Lieferketten und SBOMs

Die neuen Maßstäbe für Open Source Integration

www.pwc.de/opensource

pwc

Julian Schauder
Manager, OSS Management Services

Moskauer Str. 19
40227 Düsseldorf, Germany

+49 211 981-4786
+49 160 96603979

julian.schauder@pwc.com

PricewaterhouseCoopers in Deutschland

PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft hat ihren Firmensitz in Frankfurt am Main

PwC ist in Deutschland mit mehr als 12.000 Mitarbeitenden und einem Umsatzvolumen von rund €2,4 Milliarden die führende Wirtschaftsprüfungs- und Beratungsgesellschaft. An 21 Standorten arbeiten Expert:innen für nationale und internationale Mandanten jeder Größe. PwC Deutschland bietet Dienstleistungen in den Bereichen Wirtschaftsprüfung und prüfungsnahe Dienstleistungen (Assurance), Steuerberatung (Tax) sowie in den Bereichen Consulting und Deals (Advisory). Eine hohe Qualitätsorientierung sowie vorausschauendes Denken und Handeln kennzeichnen die Aktivitäten des Unternehmens.

Wir stellen Prüfungs- und Beratungsservices für Unternehmen jeder Größe bereit. Stark ausgebaut wurde der Geschäftsbereich Mittelstand, der die Unternehmen mit einem dichten Kontaktnetzwerk direkt vor Ort betreut. Auch Unternehmen der öffentlichen Hand, Verbände, kommunale Träger und andere Organisationen vertrauen unserem Wissen und unserer langjährigen Erfahrung. Aus gutem Grund: rund 600 Partner:innen und mehr als 12.000 Expert:innen verfügen über umfassende Kenntnisse in allen wichtigen Branchen und bieten maßgeschneiderte Dienstleistungen aus einer Hand.

Standorte und Mitarbeiter:innen

	Standorte	Mitarbeiterinnen und Mitarbeiter
Weltweit	712	295.000
Europa	302	105.000
Deutschland	**21**	**12.000**

Our purpose is to build trust in society and solve important problems

Enable digital future & **Reduce risks**

Consulting & Implementation

Open Source Strategy and Enablement

Managed Services

OSPO as a Service

Audit & Certification

ISO 5230 Certifications and Supplier Audits

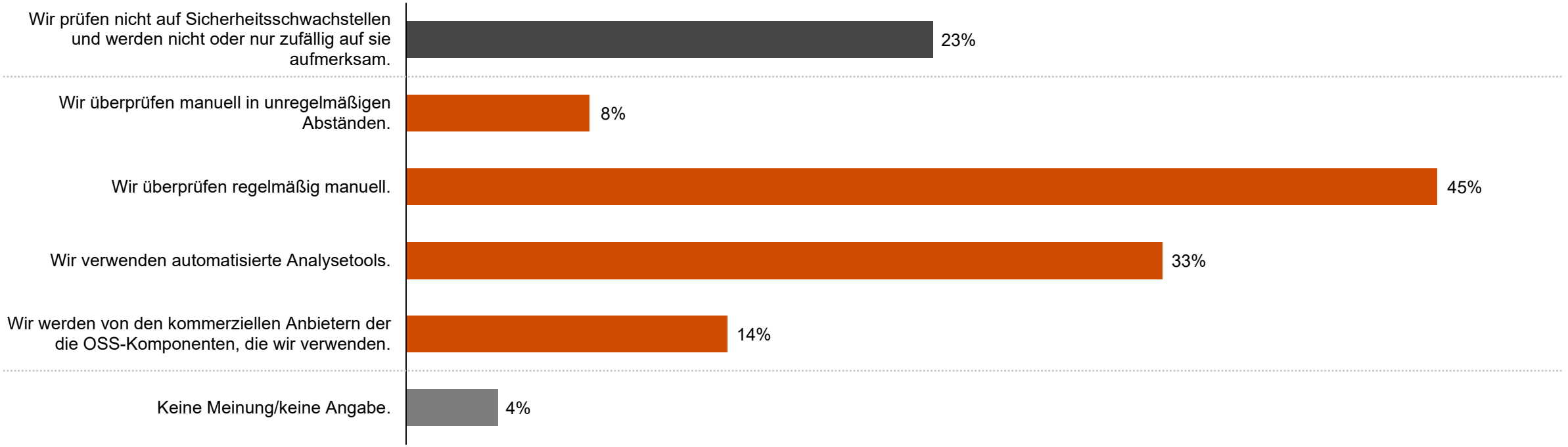
Wohin bewegen sich Markt und Regulierung?

