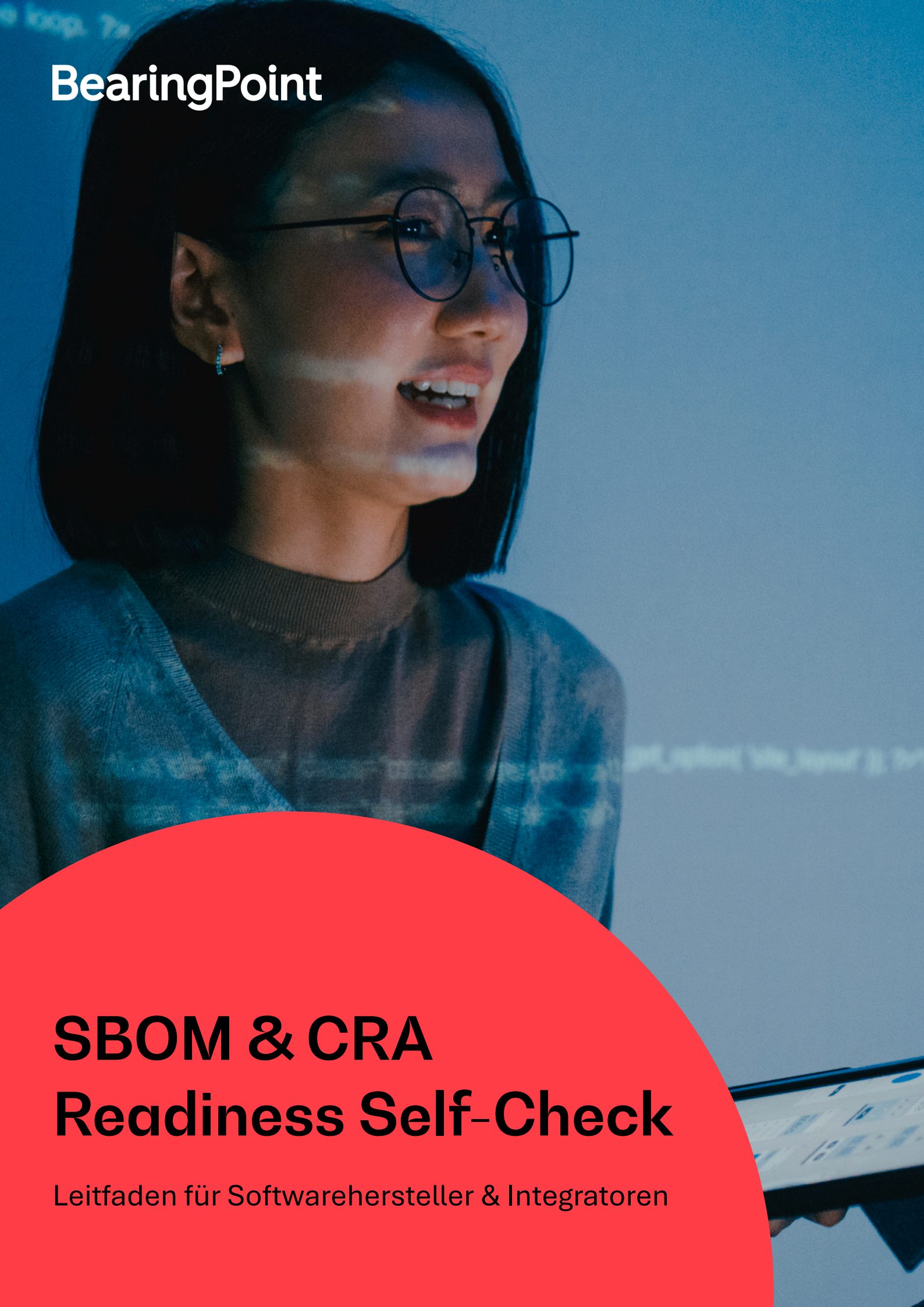
BearingPoint



SBOM & CRA Readiness Self-Check

Leitfaden für Softwarehersteller & Integratoren

Sind Ihre Softwareprodukte bereit für SBOM-Anforderungen und den EU Cyber Resilience Act (CRA)?

Unternehmen, die früh investieren, verwandeln regulatorischen Druck in einen Wettbewerbsvorteil. Angesichts der Lifecycle-Security- und Rechenschaftsanforderungen des CRA wird SBOM-Management zur Grundlage für Security by Design – nicht nur zu einem Compliance-Häkchen. Diese kurze Checkliste hilft Ihnen, Lücken schnell zu identifizieren, und zeigt, wie BearingPoint Sie unterstützen kann.

