Supply-Chain Security in der Softwareentwicklung

Management von Open-Source-Komponenten in der Praxis

Dr. Anatoli Kalysch

27. Juni 2025

5. Semester DIS
HAW Ansbach

whoami

- Science
  - Associated Postdoc @ FAU (Focus: Mobile Security, IT-Forensics, Reverse Engineering)
  - Lecturer (Fokus: Mobile Application Security, Cyber Security)
  - Conference reviewer (Fokus: Mobile Security, Malware Analysis, Reverse Engineering)
- Industry
  - Penetration tester (Fokus: Mobile & Backend Pentesting for Fintech & Insurance)
  - Co-Founder @ TALOS Insights GbR (Fokus: NLP, Serverless, IP & Competitive Intelligence)
  - Senior Information Security Officer & deputy @ CSO Taurus SA (Fokus: GRC, Incident Response & TPRM)
  - Chief Information Security Officer @ DB Connect GmbH (Fokus: GRC, TPRM & Vulnerability Research)

01 **Lernziele**
Des heutigen Fachvortrags

02 **Definition und Kontext**
Supply-Was?

03 **Problemstellungen**
Was macht die Absicherung von Supply-Chains komplex?

Supply-Chain Security

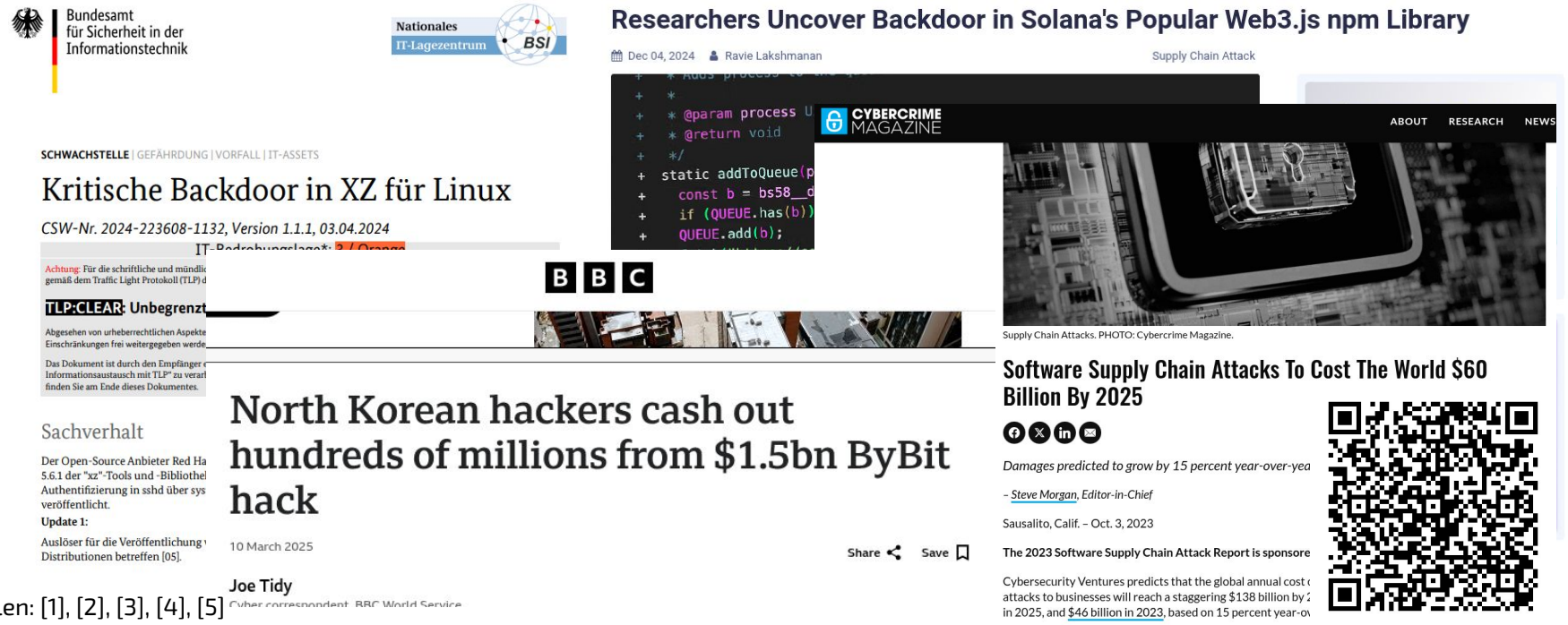
04 **Heutiges SOTA**
Ausgesuchte Ansätze zur Risikobehandlung

05 **Fazit und Quellen**
Offene Diskussion und Fragen

Was schauen wir genauer an?