Was ist das neue Maß und wie können wir uns vorbereiten?

OSS als ignoriertes Risiko?

Open Source Software Security Assessment

Welchen Ansatz verfolgen Sie in Ihrem Unternehmen, um die Sicherheit der von Ihnen verwendeten OSS-Komponenten zu überprüfen?



Stichprobe: Alle befragten Unternehmen mit mindestens 20 Mitarbeitern, die OSS einsetzen oder integrieren (n = 820); Mehrfachnennungen erlaubt; Quelle: Bitkom Forschung

Open Source has become more formal

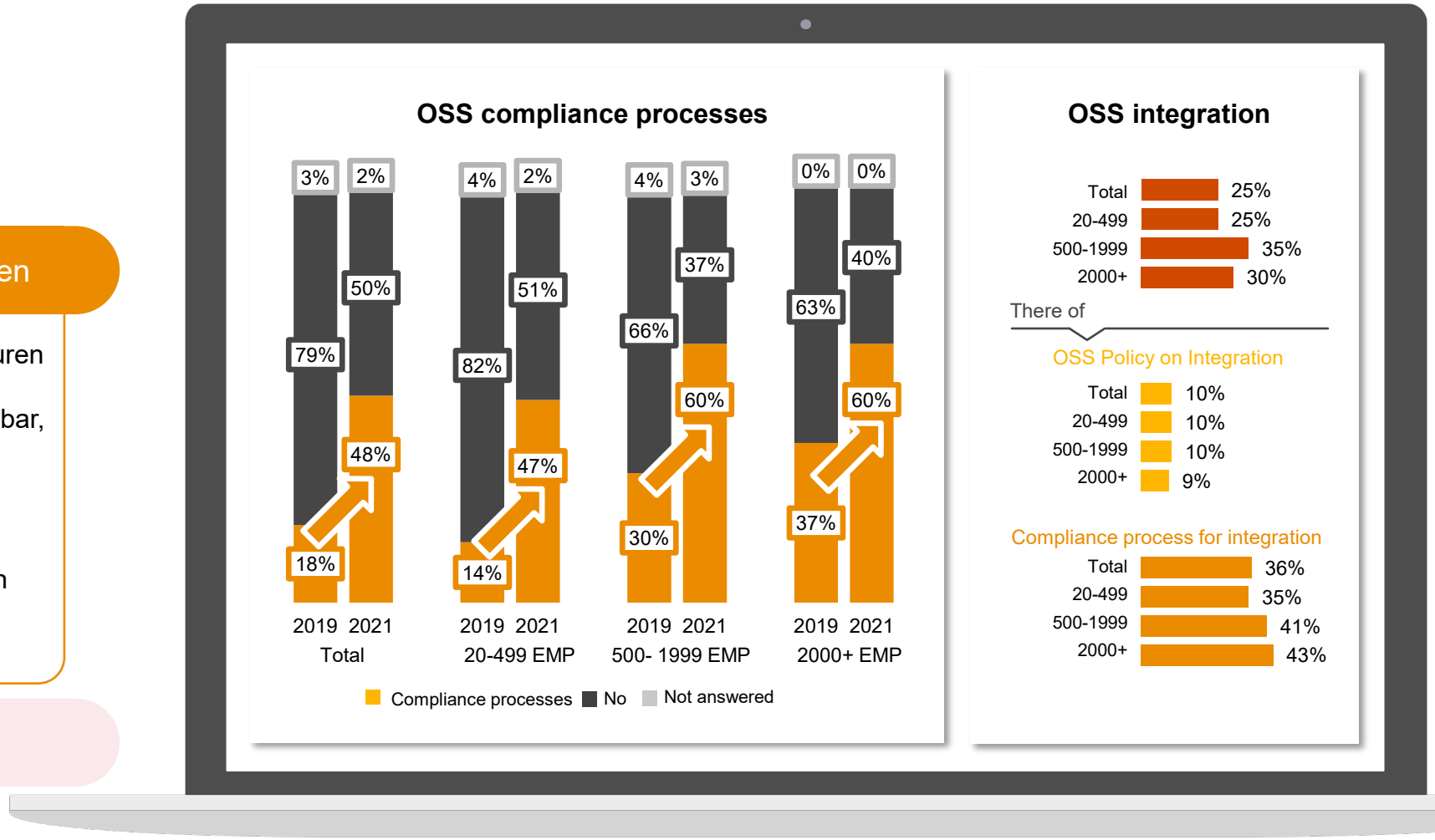
Two key findings from Bitkom Monitor ‘21 (1/2)

