OpenDirection

Digitale Souveränität bewerten

Kriterien, Selbsttests und Assessmentverfahren für Organisationen im Vergleich

Kernaussage

Aktuell existiert weder in Deutschland noch auf Ebene der Europäischen Union ein allgemein verbindlicher Bewertungsstandard für die digitale Souveränität einer Organisation. Für eine belastbare Beurteilung müssen deshalb die organisationsweite Standortbestimmung, die Bewertung kritischer IT-Services und überprüfbare Nachweise miteinander verbunden werden.

Stand 14. September 2026

Orientierung für Strategie, Beschaffung, Governance und Portfoliosteuerung

opendirection.de

Inhalt

Hinweis zum Stand Die Veröffentlichung bildet den öffentlich verfügbaren Stand vom 14. September 2026 ab. Rechtliche und regulatorische Vorgaben können sich ändern. Die Einordnung ersetzt keine Rechtsberatung.

1 Ziel, regulatorischer Status und Einordnung

Diese Veröffentlichung gibt einen Überblick über verfügbare Kriterienkataloge, Selbsttests und Assessmentverfahren zur Bewertung der digitalen Souveränität von Organisationen. Sie unterscheidet zwischen unmittelbar nutzbaren Tests, professionell begleiteten Assessments und Modellen, die Kriterien und Zielbilder beschreiben, aber noch kein direkt ausführbares Bewertungsverfahren bereitstellen.

Keine allgemein verbindlichen Bewertungsvorgaben

Nach dem derzeit öffentlich verfügbaren Stand existiert weder in Deutschland noch auf Ebene der Europäischen Union eine allgemein verbindliche gesetzliche Definition, nach der der Grad der digitalen Souveränität einer Organisation einheitlich gemessen, zertifiziert oder in einen verbindlichen Reifegrad eingeordnet werden muss. Das ZenDiS stellt fest, dass bislang keine belastbare und allgemein anerkannte Grundlage besteht, mit der die digitale Souveränität der öffentlichen Verwaltung insgesamt valide bewertet und verglichen werden kann. Der veröffentlichte Kriterienkatalog soll deshalb als Grundlage für einen künftig praxisfähigen Souveränitätscheck dienen. [1]

- Kein gesetzlich vorgeschriebener organisationsweiter Souveränitätstest
- Kein verbindlicher und anbieterübergreifender Souveränitätsscore
- Keine staatlich vorgeschriebene Reifegradskala
- Keine allgemeine Zertifizierung als digital souveräne Organisation
- Keine abschließend normierte Gewichtung einzelner Souveränitätskriterien

Verbindliche Vorgaben in angrenzenden Bereichen

Unabhängig davon bestehen verbindliche europäische und nationale Regelungen, die einzelne Aspekte digitaler Souveränität betreffen. Sie bilden jedoch keinen vollständigen Bewertungsstandard für die digitale Souveränität einer Organisation.

Regelwerk	Bezug zur digitalen Souveränität
Datenschutz-Grundverordnung DSGVO	Kontrolle über personenbezogene Daten, Rechtsgrundlagen, Auftragsverarbeitung, Drittlandübermittlungen und Betroffenenrechte
NIS2 und nationale Umsetzung	Risikomanagement, Lieferkettensicherheit, Sicherheitsmaßnahmen, Vorfallmanagement und Resilienz
Digital Operational Resilience Act DORA	Operative Resilienz, Drittanbietersteuerung und Exit-Anforderungen im Finanzsektor
EU AI Act	Governance, Risikomanagement, Transparenz und Kontrolle beim Einsatz von KI-Systemen
EU Data Act	Datenzugang, Datenportabilität und Wechselmöglichkeiten insbesondere bei Cloud- und Datenverarbeitungsdiensten

Regelwerk	Bezug zur digitalen Souveränität
Cyber Resilience Act CRA	Sicherheitsanforderungen, Schwachstellenmanagement und Verantwortlichkeiten für Produkte mit digitalen Elementen
Vergabe-, Haushalts- und Datenschutzrecht	Nachvollziehbare Beschaffung, Wirtschaftlichkeit, Wettbewerb und rechtssichere Verarbeitung

Strategische und beschaffungsbezogene Vorgaben

- Die Strategie des IT-Planungsrats definiert Wechselmöglichkeit, Gestaltungsfähigkeit und Einflussnahme als zentrale Ziele.
- Das ZenDiS entwickelt daraus Kriterien für Organisationen und IT-Services.
- Das EU Cloud Sovereignty Framework stellt einen detaillierten Bewertungsrahmen für Cloud-Beschaffungen bereit.
- BSI IT-Grundschutz, BSI C5 und vergleichbare Standards können Sicherheits- und Kontrollanforderungen nachweisen.

