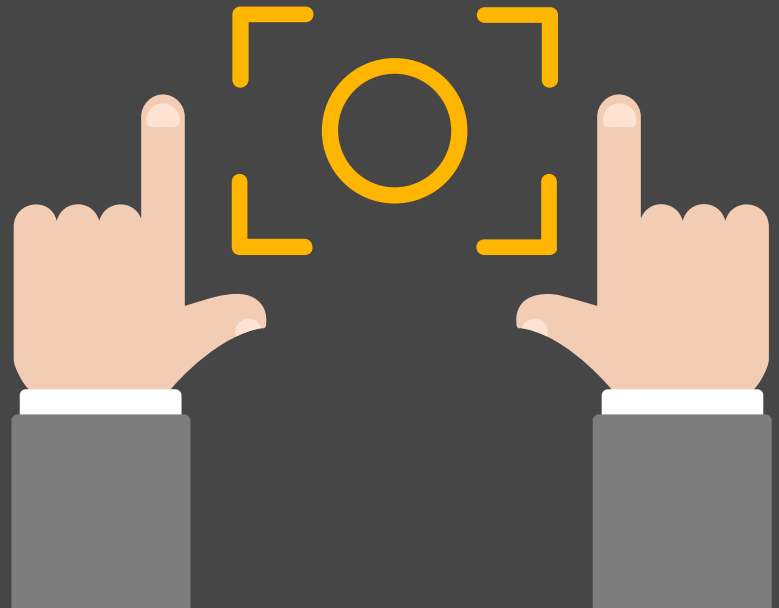
Open Source Management in der Regulatorik – Regelrecht genial oder geregelter Wahnsinn?

Katharina Grauf
BFOSS Erfurt, September 2024

Katharina Grauf
OSS-Expertin @ PwC Deutschland
+49 160 5526026
katharina.grauf@pwc.com

Agenda

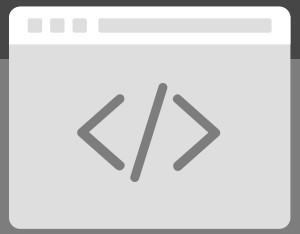
1. Relevanz von Open Source in der Regulatorik
2. Anforderungen an das OSS Management durch DORA und CRA
3. Einordnung und Umsetzungsempfehlungen



1 Relevanz von Open Source in der Regulatorik

Open Source Software Management

Operativ notwendig, regulatorisch gefordert



BSI-KritisV

BSI – Angriffserkennung durch Betreiber kritischer Infrastrukturen

BSI SBOM

BSI – Anforderungen an die Qualität von SBOMs

BAIT

BaFin – Aufsichtsrechtliche Anforderungen an die FS IT

Die Zahl kritischer Sicherheitsvorfälle steigt auch in OSS-Komponenten stetig

84%

der Codebasen enthalten **mind. eine Open Source-Schwachstelle** (2023).

Log4j (2021),
Sushiswap (2023)

45%

der Unternehmen werden bis 2025 **Angriffe auf die Software-Lieferkette** erfahren.

Solarwinds (2019),
XZ Utils (2024)

~ 50%

der Unternehmen in DE verfügen **nicht** über angemessene Werkzeuge für **OSS-Sicherheitsprüfungen***.

* Quelle: Aktuelle Zahlen für Deutschland laut Bitkom Monitor 2023: https://www.pwc.de/en/opensource/survey2023

Relevante Fragestellungen zum sicheren OSS Einsatz

Regulatorische Compliance fordert vollumfängliche Transparenz hinsichtlich des Einsatzes von OSS in eigenentwickelter sowie zugelieferter Software

Interne Verwendung von OSS

- Verfolgen Sie die Nutzung von Bibliotheken Dritter, einschließlich OSS?
- Verfügen Sie über Kontrollen zum Schutz der Integrität des Quellcodes von IKT-Systemen, die intern entwickelt werden?
- Verfügen Sie über angemessene Tools, um Quellcode zu überprüfen, bevor Sie ihn einsetzen?
- Sind sich Ihre Entwickler der OSS bewusst, z.B. durch eine OSS Policy und Schulungen?

