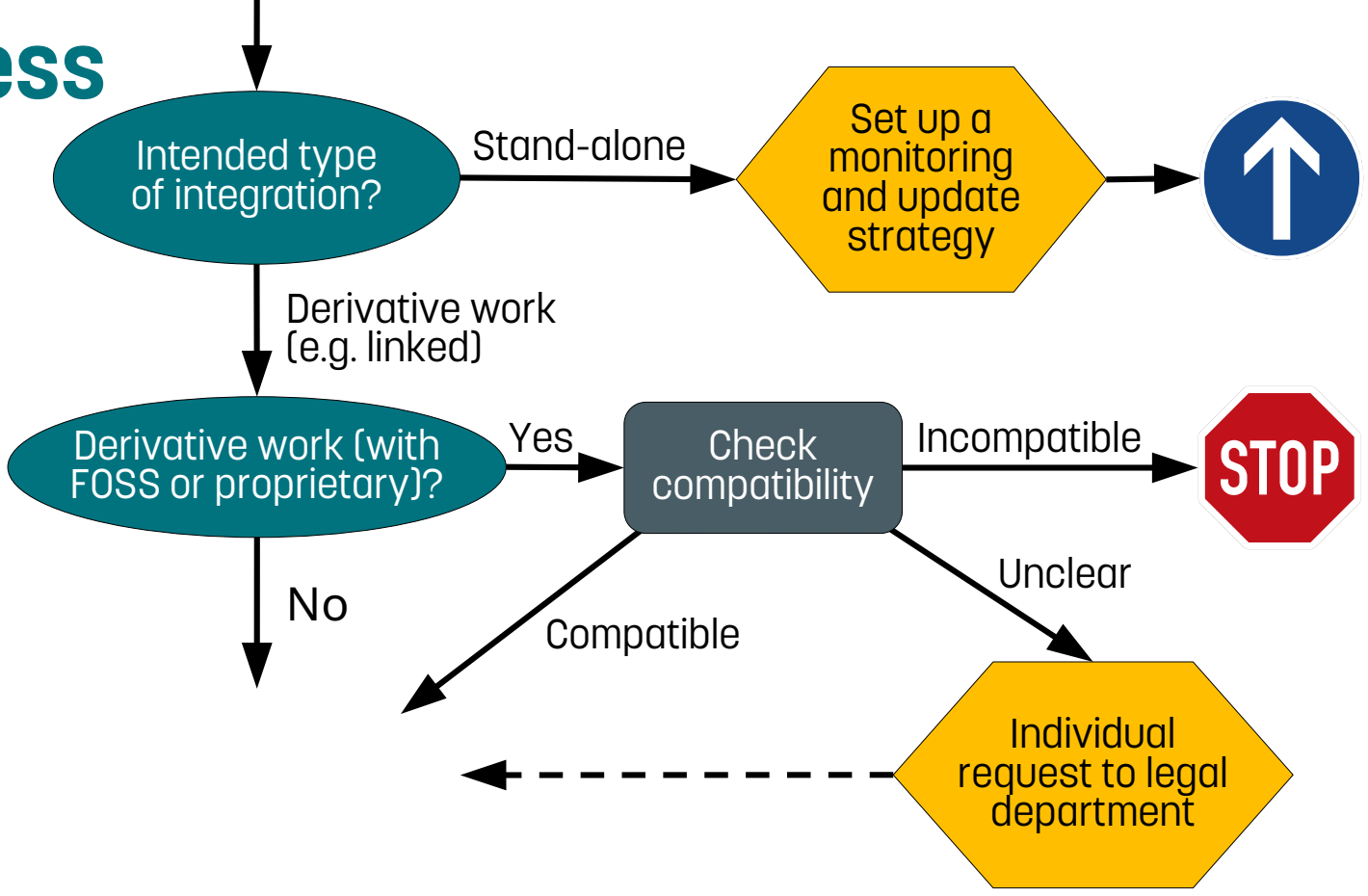
Approval process (2)



Approval process (3)



Approval process (3)



Approval process (3)