Diese Ansätze sind nicht automatisch allgemein rechtsverbindlich. Sie können verbindlich werden, wenn sie in Gesetzen, Verwaltungsvorschriften, Beschaffungsunterlagen, Verträgen, Sicherheitsrichtlinien oder internen Organisationsvorgaben ausdrücklich vorgeschrieben werden. Das EU Cloud Sovereignty Framework ist beispielsweise kein allgemeines Gesetz, kann aber in einem konkreten Vergabeverfahren als Mindest- oder Zuschlagskriterium verbindlich eingesetzt werden. [2]

Unterscheidung der Bewertungsansätze

1. Funktionale Selbsttests erfassen Antworten, berechnen einen Wert oder Reifegrad und geben eine unmittelbare Auswertung aus.
2. Begleitete oder softwaregestützte Assessments kombinieren Fragebögen, Datenaufnahme, Beratung, Nachweise und teilweise automatisierte Analysen.
3. Kriterien- und Orientierungsmodelle beschreiben relevante Anforderungen, stellen aber noch kein unmittelbar ausführbares Bewertungsverfahren bereit.

Wichtige Einschränkung Ein hoher Wert in einem Selbsttest ist nicht mit einer Zertifizierung gleichzusetzen. Die meisten Selbsttests beruhen auf Selbstauskünften. Sie prüfen nicht automatisch technische Eigenschaften, vertragliche Zusagen oder die tatsächliche Durchführbarkeit eines Anbieterwechsels.

2 Bewertungsansätze im Überblick

Quelle	Art des Ansatzes	Auswertung	Ebene	Schwerpunkte
OpenDirection	Browserbasierter Online-Selbsttest	Ja	Gesamtorganisation	Strategie, Infrastruktur, Anwendungen, Daten, Kompetenzen, Zusammenarbeit
KDN-Selbsttest	Browserbasierte HTML-Datei ohne externe Anbindung	Ja	Gesamtorganisation	Open Source, Standards, Betrieb, Resilienz, Verträge, Wirtschaftlichkeit, Prüfbarkeit, Zusammenarbeit
ÖFIT Fraunhofer FOKUS	Online-Selbsttest	Ja	Gesamtorganisation	Mitarbeitende, Außenauftritt, Daten, Sicherheit, Hard- und Software
Red Hat	Online-Readiness-Assessment	Ja	Organisation und IT-Landschaft	Daten, Technik, Betrieb, Sicherheit, Open Source, Governance, Managed Services
SUSE	Online-Assessment	Ja	Cloud- und Technologielandschaft	Acht Ziele des EU Cloud Sovereignty Framework
GISA	Reifegrad-Selbstbewertung	Ja	Kommune oder Behörde	Strategie, Digitalisierung, Verwaltungscloud, Infrastruktur, Daten, Open Source
Bechtle BIoS	Begleitetes softwaregestütztes Assessment	Ja	Prozesse, Services und IT-Architektur	Datenhoheit, technologische Unabhängigkeit, Kompetenzen
Stadt München SDS	Organisationsinternes Bewertungsverfahren	Ja	Kritische IT-Services	Anbieterabhängigkeit, Wechselmöglichkeit, Standards, Einflussnahme, Recht und Sicherheit
Europäische Kommission	Beschaffungs- und Bewertungsrahmen	Bei Anwendung	Cloud-Services und Anbieter	Acht Souveränitätsziele, Nachweise, Mindestniveaus und gewichteter Score
ZenDiS	Kriterienkatalog und Diskussionspapier	Noch nicht allgemein	Öffentliche Verwaltung und IT-Services	Organisation, Anwendungen, Daten, Betrieb
IT-Planungsrat	Strategischer Orientierungsrahmen	Nein	Öffentliche Verwaltung	Wechselmöglichkeit, Gestaltungsfähigkeit, Einflussnahme

