

RISIKO-RADAR

7 STEUERUNGSDIMENSIONEN DER DIGITALEN SOUVERÄNITÄT

Orientierung für die Arbeit an den Workshop-Szenarien

Die sieben Dimensionen helfen dabei, digitale Souveränität nicht nur technisch, sondern ganzheitlich aus Sicht von Steuerung, Daten, Betrieb, Lieferkette, Recht und Sicherheit zu betrachten. Sie dienen als Denkraum für die Ausarbeitung der Szenarien aus CIO-Perspektive.

SOUVERÄN
SICHER
HANDLUNGSFÄHIG

DIGITALE
SOUVERÄNITÄT STÄRKT
UNSERE ZUKUNFT.

VERANTWORTUNG HEUTE.
HANDLUNGSFÄHIGKEIT MORGEN.



CIO Accountability Lens – über alle Dimensionen hinweg prüfen:



KENNEN

Rollen und Abhängigkeiten transparent machen



BEWERTEN

Auswirkungen und Kritikalität einschätzen



ENTSCHEIDEN

bewusst positionieren und Entscheidungen herbeiführen



HANDELN

Maßnahmen veranlassen



ESKALIEREN

Restrisiken auf die richtige Ebene bringen



NACHWEISEN

Umsetzung und Wirksamkeit belegen

CIO ACCOUNTABILITY RADAR

SOUVERÄN
SICHER
HANDLUNGSFÄHIG

DIGITALE
SOUVERÄNITÄT STÄRKT
UNSERE ZUKUNFT.

10 zentrale Risikofelder aus der CIO-Perspektive

Führungsverantwortung erkennen. Bewusst steuern. Handlungsfähig bleiben.



Der CIO muss nicht jedes Risiko verhindern. Er muss sicherstellen, dass relevante Risiken bekannt, bewertet, angemessen adressiert und verbleibende Restrisiken bewusst entschieden sind.

Managementperspektive;
keine individuelle rechtliche
Bewertung oder Rechtsberatung.

RISIKO-RADAR

Konkrete Risiken in den 7 Steuerungsdimensionen der digitalen Souveränität

Was kann mit unserer digitalen Handlungsfähigkeit passieren?

Die sieben Dimensionen machen sichtbar, welche Risiken ein CIO im Blick behalten muss, um digitale Handlungsfähigkeit, Kontrolle und Resilienz der eigenen Organisation zu sichern.

SOUVERÄN
SICHER
HANDLUNGSFÄHIG

VERANTWORTUNG HEUTE.
HANDLUNGSFÄHIGKEIT
MORGEN.



Diese Risiken können einzeln, kombiniert oder unerwartet eintreten.

Entscheidend ist, sie frühzeitig zu erkennen, bewusst zu steuern und angemessen zu adressieren.

DIGITALE SOUVERÄNITÄT

3 Szenarien für die CIO-Perspektive

Reale Entscheidungssituationen. Strategisch denken. Handlungsfähig bleiben.

HEUTE
VERANTWORTUNG
FÜR MORGEN.
DIGITALE
SOUVERÄNITÄT.
HANDLUNGSFÄHIG.

1. Kritischer Provider fällt aus

Operative Souveränität



Ausgangslage

- Geschäftskritische Prozesse hängen an einem externen Cloud- oder SaaS-Anbieter.
- Der Anbieter gilt als zuverlässig; Alternativen wurden kaum weiterentwickelt.
- Mehrere Teams sind im Tagesgeschäft direkt auf die Plattform angewiesen.



Ereignis

- Montagmorgen: großflächiger Ausfall des Services.
- Keine belastbare Aussage zur Wiederherstellungszeit.
- Manuelle Ausweichprozesse existieren nur teilweise.



CEO-Frage

Wie lange können wir unter diesen Bedingungen weiterarbeiten, und wie gut sind wir auf einen solchen Ausfall vorbereitet?

2. Strategischer Provider ändert die Spielregeln

Strategische Souveränität



Ausgangslage

- Ein globaler Technologieanbieter trägt zentrale Plattformleistungen.
- Immer mehr Anwendungen, Daten und Prozesse basieren auf dessen Technologie.
- Die Pfadabhängigkeit ist über Jahre gewachsen.



Ereignis

- Der Anbieter ändert seine Preis- und Produktstrategie.
- Kosten steigen deutlich.
- Einzelne Produkte werden eingestellt.
- Der Migrationspfad erfordert die Nutzung proprietärer Services.
- Ein Wechsel würde 12–18 Monate dauern.



CEO-Frage

Wie Abhängig sind wir tatsächlich von diesem Anbieter, und haben wir diese Abhängigkeit bewusst akzeptiert?

