Open Source Contributions & Security

Der Weg zu einer Strategie

Martina Götz & Christof Walter | SAP SE
September, 2023

PUBLIC

SAP Global Security

THE BEST RUN SAP

Sprecher

Martina Götz

OSS Security Governance Owner

Product Security Code Governance

Christof Walter

Security Engineer

Security Validation

SAP Global Security

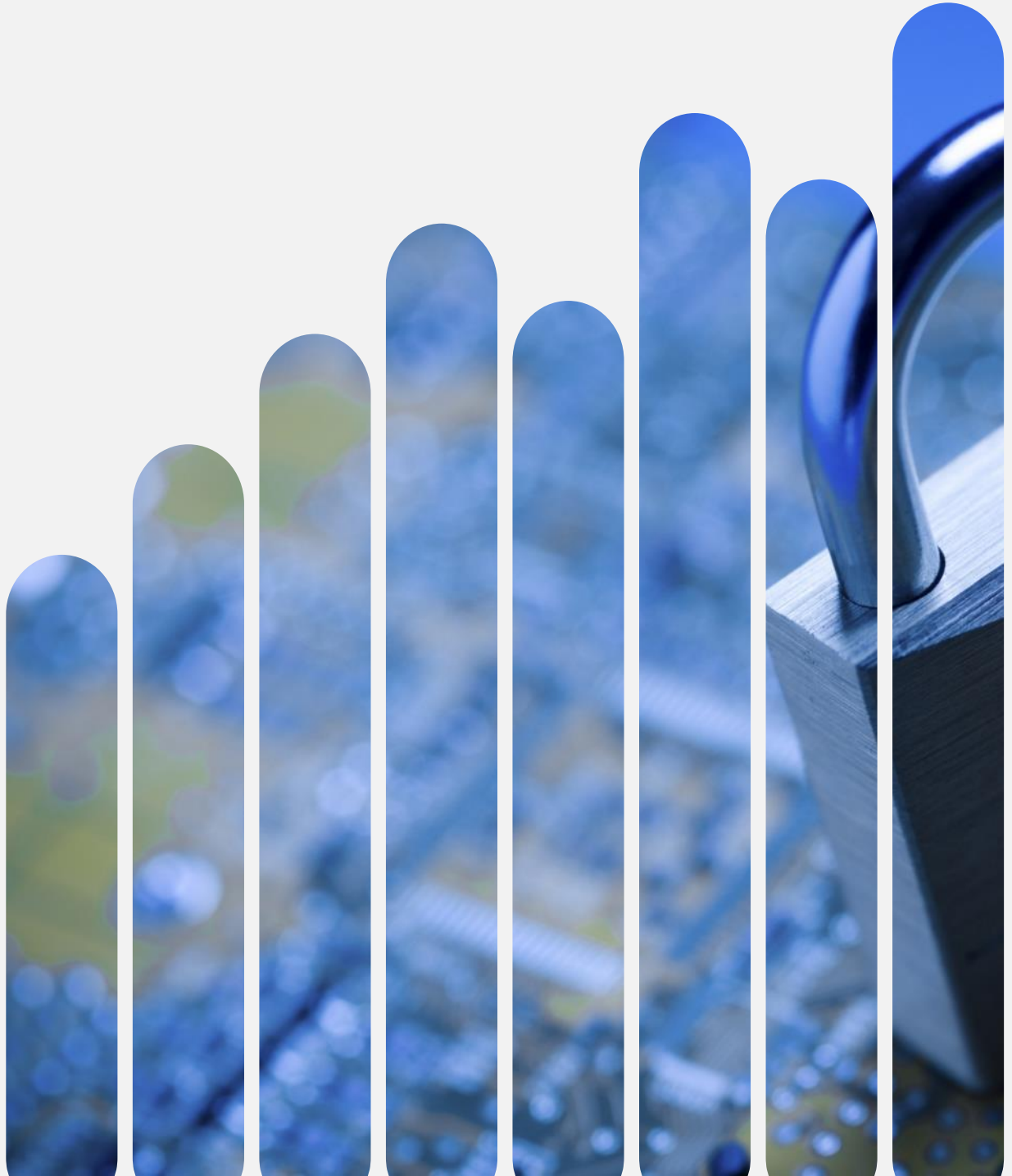
THE BEST RUN SAP

Motivation

Nutzung OSS ↗

OSS-Rolle ☑

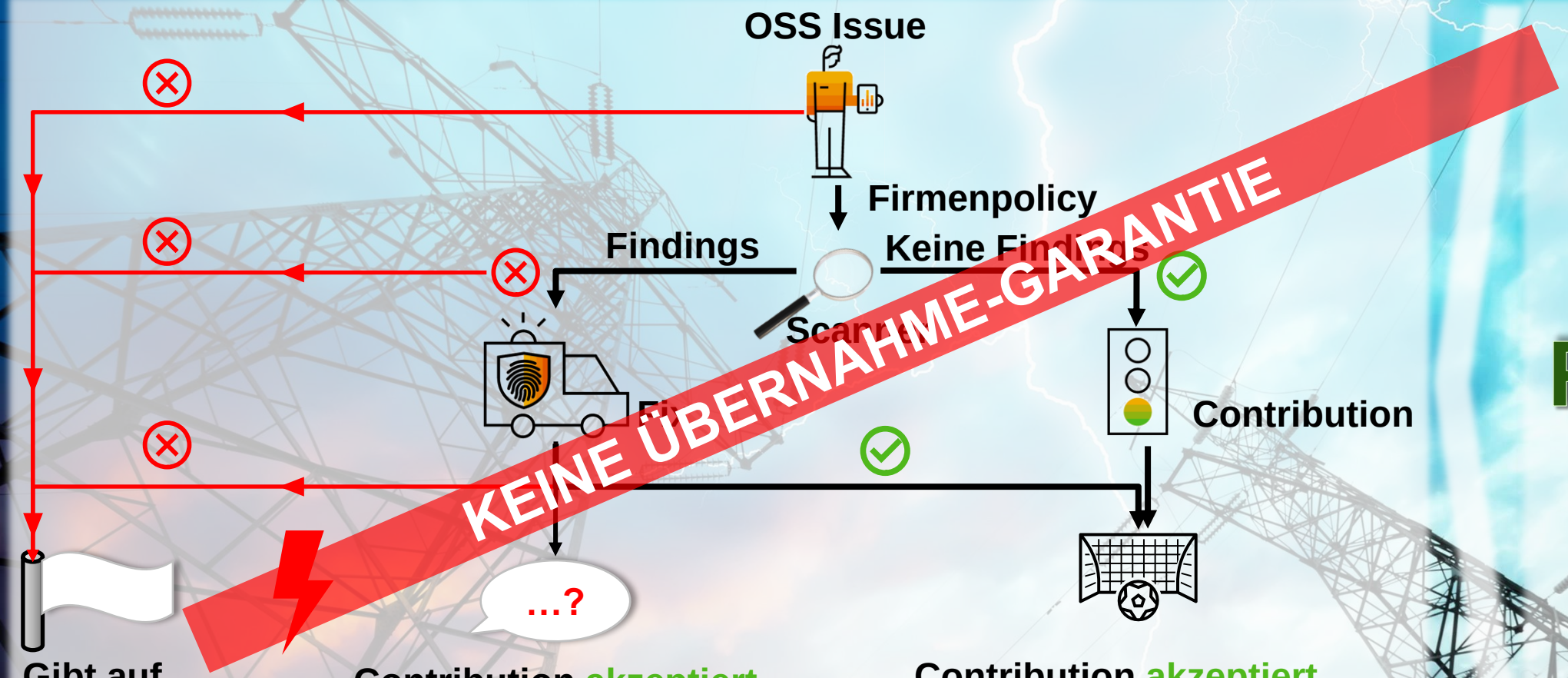
Sicherheit ?