Software von Third Party Providern

- Wissen Sie, wie Ihre Lieferanten OSS-Compliance und –Security managen?
- Liefern Ihre Lieferanten vollständige und korrekte SBOMs (Software Bills of Materials)?
- Sind Ihre Software-Lieferanten ISO 5230 / ISO 18974 zertifiziert?
- Verfügen Ihre Lieferanten über geeignete Tools zum Scannen von OSS?

2 Anforderungen an das OSS Management durch DORA und CRA

Digital Operational Resilience Act (DORA) – seit 16.01.2023 in Kraft

DORA definiert detaillierte und umfassende Vorschriften für digitale Betriebsstabilität auf EU-Ebene

- **Finanzunternehmen müssen bis zum 17.01.2025 nachweislich regelkonform sein**
- Sicherstellung, dass alle Arten von IKT-bezogenen Störungen rechtzeitig und angemessen mitigiert werden
- Überwachung und Prüfung von Finanzunternehmen und deren IKT-Drittanbieter
- Durch Regulatory und Implementing Technical Standards (**RTS/ITS**) werden bestimme Artikel in DORA weiter konkretisiert.

Darum geht es in DORA

IKT-Risikomanagement

IKT-bezogene Vorfälle

Testen der digitalen operationalen Resilienz

Management des IKT-Drittparteienrisikos

Informationsaustausch

IKT-Risikomanagement in DORA

OSS Policies und Prozesse als Bestandteil des IKT-Risikomanagementrahmens

- OSS Strategie
- OSS Richtlinien
- OSS Prozesse

IKT-Risikomanagement (Art. 5 bis 16)

Taktische, organisatorische und technische Fähigkeiten im Bereich der Cybersicherheit

Artikel 6, 2.

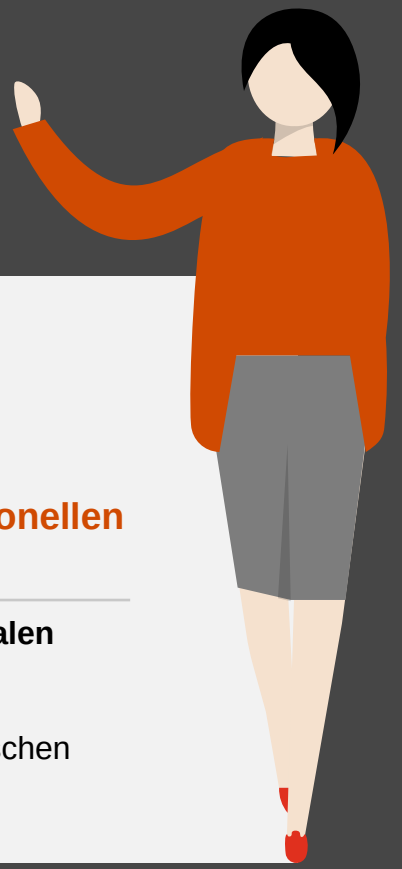
Der **Rahmen für das IKT-Risikomanagement** umfasst zumindest **Strategien, Richtlinien, Verfahren, IKT-Protokolle und Instrumente**, die erforderlich sind, um alle Informationswerte und IKT-Vermögenswerte, einschließlich **Computersoftware**, (...) ordnungsgemäß und **angemessen zu schützen**, um sicherzustellen, dass alle Informationswerte und IKT-Vermögenswerte angemessen vor Risiken, einschließlich Schäden und unbefugtem Zugriff oder unbefugter Nutzung, geschützt sind.

IKT-bezogene Vorfälle und Testing in DORA

- OSS Tooling
- OSS Code Analyse

Artikel 25, 1.

Das **Testprogramm für die digitale operationelle Resilienz** (...) sieht die Durchführung geeigneter Tests vor, wie z. B. **Bewertungen von Schwachstellen** und **Scans, Open Source-Analysen**, Bewertungen der Netzwerksicherheit, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und **Scans von Softwarelösungen, Überprüfungen des Quellcodes**, wo dies möglich ist, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests.



