

Regulierung von OSS

Beschränken oder fördern gesetzliche Regulierungen
den internationalen, offenen, kollaborativen Raum der
Open Source Software?

September 2023

Your speaker



Julian Rau | OSS Expert

📍 Stuttgart
☎ +49 151 16584615
✉ julian.rau@pwc.com

Background in Business IT

Technical expertise in:

- OSS Management Systems
- Open Source Programm Office
- Open Source for the public sector
- Agile software development

Agenda

- 1 Entwicklung von Open Source
Regulierung
- 2 Chancen und Herausforderung durch
Regulierung von Open Source
- 3 Call to action

Entwicklung von Open Source-Regulierung

This overview is intended to show a selection of current guidelines and documentation referring to Open Source Management and does not claim to be complete.

Cyber Resilience Act

EU – Cybersecurity requirements for products with digital elements



BAIT

BaFin – Supervisory Requirements for IT in Financial Institutions



TIBER

EU – Framework for Threat Intelligence-based Ethical Red Teaming



BSI-KritisV

BSI – Critical infrastructure operators must implement attack detection systems



BSI SBOM

BSI – Minimum Requirements for quality of SBOMs



DORA

EU – Digital Operational Resilience Act to increase the digital resilience of financial institutions



VAIT

BaFin – Supervisory Requirements for IT in Insurance Undertakings



EU MDCG

EU – Guidance on Cyber Security for medical Devices



FDA GoCS

US – Food and Drug Administration Guidance on Cyber Security Responsibilities for Medical Devices Manufacturers



Secure Supply Chain for IoT

EU – Security Guidelines the IoT supply chain



Securing Open Source Software Act

US Framework incorporating government, industry, and OSS community frameworks



...

Deutschland

Bankaufsichtliche Anforderungen an die IT: BAIT

„Die Integrität der Anwendung (insbesondere des **Quellcodes**) ist angemessen sicherzustellen. Zudem müssen u. a. Vorkehrungen getroffen werden, die erkennen lassen, ob eine Anwendung versehentlich geändert oder absichtlich manipuliert wurde.“ (7.9)

„Für die Anwendungsentwicklung sind **angemessene Prozesse** festzulegen, ...“
(7.6 Anforderung)



2017

Europa

Guidance on Cyber Security for Medical Devices

„Additional security testing can be done by using tools for secure code analysis and tools that **scan for open source code** and libraries used in the product, to identify components with known issues.“ (3.7)



2019

Europa

EU Secure Supply Chain for IoT

„The usage of third-party software introduces a degree of uncertainty that acts as a threat to the security of the supply chain. These **software components must be documented** as part of the supply chain security process... organizations should prefer those that have passed an evaluation and **certification process** ...“ (05-PRO)

“A **SBOM** describes the software components used as building blocks of any given product in an exhaustive fashion, including both open source and commercial packages or libraries” (13-PRO)



2020

Securing Open Source Software Act

“... for assessing the **risk of open source software components**, including direct and indirect **open source software dependencies**...” (6th page)



2021

Europa

Digital Operational Resilience Act: DORA

The digital operational resilience testing programme (...) shall provide (...) **the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses**, network security assessments, gap analyses, physical security reviews, questionnaires and **scanning software solutions, source code reviews** where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing. (Art. 25, 1)



2023

Deutschland

BSI SBOM-Anforderungen: TR-03183-2

„Eine SBOM sollte bei jedem Software-Ersteller und -Anbieter vorhanden sein, um Software-Komplexität transparent darstellen zu können und um zu wissen, welche Bestandteile (z. B. Bibliotheken) eingesetzt werden ...“



2023

Europa

EU Cyber Resilience Act: EU CRA

„... erforderlichen **Korrekturmaßnahmen ergriffen werden**, um die Konformität dieses Produkts mit digitalen Elementen oder den vom Hersteller eingerichteten Verfahren in Übereinstimmung zu bringen zu ergreifen oder das Produkt gegebenenfalls zurückzunehmen oder zurückzurufen.“(14.4)

„sollte **freie und quelloffene Software** die außerhalb einer kommerziellen Tätigkeit entwickelt oder bereitgestellt wird, **nicht unter diese Verordnung fallen**“ (Präambel Punkt 10)



tbd.