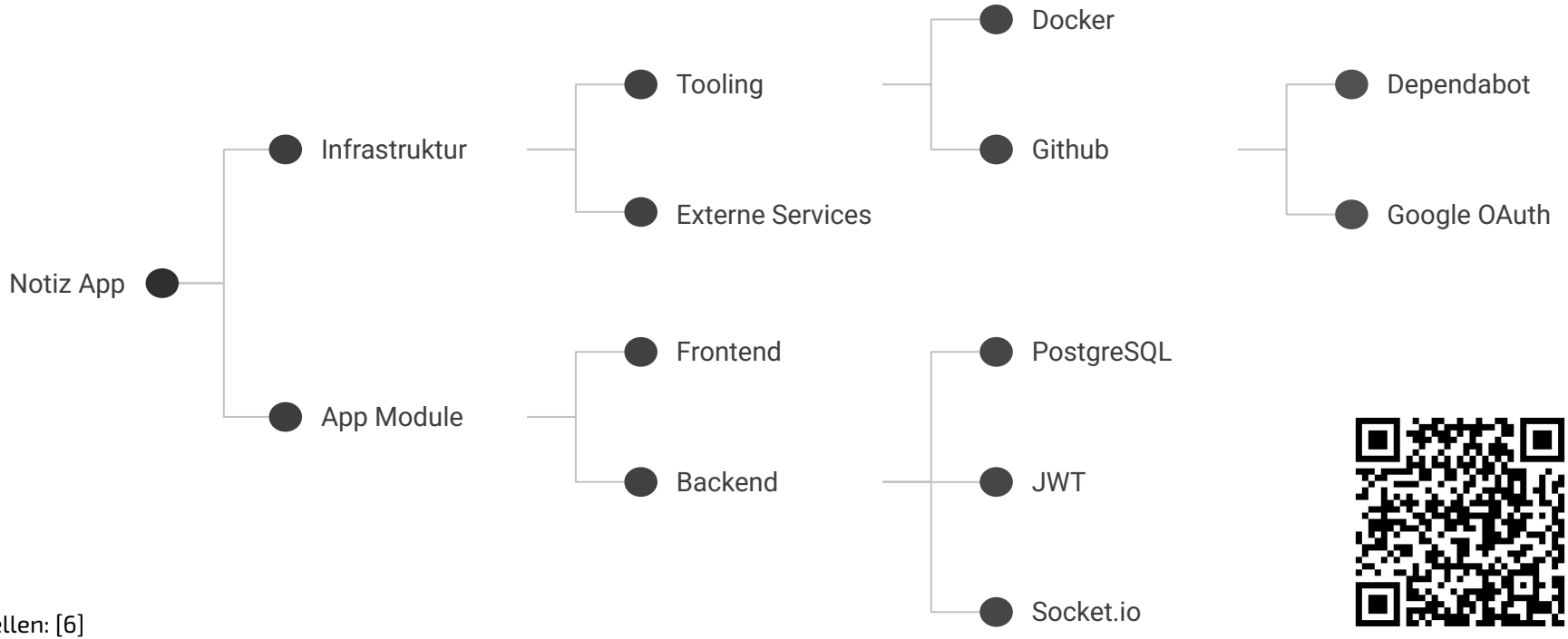
- Begriffe und Relevanz einordnen
  - Was ist eine Lieferkette im Softwarebereich?
  - Warum ist Open-Source schwierig?
- Risiken und Schutzmaßnahmen verstehen
  - Kann ich Lieferketten trotzdem absichern?
  - Wie binde ich Schutzmaßnahmen in meine Softwareprozesse ein?
- Praxisrelevanz (Rechtliche Grundlagen, (S)SDLC, Risikomanagement und Lieferantenbewertung)

Software Supply-Chain - Praktische Relevanz?



Quellen: [1], [2], [3], [4], [5]

Software Supply-Chain - Definition (für heute)



Quellen: [6]

Grenzfälle unserer Definition

- Wo ziehen wir die Grenze?
  - Hardwarekomponenten / Chipsysteme? Treiber? Kernelkomponenten?
  - Wie tief möchte ich gehen? T1 / T2 / welche Rekursionstiefe der Betrachtung?
  - NIST: '[...] a collection of steps that create, transform, and assess the quality and policy conformance of software artifacts[...]'. [7]
- Welche Dimensionen sollten wir zusätzlich betrachten?
  - Menschlicher Faktor? KI-Faktor? Generierung von Code relevant?
  - Manipulation der Zwischenergebnisse in das Bedrohungsmodell einschließen, sog. Artefakte?
- Bedrohungsmodell muss an das Unternehmen angepasst werden! -> **RM / BIA**