IKT-bezogene Vorfälle (Art. 17 bis 23)

IKT-bezogene Vorfälle
Erkennung, Meldung und Behandlung von ICT-bezogenen Vorfällen

Tests der digitalen operationellen Resilienz (Art. 24 bis 27)

Testen der digitalen operationalen Resilienz
Regelmäßige Tests von Ausfall-sicherheitsmaßnahmen und kritischen Systemen

DORA Schwerpunkte und zugehörige RTS/ITS

- OSS Scanning
- OSS Security Analyse

Artikel 10, 2. (d)

Verfahren für das **Schwachstellenmanagement** müssen (…):

die Verfolgung der **Nutzung von Bibliotheken Dritter** ermöglichen, einschließlich **Open Source**, die von IKT-Diensten verwendet werden, die kritische oder wichtige Funktionen von IKT-Diensten unterstützen (…).

Das **Finanzinstitut überwacht,** gegebenenfalls **in Zusammenarbeit mit dem IKT-Drittdienstleister**, die Version und mögliche Aktualisierungen der **Bibliotheken Dritter.**

Artikel 16, 2.

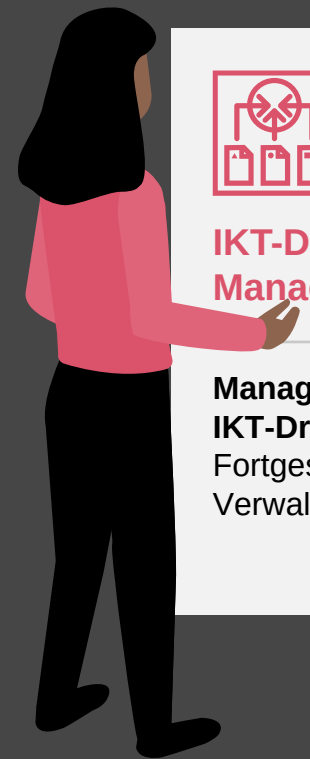
Die Finanzunternehmen entwickeln, dokumentieren und implementieren ein **Verfahren für die Beschaffung, Entwicklung und Wartung von IKT-Systemen** (...):

(...) führen **Quellcodeüberprüfungen** durch (...)

(...) **analysieren Schwachstellen** und **Anomalien im Quellcode** (...)

(...) führen Kontrollen zum Schutz der **Integrität des Quellcodes** von IKT-Systemen ein

(…) die Anforderung, dass proprietäre Software und, soweit machbar, **der Quellcode** (...)**, der von IKT-Drittanbietern bereitgestellt wird** oder **aus Open Source-Projekten** stammt, **vor ihrem Einsatz analysiert** und **getestet werden muss** (...)



IKT-Drittparteirisiko-Management (Art. 28 bis 44)

Management des IKT-Drittparteienrisikos
Fortgeschrittene Überwachung und Verwaltung von Drittparteirisiken

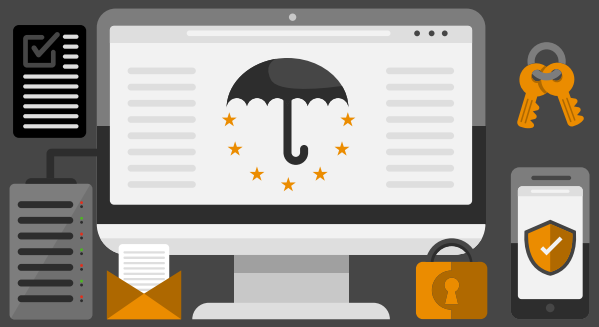
CRA-Anforderungen an das Risikomanagement von OSS

Vorherige CRA-Fassungen: unklar, inwiefern OSS-Projekte und die Community für OSS Security verantwortlich sind

CRA Update: Gesamtprodukt einschl. OSS-Komponenten müssen Mindestsicherheitsanforderungen der CRA erfüllen
→ **Hersteller** sind für die **Sicherheit** des Gesamtprodukts **verantwortlich** und müssen daher **OSS managen**

2023 **2024**

Zentrale Anforderungen der CRA an das Management von OSS:



- ✓ **Software-Stückliste** (SBOM) inkl. Open Source-Abhängigkeiten
- ✓ **OSS-Schwachstellen** Überwachung & Berichterstattung
- ✓ **Contribution** von **Security Fixes**

erfordert **Transparenz** bzgl. verwendeter OSS in Eigenentwicklungen **und** OSS in zugelieferter Software

Rahmenbedingungen für den sicheren Einsatz von OSS notwendig

CRA-Anforderungen an das Risikomanagement von OSS

- OSS Scanning
- SBOM Erstellung

Software Bill of Material (SBOM)