3 wesentliche Szenarien

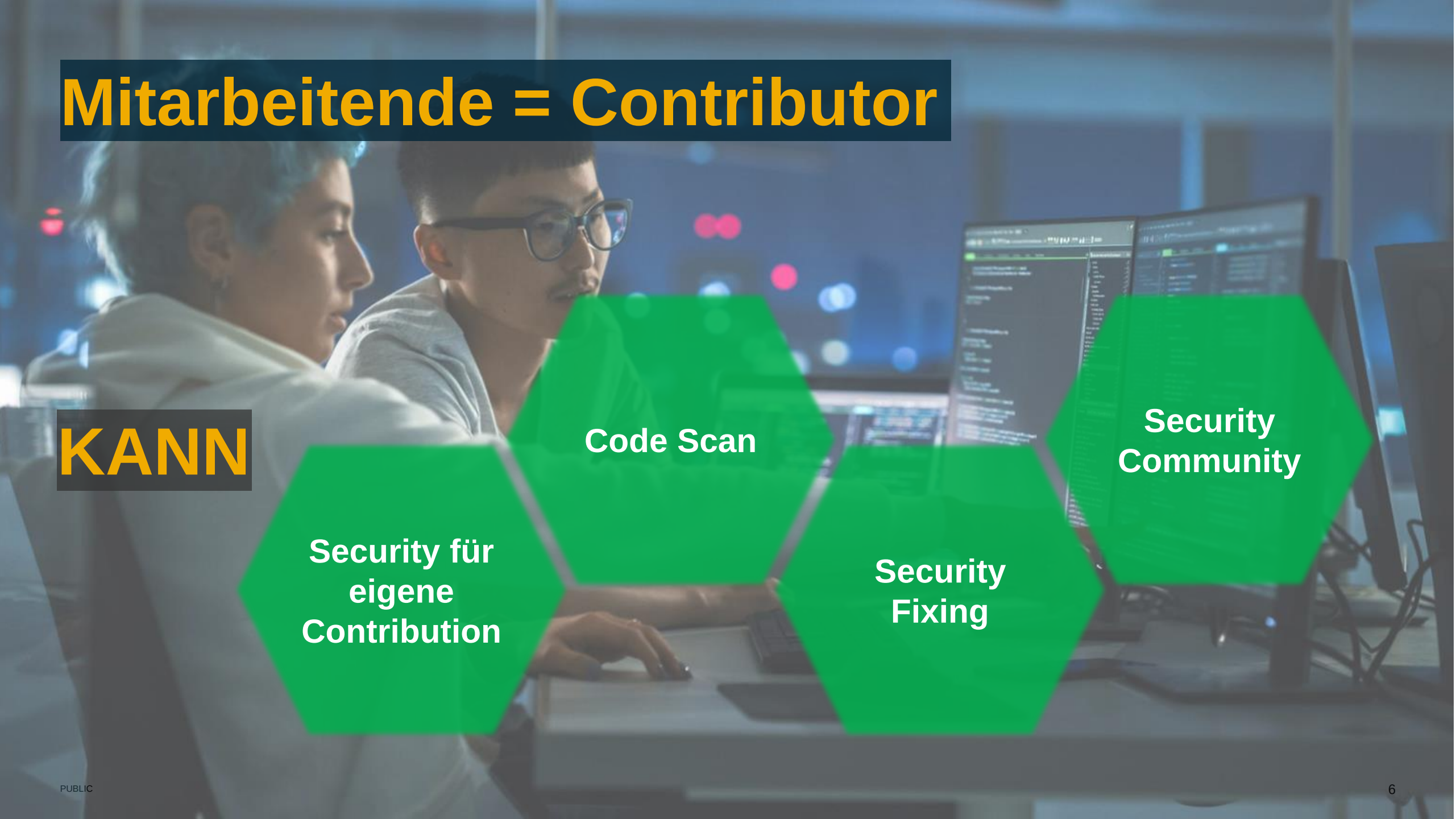
- Mitarbeitende = Contributor
- Mitarbeitende = Maintainer
- Firma = Publisher einer Open Source Library und Hauptmaintainer

OSS ⇔ eigener Code?