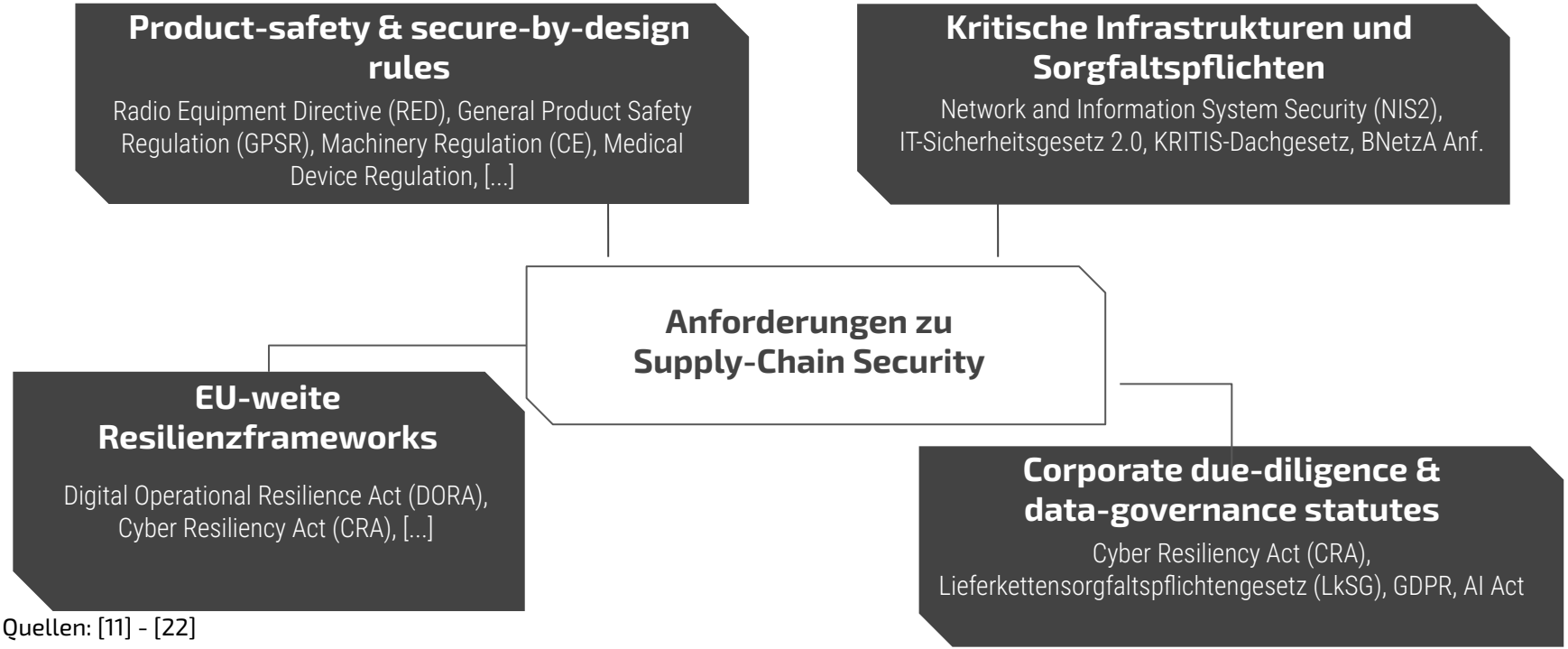
Quellen: [7], [8], [9]

Open-Source - Fluch oder Segen?

- Risikoreich
  - Unbekannt: Autoren, Unterstützung (intern & extern)
  - Lizenzmodell? KI-Anteil? Bereits gescannt auf Schwachstellen und alte Abhängigkeiten?
- Was ist die Alternative
  - Budget / Zeitrahmen für Alternative?
  - Business Cases schwierig
- Fazit: Open-Source Umgang muss gelernt werden
  - Sie werden nicht den Open-Source Korpus neu coden

Quellen: [10]

Gesetzeslage zu Supply-Chain Security



Quellen: [11] - [22]

Wie bekomme ich das alles unter einen Hut?