Positiver Trend bei Compliance-Strukturen

Ein deutlicher Anstieg der Compliance-Strukturen zur Kontrolle von OSS ist über alle Unternehmensgrößen hinweg deutlich erkennbar, besonders ausgeprägt bei KMU.

Allerdings besteht noch Handlungsbedarf bei Umfang und Gestaltung der Compliance-Prozesse, wie das Beispiel der Integration von OSS zeigt. Rund zwei Drittel integrieren OSS ohne zugehörige Compliance-Prozesse.

Der Mehrwert von ISO 5230



Open Source has become more formal

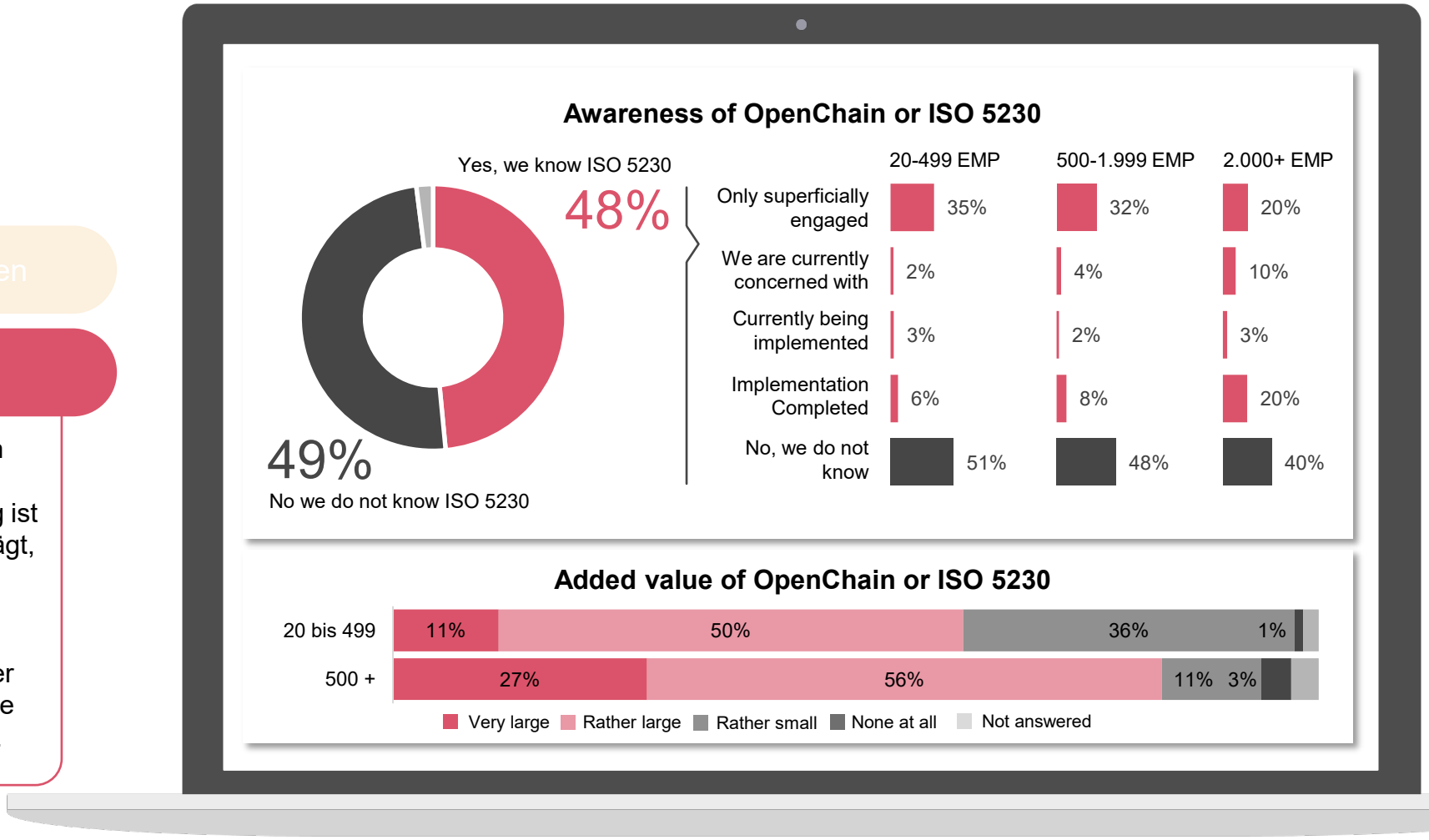
Two key findings from Bitkom Monitor ’21 (2/2)