SBOM-Grundlagen

- ☐ Können Sie für jede veröffentlichte Produktversion eine SBOM erstellen?
- ☐ Enthält sie direkte & transitive Abhängigkeiten (Open Source und Third-Party)?
- ☐ Enthält sie eingebettete Snippets oder wiederverwendeten Quellcode?
- ☐ Ist die SBOM versioniert und einem bestimmten Produkt-Release oder Build zuordenbar?

Schwachstellen & Sicherheit (CRA-relevant)

- ☐ Werden SBOM-Komponenten kontinuierlich auf neue Schwachstellen überwacht?
- ☐ Können Sie Probleme von Komponente → Produkt → Behebung nachverfolgen?
- ☐ Haben Sie einen definierten Prozess für Schwachstellen-Offenlegung und Kundenbenachrichtigung?

Open-Source-Lizenz-Compliance

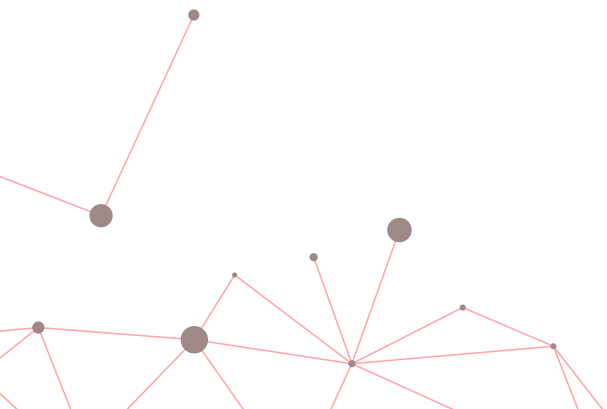
- ☐ Sind alle Lizenzen in Ihrer SBOM klar identifiziert?
- ☐ Kennen und erfüllen Sie die Lizenzverpflichtungen?
- ☐ Können Sie Lizenzdokumentation (Texte, Copyrights, Attributionen) für die Distribution erstellen?
- ☐ Werden Lizenzrisiken vor dem Release erfasst und minimiert?
- ☐ Gibt es eine definierte OSS-Richtlinie und einen Freigabeprozess?
- ☐ Sind Entwickler in OSS-Nutzung und Lizenzregeln geschult?

CRA Readiness

- [ ] Wissen Sie, welche Ihrer Produkte unter den CRA fallen?
- [ ] Können Sie Nachweise erbringen für:
  - [ ] SBOMs
  - [ ] Schwachstellenmanagement
  - [ ] Secure-by-Design-Praktiken
- [ ] Sind Sie auf Kunden-Due-Diligence oder behördliche Anfragen vorbereitet?

Wie bereit sind Sie?

- [ ] Überwiegend „Ja" – Sie sind auf dem richtigen Weg, aber Automatisierung und Nachweise zählen.
- [ ] Mehrere „Nein" – hohes Risiko von CRA-Non-Compliance und Verzögerungen bei Kunden.



Erhalten Sie ein maßgeschneidertes SBOM- & CRA-Readiness-Assessment

Wir helfen Organisationen, von Ad-hoc-SBOMs zu CRA-fähigen, auditierbaren Prozessen zu gelangen:

- SBOM-Erstellung & Automatisierung (CI/CD-ready)
- Schwachstellen- und Abhängigkeits-Monitoring
- Open-Source-Lizenz-Compliance & Dokumentation
- Laufende Compliance- und Reporting-Services
- CRA-Gap-Analyse und Readiness-Roadmap

Warum uns?

Nachgewiesene Erfolgsbilanz

Expertise in Open-Source-Compliance, Cybersecurity und regulatorischer Transformation

Globale Präsenz

Tiefes EU-Regulierungs-Know-how in Advisory und Managed Services

Flexibel & praxisnah

Herstellerunabhängige Unterstützung, abgestimmt auf bestehende Tools und Entwicklungsumgebungen

Über uns

Bei BearingPoint befähigen wir Organisationen, sichere und konforme Software-Ökosysteme aufzubauen – mit integrierten Services für SBOM-Management, Risiko-Governance und CRA-Readiness. Unser End-to-End-Ansatz hilft Kunden, Softwaretransparenz zu stärken, Compliance-Risiken zu reduzieren und eine skalierbare Grundlage für Cyber-Resilienz zu schaffen.

Fordern Sie noch heute Ihre SBOM-Management-Demo an

BearingPoint