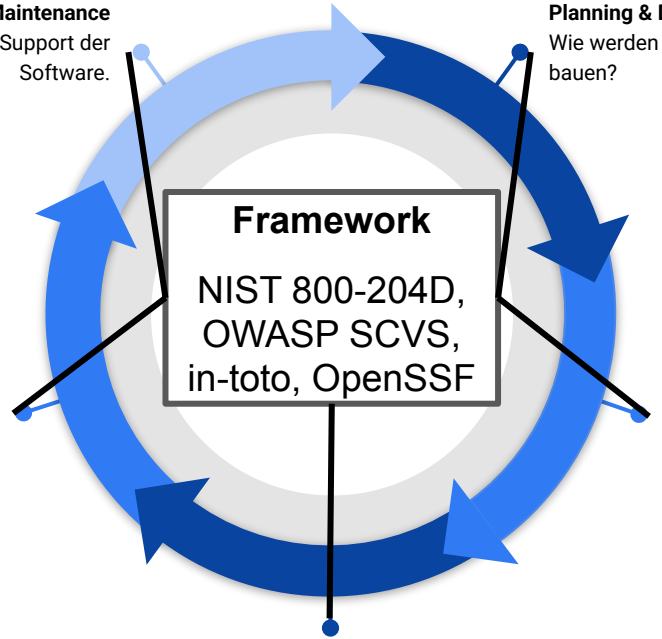
- Governance
  - Anforderungen kennen
  - Gap-Analyse zum IST-Stand
- Quality Gates in der Entwicklung (UND AKQUISE / VALIDIERUNG von Open-Source)
  - Menschlicher Faktor? KI-Faktor? Generierung von Code relevant?
  - Manipulation der Zwischenergebnisse in das Bedrohungsmodell einschließen, sog. Artefakte?
- **Weder fängt Supply-Chain Sicherheit an Ihren Unternehmensgrenzen an, noch endet sie dort.**

Quellen: [7], [9]

Securing the Software Development Life Cycle

Vulnerability Management, Pentesting

Patch- und Configuration-management, SLSA Artifacts



Maintenance
Update und Support der Software.

Planning & Design
Wie werden wir die Software bauen?

Deployment
Software wurde nach der Spezifikation erstellt.

Implement
Schreiben und Bauen der Software.

Testing & Integration
Quality Assurance und Integration der Ergebnisse.

SCA, SBOM, Peer Review, SAST

Build Toolchain, Hardening, Version Pinning, SAST + DAST

Quellen: [7]. [8]. [23]

VIELEN DANK!

Fragen? Anmerkungen?

anatoli@kalysch.com

Literatur

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI). 2024. *Kritische Backdoor in XZ für Linux* (CSW-Nr. 2024-223608-1032, Version 1.1.1). Technical Report, 4 pp. BSI, Bonn, Germany (3 Apr. 2024). Retrieved 25 June 2025 from https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2024/2024-223608-1032.pdf.

[2] Marc Ohm, Henrik Plate, Arnold Sykosch, and Michael Meier. 2020. *Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks*. In *Proc. 17th Conf. on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA 2020)*, LNCS 12224. Springer, 23-43. DOI:https://doi.org/10.48550/arXiv.2005.09535.

[3] Steve Morgan. 2023. *Software Supply Chain Attacks to Cost the World $60 Billion by 2025*. Cybersecurity Ventures (3 Oct. 2023). Retrieved 25 June 2025 from https://cybersecurityventures.com/software-supply-chain-attacks-to-cost-the-world-60-billion-by-2025/.

[4] BBC News. 2025. *North Korean Hackers Cash Out Hundreds of Millions from $1.5 Billion ByBit Hack* (9 Mar. 2025). Retrieved 25 June 2025 from https://www.bbc.com/news/articles/c2kgndwwd7lo.

[5] Sean Cordey. 2023. *Software Supply Chain Attacks: An Illustrated Typological Review*. CSS Risk & Resilience Report 2023-01. Center for Security Studies (CSS), ETH Zürich, Switzerland, 50 pp. DOI:https://doi.org/10.3929/ethz-b-000584947.
https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2023-01-Software-Supply-Chain-Attacks.pdf

[6] Anatoli Kalysch. 2025. *online_notiz_template* (GitHub repository). Version *main*, MIT License. Retrieved 25 June 2025 from https://github.com/anatolikalysch/online_notiz_template.

[7] Ramaswamy Chandramouli, Frederick Kautz, and Santiago Torres-Arias. 2024. *Strategies for the Integration of Software Supply Chain Security in DevSecOps CI/CD Pipelines*. NIST Special Publication 800-204D. National Institute of Standards and Technology, Gaithersburg, MD, USA. DOI:https://doi.org/10.6028/NIST.SP.800-204D.

Literatur

[8] OpenSSF. 2025. *SLSA – Supply-chain Levels for Software Artifacts*. https://slsa.dev/ (accessed 25 June 2025).