Positiver Trend bei Compliance-Strukturen

Der Mehrwert von ISO 5230

Die große Mehrheit erkennt den Mehrwert von ISO 5230 als Standard für das OSS-Management. Der Bedarf an Standardisierung ist bei großen Unternehmen besonders ausgeprägt, so dass sie das Thema weiter vorantreiben werden.

Es ist davon auszugehen, dass alle Teilnehmer an Software-Lieferketten in absehbarer Zeit die Anforderungen von ISO 5230 erfüllen werden.



Herausforderungen für OSS

1. Sicherheitsproblemen

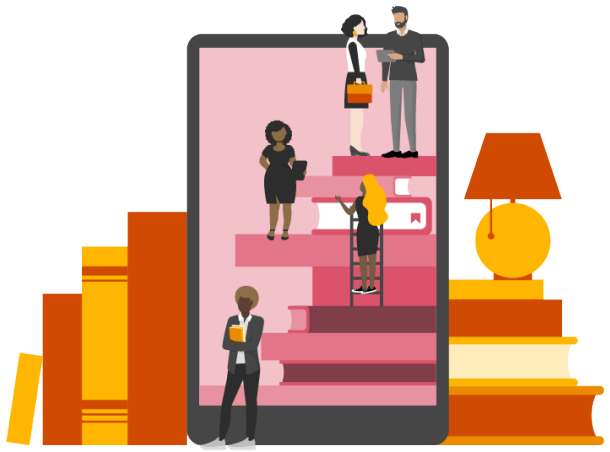
   z.B. CVE's, kompromittierte Pakete und Abhängigkeitsverwirrung

2. Rechtliche Probleme

   z.B. Komplexe rechtliche Verpflichtungen, Inkompatibilität, CopyLeft und Tivoization

3. Wartungsproblemen

   z. B. mangelnde Wartung von Paketen, fehlendes Know-how-Management oder Sponsoring



Was sagt ISO 5230?