3 Funktionale Selbsttests

3.1 OpenDirection-Selbsttest

Der OpenDirection-Selbsttest besteht aus 24 Aussagen in sechs Themenfeldern. Jede Aussage wird mit 0, 1 oder 2 Punkten bewertet; insgesamt sind 48 Punkte erreichbar. Die Auswertung erfolgt unmittelbar im Browser. Neben dem Gesamtscore werden schwache Themenfelder und prioritäre Handlungsbereiche ausgewiesen. Antworten werden nicht automatisch übertragen oder gespeichert. [3]

Themenfeld	Bewertungsgegenstand
Strategie	Zielbild, Verantwortlichkeiten, Entscheidungsgrundlagen und regelmäßige Steuerung
Infrastruktur	Abhängigkeiten, Betriebsmodelle, Resilienz und Austauschbarkeit grundlegender Komponenten
Anwendungen	Modularität, Schnittstellen, Standards, Alternativen und Exit-Fähigkeit
Daten	Datenzugriff, Datenformate, Portabilität sowie Speicher- und Verarbeitungsorte
Kompetenzen	Betriebs-, Architektur-, Beschaffungs- und Anwenderkompetenzen sowie Wissenssicherung
Zusammenarbeit	Kooperation, gemeinsames Anforderungsmanagement und Einflussnahme auf Anbieter

Einordnung Vollständig funktionaler Online-Selbsttest für eine erste strategische Standortbestimmung. Die kompakte Bewertung ersetzt keine technische Prüfung oder belastbare Anbieterbewertung.

3.2 KDN-Selbsttest

Der KDN-Selbsttest ist als browserbasierte HTML-Datei umgesetzt. Er kann lokal in einem Browser geöffnet und verwendet werden und benötigt keine externe technische Anbindung. Beantwortung und Auswertung erfolgen innerhalb der HTML-Anwendung. Dadurch ist der Test auch in abgeschotteten Verwaltungsnetzen oder ohne Internetzugang einsetzbar. Die eingegebenen Antworten müssen nicht an einen externen Dienst oder Anbieter übertragen werden.

Themenfeld	Bewertungsgegenstand
Open Source	Einsatz, strategische Berücksichtigung und Beschaffungsmöglichkeit quelloffener Software

Themenfeld	Bewertungsgegenstand
Offene Standards	Verwendung dokumentierter, interoperabler und möglichst herstellerunabhängiger Standards
Zusammenarbeit	Kooperation mit Kommunen, IT-Dienstleistern, Communities und anderen öffentlichen Stellen
Betrieb	Eigene oder vertraglich abgesicherte Fähigkeit, Systeme zu betreiben, zu administrieren und weiterzuentwickeln
Resilienz	Wiederanlauf, Notbetrieb, Ausfallsicherheit und Umgang mit dem Wegfall eines Anbieters
Verträge	Datenzugriff, Audit-, Informations-, Kündigungs-, Herausgabe- und Unterstützungsrechte
Wirtschaftlichkeit	Langfristige Kosten, Wechselkosten und Abhängigkeiten statt alleiniger Anschaffungskosten
Prüfbarkeit	Zugang zu Dokumentationen, Schnittstellen, Sicherheitsinformationen und erforderlichen Nachweisen

Stärken und Grenzen

- Keine externe Anbindung erforderlich und lokal einsetzbar
- Datensparsame Verwendung auch in abgeschotteten Netzen
- Unmittelbar in Workshops nutzbar
- Schnelle Identifikation von Handlungsfeldern

Der Test beruht auf den Einschätzungen der Teilnehmenden. Er prüft nicht automatisch, ob vertragliche Exit-Rechte durchsetzbar sind, Daten vollständig exportiert werden können, ein Anbieterwechsel technisch erprobt wurde oder Sicherheitsangaben belegt sind.

Einordnung Funktionaler, lokal ausführbarer Selbsttest zur organisationsweiten Standortbestimmung. Für kritische Systeme ist er durch Dokumentenprüfungen, technische Nachweise und praktische Tests zu ergänzen.