Die **Erstellung einer Software Bill of Material (SBOM)**, welche die verwendeten OSS Abhängigkeiten im digitalen Produkt abbildet

Annex 1, Teil II (1):

Die Hersteller von Produkten mit digitalen Elementen müssen

(1) **Schwachstellen** und Komponenten der Produkte mit digitalen Elementen **ermitteln** und **dokumentieren**, u. a. **durch Erstellung einer Software-Stückliste** in einem gängigen maschinenlesbaren Format, aus der zumindest die obersten Abhängigkeiten der Produkte hervorgehen;

www.pwc.de/en/opensource

CRA-Anforderungen an das Risikomanagement von OSS

Kapitel II, Art. 13 (5)

Für die Zwecke der Erfüllung der in Absatz 1 festgelegten Pflicht lassen die Hersteller die **gebotene Sorgfalt** walten, wenn sie **von Dritten bezogene Komponenten** in ihre Produkte mit digitalen Elementen integrieren, sodass solche Komponenten die Cybersicherheit des Produkts mit digitalen Elementen nicht beeinträchtigen, **auch nicht bei der Integration von freier und quelloffener Software**, die nicht im Rahmen einer Geschäftstätigkeit auf dem Markt bereitgestellt wurde.

Kapitel II, Art. 13 (6)

Sobald der Hersteller eine **Schwachstelle** in einer in das Produkt mit digitalen Elementen integrierten Komponente, einschließlich **einer quelloffenen Komponente**, feststellt, **meldet er die Schwachstelle der Person oder Einrichtung**, die diese Komponente herstellt oder wartet (…). Haben Hersteller eine Software- oder Hardware Änderung entwickelt, um die Schwachstelle in dieser Komponente zu beheben, **teilen sie den betreffenden Code** oder die einschlägigen Unterlagen der Person oder Stelle, die die Komponente herstellt oder wartet, gegebenenfalls in einem maschinenlesbaren Format mit.

- OSS Security Prozesse

Fortlaufende Überwachung der eingesetzten OSS hinsichtlich bekannter Schwachstellen

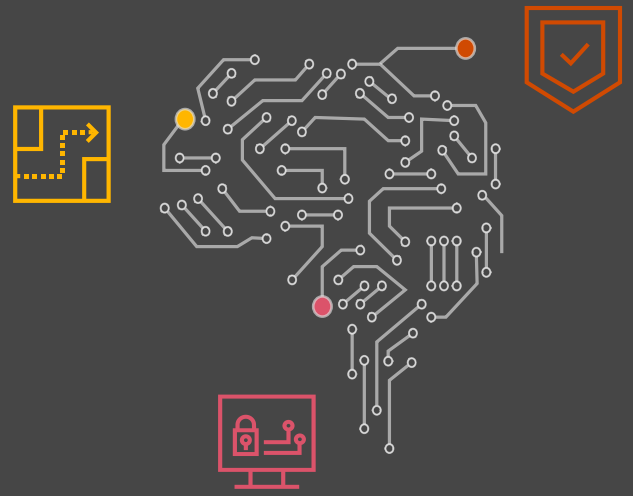
Mitteilung von Schwachstellen und **Kontribution** von Security Fixes an Hersteller

3 Einordnung & Umsetzungsempfehlungen

Synergien der Regulatorik (CRA & DORA) mit dem ISO Standard für OSS Security Management

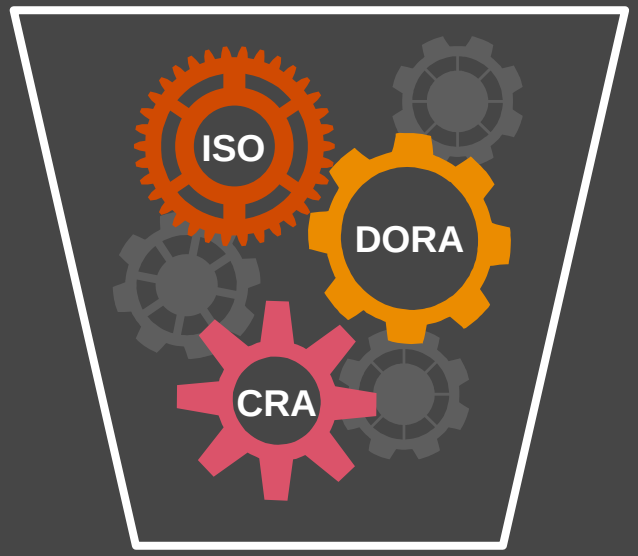
1. **Betroffenheitsanalyse**
→ Produkte und Supplier im Scope definieren

2. **DORA / CRA-Gap Assessment** zur Identifikation von Handlungsfeldern und Querschnittsthemen



Transparenz im OSS Einsatz ist der notwendige Grundstein zur erfolgreichen und effizienten Implementierung von OSS Management Praktiken.