[9] Mahzabin Tamanna, Sivana Hamer, Mindy Tran, Sascha Fahl, Yasemin Acar, and Laurie Williams. 2025. *Unraveling Challenges with Supply-Chain Levels for Software Artifacts (SLSA) for Securing the Software Supply Chain*. SSRN pre-print. DOI:https://doi.org/10.2139/ssrn.5119626 .

[10] Thomas Dohmke, Marco Iansiti, and Greg Richards. 2023. *Sea Change in Software Development: Economic and Productivity Analysis of the AI-Powered Developer Lifecycle*. arXiv pre-print arXiv:2306.15033 (26 Jun. 2023). DOI:https://doi.org/10.48550/arXiv.2306.15033 .

[11] European Parliament and Council. 2014. Directive 2014/53/EU of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment (Radio Equipment Directive). OJ L 153 (22 May 2014), 62-106. Retrieved 25 June 2025 from https://eur-lex.europa.eu/eli/dir/2014/53/oj .

[12] European Parliament and Council. 2017. Annex I – General Safety and Performance Requirements. In Regulation (EU) 2017/745 on medical devices, OJ L 117 (5 May 2017), 100-173. Consolidated text consulted 25 June 2025 at https://www.medical-device-regulation.eu/2019/07/23/annex-i-general-safety-and-performance-requirements/ .

[13] European Commission. 2025. EU's General Product Safety Regulation (GPSR): A New Era of Consumer Protection. Access2Markets News, 6 Jan 2025. Retrieved 25 June 2025 from https://trade.ec.europa.eu/access-to-markets/en/news/eus-general-product-safety-regulation-gpsr-new-era-consumer-protection .

[14] European Parliament and Council. 2022. Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). OJ L 333 (27 Dec 2022), 80-152. Retrieved 25 June 2025 from https://eur-lex.europa.eu/eli/dir/2022/2555/oj .

[15] Bundesamt für Sicherheit in der Informationstechnik (BSI). 2021. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). Web article, 7 May 2021. Accessed 25 June 2025.

Literatur

[16] Bundesministerium des Innern und für Heimat (BMI). 2024. Bundeskabinett beschließt KRITIS-Dachgesetz – Gesetz zum Schutz kritischer Anlagen. Press release, 5 Dec 2024. Retrieved 25 June 2025 from https://www.bmi.bund.de/ .

[17] Bundesnetzagentur. 2025. Bundesnetzagentur – Official Website. Accessed 25 June 2025 at https://www.bundesnetzagentur.de .

[18] European Insurance and Occupational Pensions Authority (EIOPA). 2025. Digital Operational Resilience Act (DORA). Web page, updated 17 Jan 2025. Retrieved 25 June 2025 from https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en .

[19] European Commission. 2025. Cyber Resilience Act – Policy Page. Last updated 6 Mar 2025. Retrieved 25 June 2025 from https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act .

[20] Bundesministerium für Arbeit und Soziales (BMAS). 2023. Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten (Lieferkettensorgfaltspflichtengesetz – LkSG). Entered into force 1 Jan 2023. Accessed 25 June 2025 at https://www.csr-in-deutschland.de/…/gesetz-ueber-die-unternehmerischen-sorgfaltspflichten-in-lieferketten.html .

[21] European Parliament and Council. 2016. Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR). OJ L 119 (4 May 2016), 1-88. Consolidated text retrieved 25 June 2025 from https://gdpr-info.eu/ .

[22] European Parliament and Council. 2024. Regulation (EU) 2024/1689 – Artificial Intelligence Act. OJ (12 July 2024). Retrieved 25 June 2025 from https://artificialintelligenceact.eu/the-act/ .

[23] OWASP Foundation. 2025. Software Supply Chain Security Cheat Sheet. OWASP Cheat Sheet Series, version 2025-06. Retrieved 25 June 2025 from https://cheatsheetseries.owasp.org/cheatsheets/Software_Supply_Chain_Security_Cheat_Sheet.html .

Organisatorische Aspekte der Supply-Chain Security in der Praxis

Kategorie	Beschreibung
Open-Source	Umgang mit Lizenzen, KI-Code, unbekannte Entwickler, Vertrauen.
Validierung	Was, von wem und mit welchen Prozessen muss freigegeben werden, welche Ausnahmen bestehen?
Gesetzeslage	Weltweit erst in der Mache, Umgang mit Lieferantenbewertungen? Quality-Gates erfassen Open-Source Code?
Datenschutz	Verantwortlichkeiten; Datenminimierung / Anonymisierung? Logs?
Quality Gates	Standardisierung von Formaten, Schnittstellen, IoCs.