OpenChain
Erhebt eine Bill of Materials

OpenChain
Reagiert auf die juristischen Implikationen

Security Assurance Specification
Reagiert auf die Security Implikationen

Executive Order 14028
Stellt dem Kunden eine SBOM bereit

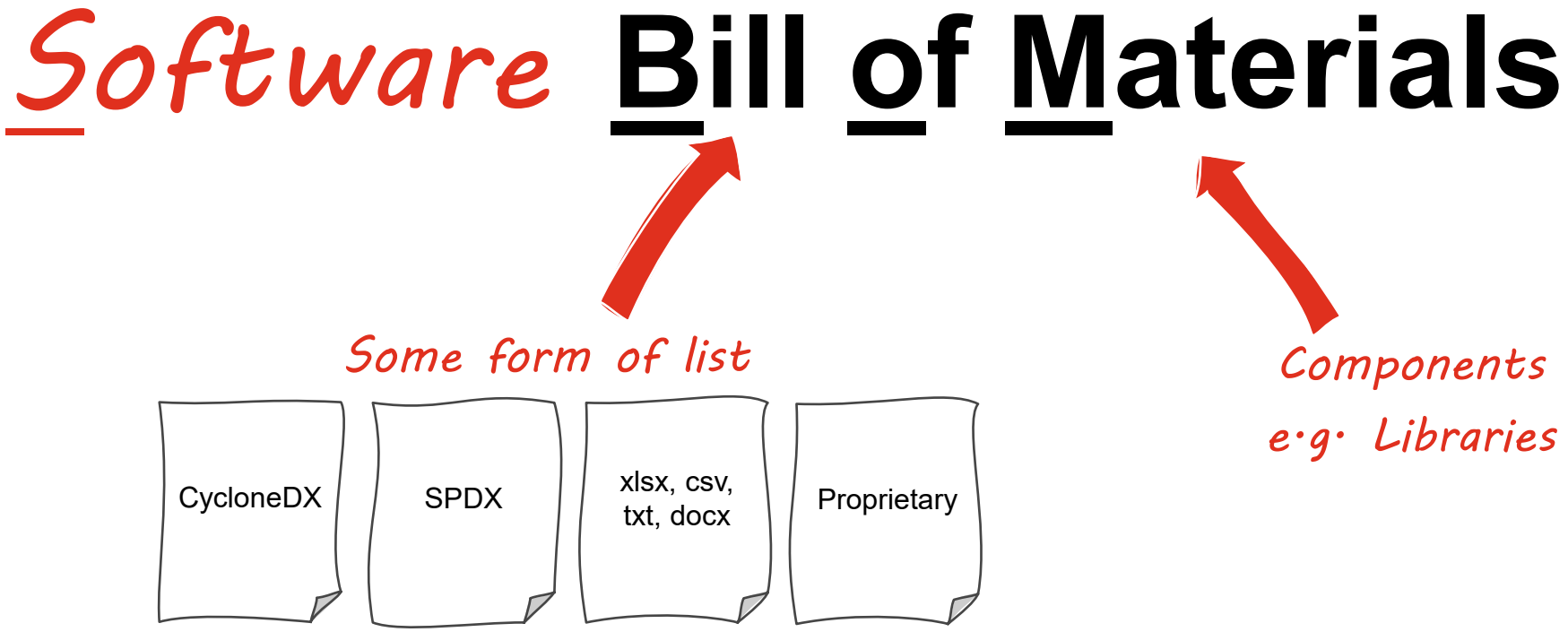
Grenze zwischen Unternehmen

OpenChain
Erhebt eine Bill of Materials

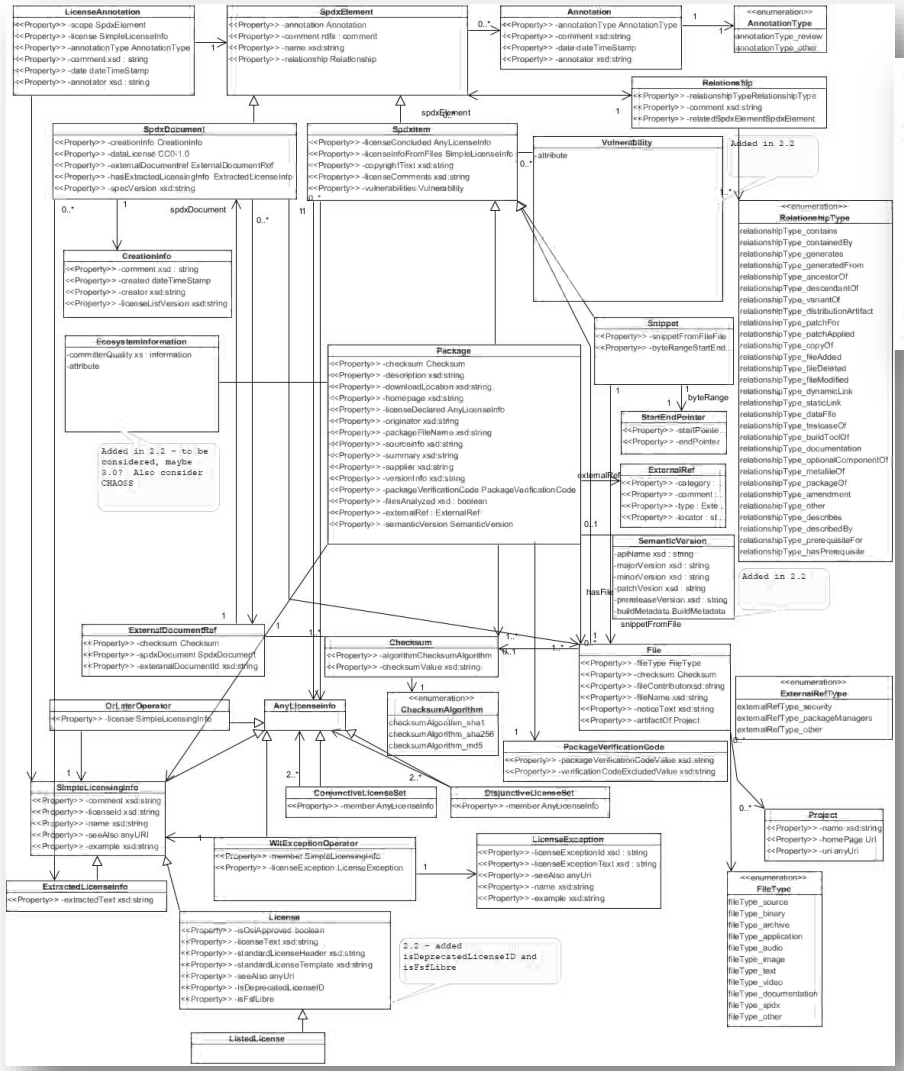
OpenChain
Reagiert auf die juristischen Implikationen