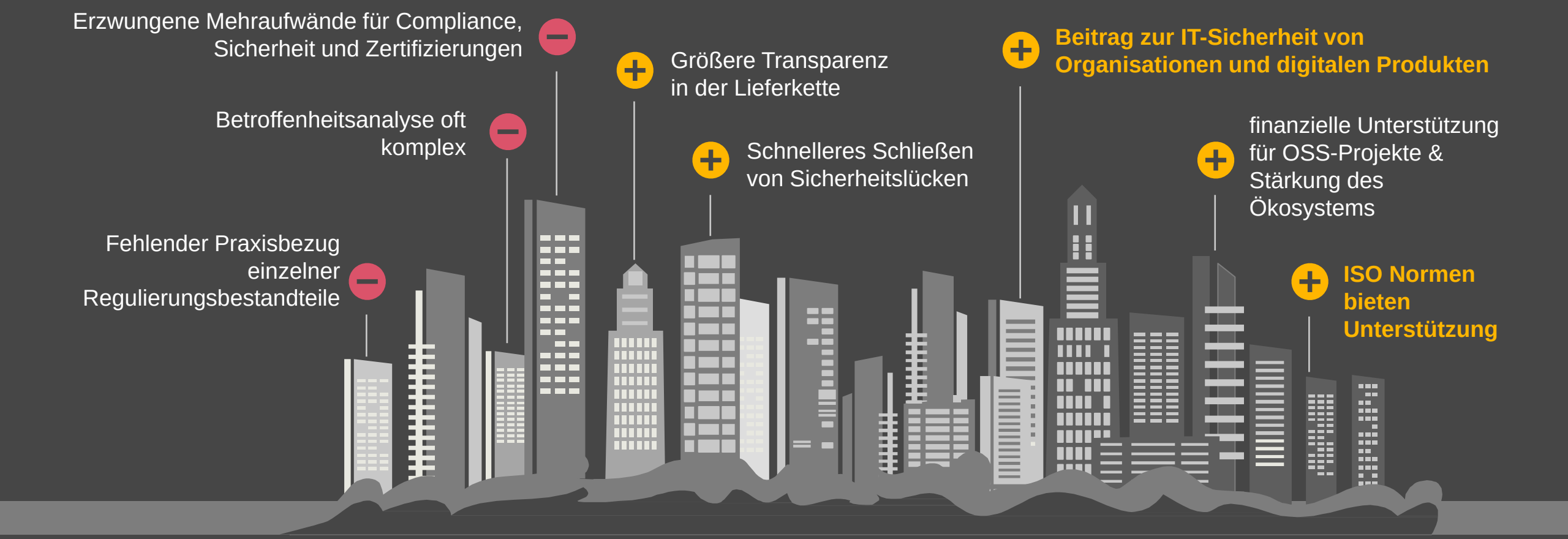
Dies umfasst die eigene Anwendungsentwicklung sowie zugelieferte Software. Ein professionelles **Supplier Management** ist wichtige Basis.



Die **ISO 18974** liefert ein Rahmenwerk zur Implementierung zielgerichteter Konformitätsmaßnahmen für DORA und CRA Compliance.

Professionelles OSS Management mit SBOMs trägt essentiell zur digitalen Resilienz von Organisationen bei

OSS in der Regulatorik
– geregelt, aber noch nicht genial



Ich freue mich auf Ihre Fragen und Kontaktaufnahme

Katharina Grauf
OSS-Expertin @ PwC Deutschland
+49 160 5526026
katharina.grauf@pwc.com

www.pwc.de/opensource

Enable digital future & mitigate risks

Beratung & Implementierung | Audit & Zertifizierung | Managed Services