Chancen und Herausforderung durch Regulierung von OSS

Für die Open Source Community und Projekte

weniger finanzielle Unterstützung
der Wirtschaft, bzw.
Open Sourcing von Firmen



Haftungsrisiken



Zertifizierungsaufwände



größeres Vertrauen in
Open Source Software



mehr finanzielle Unterstützung
durch die öffentliche Hand



mehr Feedback
bei CVEs



neue Nutzende und Contributors
in der öffentlichen Verwaltung



Chancen und Herausforderung durch Regulierung von OSS *Für Staaten*

Verlust von Innovation
und neuen Technologien



Erschließung von Open
Source Technologien



Schwierigkeiten bei der
Durchsetzung im Internet



Digitale
Souveränität



Verlust von Software Know-how und
kollaborativer Weiterentwicklung



Erhöhung der Sicherheit und
Transparenz bei digitalen Produkten



Verwaltungsaufwände
und Bürokratie



Chancen und Herausforderung durch Regulierung von OSS *Für Unternehmen*

Erzwungene extra Aufwände für Compliance,
Security und Zertifizierungen



größere Transparenz
in der Lieferkette



Mehraufwände bei eigenen
Implementierungen



Haftungsrisiken



Neue Kundenfelder, zum Beispiel
in der öffentlichen Verwaltung,
Finanzsektor oder Medizin

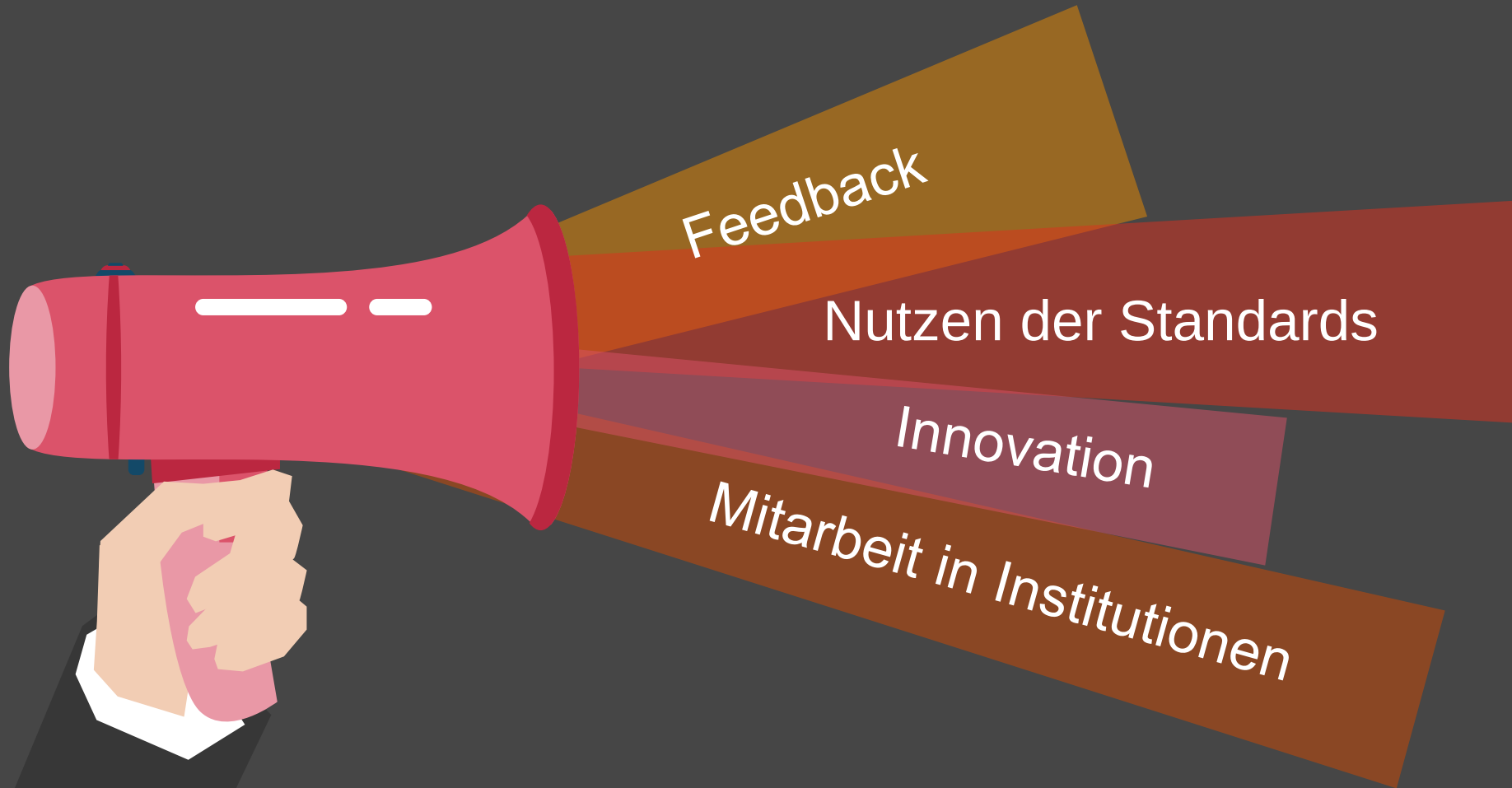


Schnelleres schließen
von Sicherheitslücken



Call for Action

„Be the lobby for the Open Source Community“



Please ask your questions or get in touch:



Julian Rau
OSS Expert
@ PwC Germany



+49 151 16584615



julian.rau@pwc.com

www.pwc.de/opensource

Enable digital future



Reduce risks

Consulting & Implementation

Audit & Certification

Managed Services