3. KI wird schneller geschäftskritisch als erwartet

Zukünftige Souveränität



Ausgangslage

- Mehrere Bereiche nutzen externe KI-Dienste produktiv.
- Die Einsatzfelder reichen von Wissenssuche bis Kundenkommunikation.
- Die Nutzung wächst schneller als ursprünglich geplant.



Ereignis

- Zentrale Arbeitsprozesse richten sich auf einen KI-Anbieter aus.
- Sensible Unternehmensdaten fließen in KI-gestützte Prozesse ein.
- Kosten und Nutzung steigen deutlich.
- Nicht alle KI-Anwendungen werden zentral erfasst oder freigegeben.



CEO-Frage

Nutzen wir KI kontrolliert als Wettbewerbsvorteil – oder bauen wir gerade die nächste strategische Abhängigkeit auf?

Von der Situation zur CIO-Verantwortung – Leitfragen für die Gruppenarbeit



WISSEN

Was muss der CIO wissen?



ENTSCHEIDEN

Was muss der CIO entscheiden?



HANDELN

Was muss der CIO vorbereiten/veranlassen?



ESKALIEREN

Welches Risiko muss der CIO transparent machen?



NACHWEISEN

Was muss der CIO belegen können?

CIO ACTION PROTOCOL

Canvas zur Bewertung und Steuerung der digitalen Souveränität

Vorstandstaugliche Sicht auf kritische Abhängigkeiten, Risiken, Maßnahmen und Entscheidungen.

SOUVERÄN
SICHER
HANDLUNGSFÄHIG

DIGITALE
SOUVERÄNITÄT
STÄRKT
UNSERE ZUKUNFT.



CEO-Leitfrage: Wie steht es um unsere digitale Souveränität?

Ziel: Die wesentlichen Handlungsfelder bewerten, den Status sichtbar machen, Risiken benennen und die nächsten Entscheidungen festhalten.

#	Handlungsfeld	CIO-Kernfrage	Status	Wesentliche Risiken / Lücken	Maßnahmen / Entscheidungen
1	Kritische Abhängigkeiten	Wissen wir, wovon unser Geschäft digital kritisch abhängt?	G Y R		
2	Bewusste Abhängigkeiten	Welche Abhängigkeiten akzeptieren wir bewusst – und warum?	G Y R		
3	Strategische Handlungsfreiheit	Wo ist unsere Reaktionsfähigkeit eingeschränkt?	G Y R		
4	Handlungsalternativen	Welche realistischen Optionen haben wir im Ernstfall?	G Y R		
5	Business Resilience	Wie lange verkraftet das Geschäft digitale Störungen?	G Y R		
6	Eigene Fähigkeiten	Welche Kompetenzen müssen wir selbst behalten?	G Y R		
7	Neue Abhängigkeiten	Wo entstehen durch KI und neue Technologien neue Risiken?	G Y R		
8	Steuerung & Review	Sind Risiken identifiziert, Maßnahmen gestartet und wird regelmäßig neu bewertet?	G Y R		



CIO Accountability Check

VON DER ANALYSE ZUR ENTSCHEIDUNG



WISSEN

Was muss ich wissen?



ENTSCHEIDEN

Was muss ich entscheiden?



HANDELN

Was muss ich veranlassen?



ESKALIEREN

Welches Restrisiko muss ich transparent machen?



NACHWEISEN

Womit kann ich die Steuerung belegen?



Nächste Schritte aus dem Workshop

IDEEN IN WIRKUNG BRINGEN



Top-3 Prioritäten in den nächsten 90 Tagen

1

2

3



Entscheidungen / Eskalationen an CEO / Vorstand

1

2

3



Review-Takt & Verantwortlichkeit



VERANTWORTUNG HEUTE. HANDLUNGSFÄHIGKEIT MORGEN.