Policy

Mitarbeitende = Contributor



KANN

- Code Scan
- Security Community
- Security für eigene Contribution
- Security Fixing

Mitarbeitende = Maintainer

Firma übernimmt mehr Verantwortung, insbesondere für Security

Soll

- ✓ Contribution auf Security prüfen
- ✓ Keine neuen Issues akzeptieren
- ✓ Code regelmäßig prüfen
- ✓ Abhängigkeiten aktualisieren

Firma als Publisher/ Hauptmaintainer

Trägt Hauptverantwortung, incl. Sicherheit

MUSS: Sicherheitspolicy

- ✓ **Anwendung passender Tools**
- ✓ **Abhängigkeiten aktualisieren**
- ✓ **Analysieren & Fixen**
- ✓ **Contributions absichern**

- ✓ **OSS wie eigenen Code behandeln**
- ✓ **Regelmäßig und zeitnah**
- ✓ **Transparenz**

Cyber Resilience Act

IT Sicherheit für Hard-/ Software (Cybersecurity Risk Assessment)

OSS-Regulierung

- **Formulierungen und Definitionen**
- **Beteiligung OSS Communities**
- **Kommerzielle Nutzung**

CRA – Folgen und Gefahren

- Überregulierung & Bürokratie
- Haftung und Due Diligence
- Rollen

Auswirkungen

- Schaden am OSS Ökosystem
- Digitale Souveränität
- Gefahr für Innovation und Wertschöpfung

CRA – Schlussfolgerungen

Allgemein

- ✓ Kommerziell- gewinnorientierte Nutzung (Downstream)
- ✓ Einbindung OSS Communities, z.B. OpenSSF
- ✓ Hilfestellungen

Strategisch-kommerziell

- ✓ Contribution-Modell wählen/ prüfen
- ✓ Vernetzung mit OSS Communities & Behörden
- ✓ Regularien ⇔ Policies, Trainings, Unterstützung
- ✓ Transparenz

CRA – Schlussfolgerungen (strat.-komm.)

Zusammenfassung

KANN

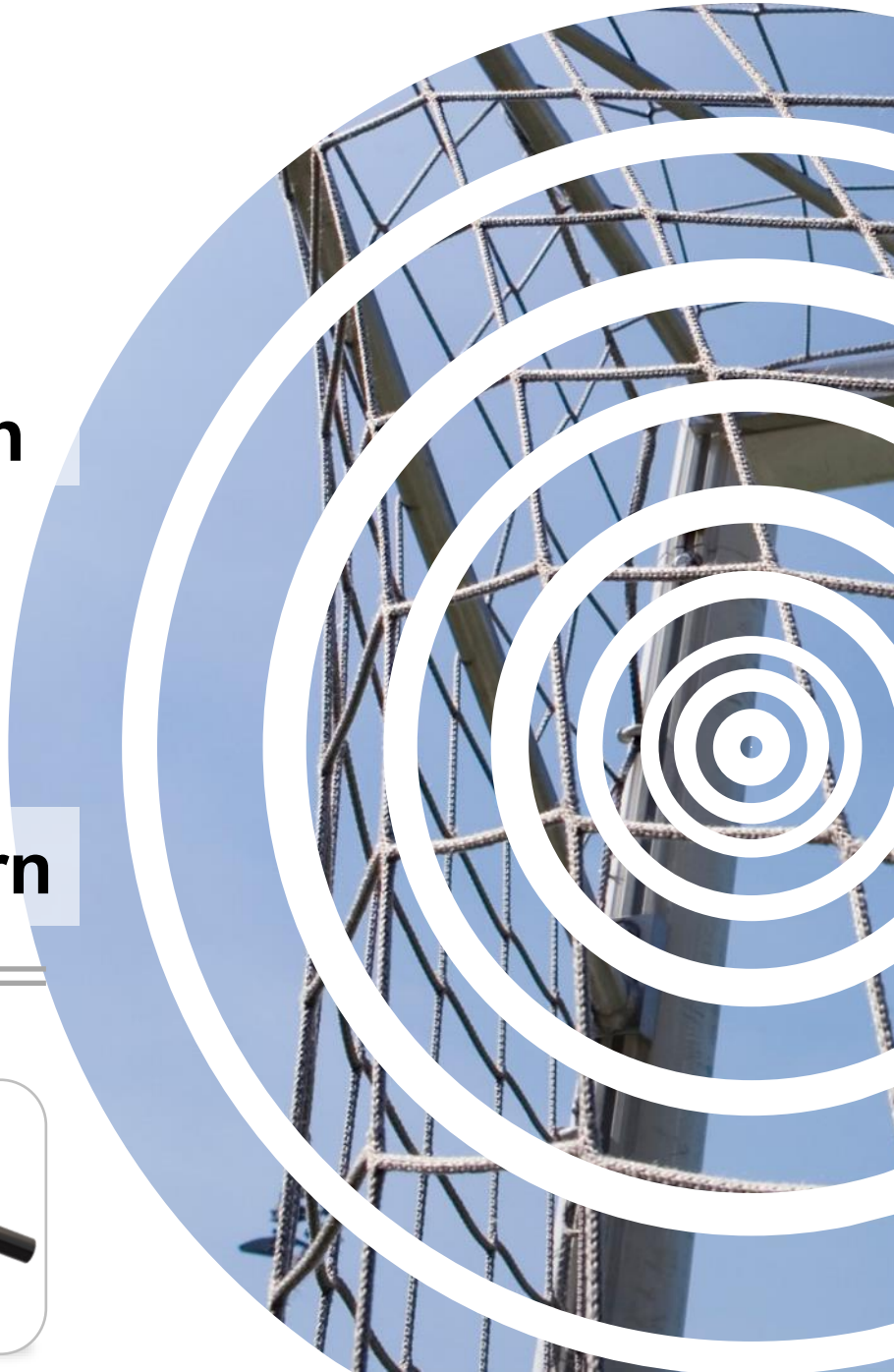
✓ **Contributer können Sicherheit verbessern**