3.3 ÖFIT-Selbsttest

Der Selbsttest des Kompetenzzentrums Öffentliche IT am Fraunhofer FOKUS richtet sich vor allem an mittlere und große Organisationen. Nach der Befragung wird eine individuelle Auswertung mit praktischen Hinweisen bereitgestellt. [4]

- Souveränität der Mitarbeitenden oder Mitglieder
- Souveränität im Außenauftritt
- Datensouveränität
- Sicherheit und Resilienz
- Hard- und Softwaresouveränität

Der Ansatz berücksichtigt stärker als viele technische Assessments die Handlungsfähigkeit von Menschen und die Außenbeziehungen einer Organisation. Beschaffung, Vertragsgestaltung, Wirtschaftlichkeit und konkrete Exit-Nachweise werden weniger detailliert betrachtet.

Einordnung Funktionaler, wissenschaftlich fundierter Reflexions- und Orientierungstest. Er ist kein technisches Audit.

3.4 Red Hat Digital Sovereignty Readiness Assessment

Red Hat bietet ein Self-Service-Assessment mit unmittelbarer Reifegradeinordnung und Maßnahmen-Roadmap an. Die zugrunde liegenden logischen Blueprints werden nach Angaben von Red Hat als Open Source veröffentlicht. [5]

Dimension	Gegenstand
Datensouveränität	Physische und rechtliche Kontrolle über Daten während des gesamten Lebenszyklus
Technische Souveränität	Transparenz und Zusammensetzung des Software-Stacks
Operative Souveränität	Eigenständiger Betrieb, Wartung und Wiederherstellung
Sicherheitssouveränität	Unabhängige Prüfung und Validierung der Systemintegrität
Open-Source-Bewusstsein	Offene Innovation zur Verringerung von Lock-in
Aufsicht durch die Leitung	Verankerung in Strategie und Governance
Managed Services	Wahlmöglichkeiten bei Regionen, Rechenzentren und Bereitstellungsmodellen

Die Ergebnisse werden den Stufen Grundlage, In Entwicklung, Strategisch und Fortgeschritten zugeordnet. Diese Logik entspricht den verbreiteten Reifegradstufen Foundation, Developing, Strategic und Advanced.

Einordnung Funktionaler und transparenter Readiness-Test mit technisch-betrieblichem Schwerpunkt. Für eine neutrale Gesamtbewertung sind Vertrags-, Wirtschaftlichkeits- und organisationsspezifische Kriterien zu ergänzen.

3.5 SUSE Cloud Sovereignty Framework Self Assessment

Das SUSE-Assessment umfasst 32 Fragen und orientiert sich an den acht Zielen des EU Cloud Sovereignty Framework. Es liefert eine Bewertung erkannter Lücken und konkrete Handlungsempfehlungen. [6]

- Strategie
- Recht und Jurisdiktion
- Daten und KI
- Betrieb
- Lieferkette
- Technologie
- Sicherheit und Compliance
- Nachhaltigkeit

Der Ansatz eignet sich besonders für Cloud-Strategien, Cloud-Beschaffungen und internationale Lieferketten. Allgemeine Organisationsfragen, Anwenderkompetenzen, Change Management und kommunale Kooperationen werden weniger umfassend abgebildet.

Einordnung Funktionaler Cloud-Selbsttest mit enger Anbindung an den europäischen Bewertungsrahmen.

3.6 GISA-Reifegradmodell

Das GISA-Modell ermöglicht eine Selbstbewertung und ordnet die Organisation einem von vier Reifegraden zu: Einsteiger, Fortgeschritten, Profi und Experte. Die Auswertung enthält unter anderem eine grafische Darstellung. [7]

Handlungsfeld	Kernaussage
Management und Strategie	Souveränität ist bei der Leitung verankert und wird aktiv gesteuert
Allgemeiner Digitalisierungsgrad	Digitale Prozesse und Dienste sind organisatorisch etabliert
Verwaltungscloud und Souveränität	Lösungen, Komponenten und Anbieter können gewechselt werden
IT-Infrastruktur	Bereitstellung und Betrieb werden durch klare Prozesse und Verantwortlichkeiten gesteuert
Daten und Sicherheit	Datenstrategie, Schutzmaßnahmen und regulatorische Anforderungen sind verankert
Open Source	Offene und standardisierte Technologien werden systematisch berücksichtigt

Einordnung Funktionales kommunales Reifegradmodell. Bei der Interpretation sollten allgemeiner Digitalisierungsgrad und tatsächliche Souveränität getrennt betrachtet werden.