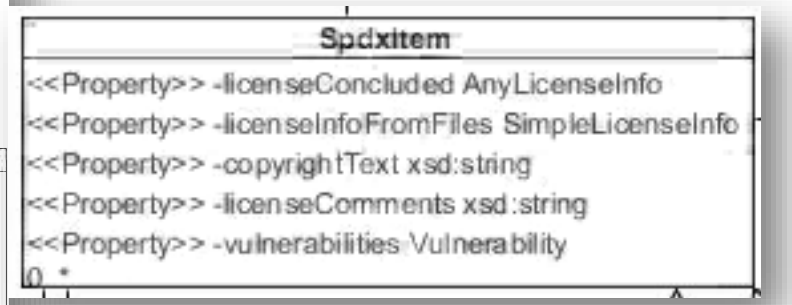
Security Assurance Specification
Reagiert auf die Security Implikationen

A recap – what are SBOMS?



It’s complicated





Materials

SPDX 2.2.2

https://spdx.github.io/spdx-spec/RDF-object-model-and-identifier-syntax/

It’s simple

Software **Bill of Materials**

NTIA Minimum Elements

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

Weitere Empfehlung:

- Component-Hash
- Lizenzinformationen
- …

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

The Model

External SBOMS

Know your Components

Source + Name + Version (PURL)

OSS Programme und Sondervereinbarungen

Manage your Components

Legal (e.g. via 5230)

All detectable Authors & Copyrights

All Relevant Licenses

Curation of Legal Information

Security

Package Origin / SLSA / Sigstore

CVEs

Deprecation

…

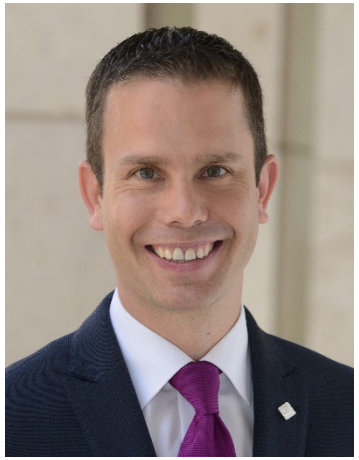
Reuse and Skill-Building

Upstream Support

To sum it up

- **Open Source Formalisierung findet Einzug.**
  Eine Orientiert am Kern von Open Chain bietet sich an.
- **Vollständig ist nur die Betrachtung aller Produkte.**
  Auch eingekaufter und weitergegebener Komponenten.
- **Minimum requirements SBOMS sollten erhoben und weitergegeben werden.**
  Bonus: Erweiterung der SBOMS für fachliche Probleme (legal, security,..).

Building Trust in Open Source Software
OSS Enablement, Certifications, and Managed Services



Marcel Scholze
Director, Head of OSS Management Services

Friedrich-Ebert-Anlage 35 - 37
60327 Frankfurt am Main, Germany

+49 69 9585-1746
+49 151 16157049

marcel.scholze@pwc.com

Julian Schauder
Manager, Technical Expert, OSS Management Services

Moskauer Str. 19
40227 Düsseldorf, Germany

+49 211 981-4786
+49 160 96603979

julian.schauder@pwc.com

www.pwc.de/opensource