KLARER
SOUVERÄNER
STÄRKER

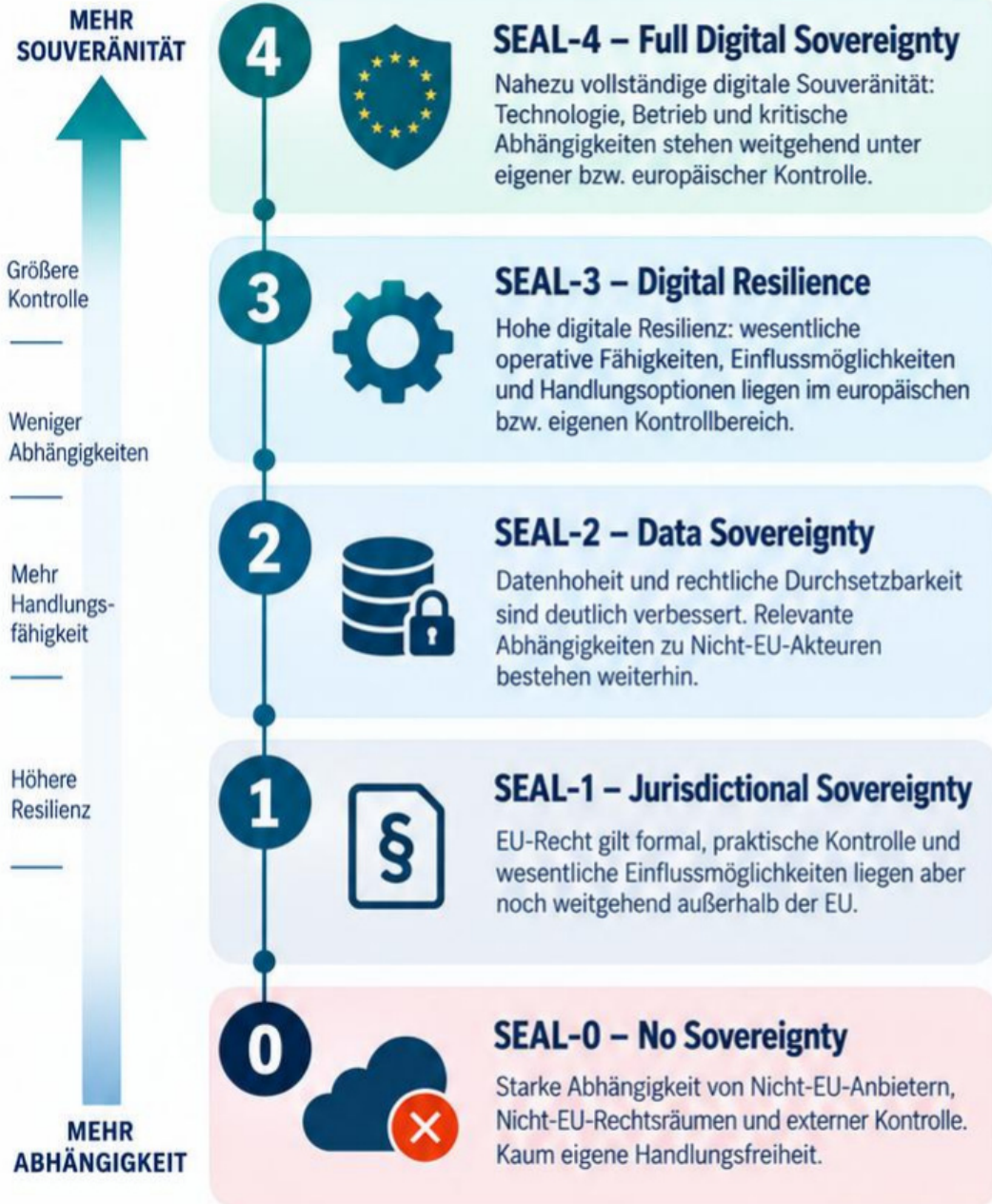
SEAL-MODELL

BEWUSST
BEWERTEN
ENTSCHEIDEN

DIGITALE SOUVERÄNITÄT
BRAUCHT KLARE NIVEAUS.

Souveränitätsniveaus im Cloud Sovereignty Framework

Orientierung für den CIO: Nicht jede Cloud-Leistung braucht maximale Souveränität – entscheidend ist, welches Niveau wir bewusst benötigen und welche Abhängigkeiten wir akzeptieren.



Wie lese ich die SEAL-Logik?

- 1** SEAL ist kein Ja/Nein, sondern ein abgestuftes Souveränitätsniveau.
- 2** Je kritischer ein Service, desto bewusster muss das erforderliche Niveau festgelegt werden.
- 3** Nicht jede Leistung braucht SEAL-4.
- 4** Wichtig ist die bewusste Entscheidung über akzeptierte Abhängigkeiten.

Worauf der CIO achten sollte

- 1** Welche Leistungen sind geschäftskritisch?
- 2** Wo bestehen Rechts-, Provider- oder Lieferkettenabhängigkeiten?
- 3** Welche Daten, Schlüssel und Betriebsfunktionen müssen unter Kontrolle bleiben?
- 4** Wie reversibel ist die Entscheidung?
- 5** Welches SEAL-Niveau ist für diesen Fall angemessen?

Übersetzung ins CIO Action Protocol

VON DER EINORDNUNG ZUR UMSETZUNG.



1 Kritische Services identifizieren



2 Erforderliches Souveränitätsniveau festlegen



3 Abhängigkeiten transparent machen



4 Restrisiken bewusst akzeptieren oder reduzieren



5 Regelmäßig überprüfen und neu bewerten



Orientierungsposter für die Workshoparbeit – vereinfachte Darstellung der SEAL-Logik.

KLARE NIVEAUS.
STARKE ENTSCHEIDUNGEN.
SOUVERÄNE ZUKUNFT.