SOLL

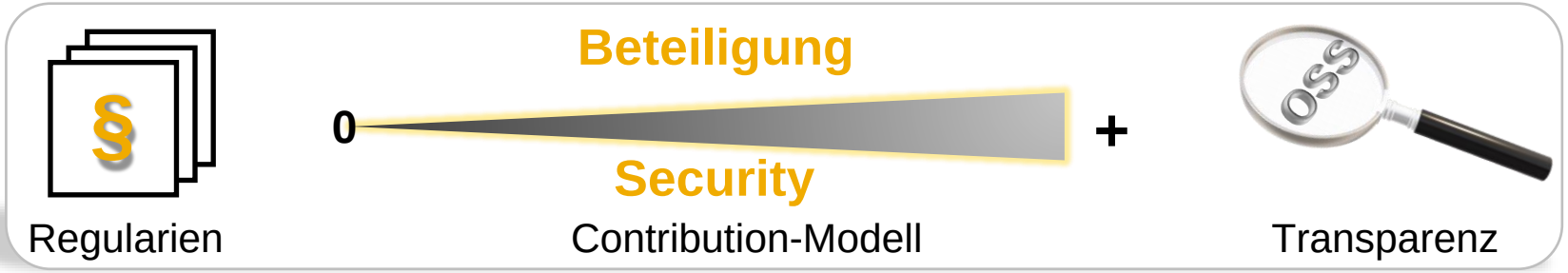
✓ **Maintainer sollen Sicherheit verbessern**

MUSS

✓ **„Publisher" müssen Sicherheit verbessern**



OSS Security Policy & Transparenz



Danke für Ihre Aufmerksamkeit

Fr. Martina Goetz

SAP SE

Dietmar-Hopp-Allee 16

69190 Walldorf, Germany

Mail: martina.goetz@sap.com

Phone: +49 6227 7 48986

Hr. Christof Walter

SAP SE

Dietmar-Hopp-Allee 16

69190 Walldorf, Germany

Mail: christof.walter@sap.com

Phone: +49 6227 7 67464