4 Begleitete und organisationsinterne Assessments

4.1 Bechtle Index of Sovereignty BIoS

Der Bechtle Index of Sovereignty ist ein softwaregestütztes und durch Beratende begleitetes Assessment. Bewertet werden IT-Komponenten, Anwendungsservices, zentrale Geschäfts- und Verwaltungsprozesse sowie die übergreifende Business-Architektur. Ergebnisse können fortgeschrieben und für Szenarioanalysen verwendet werden. [8]

- Datenhoheit
- Technologische Unabhängigkeit
- Kompetenzen entlang zentraler Geschäfts- und Verwaltungsprozesse
- Abhängigkeiten und Risiken
- Alternative Technologien und tatsächliche Veränderungen
- Regulatorische Anforderungen und priorisierte Maßnahmen

BIoS geht über einen klassischen Selbsttest hinaus. Nicht öffentlich dokumentiert sind bislang der vollständige Kriterienkatalog, die Gewichtungslogik und die genaue Funktionsweise der KI-gestützten Aggregation. Die Bezeichnung als objektives Referenzmaß ist daher von außen noch nicht vollständig nachvollziehbar. Das Verfahren wurde 2026 zunächst in Deutschland, Österreich und der Schweiz pilotiert. [9]

Einordnung Funktionales, professionell begleitetes Assessment mit hoher Analysetiefe, aber proprietärer und bislang nur teilweise transparenter Methodik.

4.2 Score für Digitale Souveränität der Stadt München

Die Stadt München hat einen strukturierten Fragenkatalog mit quantitativer Bewertung für einzelne IT-Services entwickelt. Die Methodik wurde wissenschaftlich durch die Technische Universität München begleitet und ist unter CC BY-SA 4.0 nachnutzbar. [10]

- Hersteller- und Anbieterabhängigkeiten
- Wechselmöglichkeiten, Open Source und offene Standards
- Einfluss auf Betrieb, Weiterentwicklung und Daten
- Sicherheits- und Rechtsaspekte

Die Ergebnisse werden einer von fünf SDS-Kategorien zugeordnet. Im September und Oktober 2025 wurden 194 besonders kritische Anwendungsservices aus insgesamt 2.780 Services analysiert. Die risikobasierte Auswahl nach Geschäftskritikalität ist eine besondere Stärke des Ansatzes.

Einordnung Funktionales und praktisch erprobtes Bewertungsverfahren. Der Schwerpunkt liegt auf einzelnen IT-Services und weniger auf der Gesamtorganisation.

5 Kriterienmodelle und Bewertungsrahmen

5.1 ZenDiS-Kriterienkatalog

Das ZenDiS-Diskussionspapier Kriterien zur Bewertung von Digitaler Souveränität überführt die drei Ziele des IT-Planungsrats in einen detaillierten Kriterienkatalog. Der veröffentlichte Stand vom März 2026 ist als Grundlage für die Entwicklung eines Souveränitätschecks angelegt. [1]

Kategorie	Kriterien
Organisation und Fähigkeiten	Strategie, IT-Governance und Management, Risikomanagement, Beschaffung und Vergabe, Auftraggeberfähigkeit, Kompetenzen
Digitale Anwendungen und Dienste	Softwareabhängigkeiten, Modularität, Standards, Schnittstellen, Dokumentation, Lieferkettentransparenz
Informationen und Daten	Datenlokation, Datensicherheit, Datenschutz, offene und interoperable Datenstrukturen
Betrieb und Infrastruktur	Providerabhängigkeit, Kundenverhältnis, Exit-Fähigkeit, Resilienz, Business Continuity, Sicherheit und Compliance

Die Bewertung soll risikobasiert erfolgen. Maßgeblich sind insbesondere Kritikalität der Verwaltungsprozesse, Datenkritikalität, Abhängigkeitsgrad, Rechtsrisiken, Sicherheitslage und Zuverlässigkeit der Lieferkette.

Einordnung Sehr geeignete fachliche Grundlage für die öffentliche Verwaltung. Die veröffentlichte Fassung ist jedoch noch kein vollständig operationalisierter und allgemein verfügbarer Selbsttest.

5.2 EU Cloud Sovereignty Framework

Das Cloud Sovereignty Framework der Europäischen Kommission ist primär ein Bewertungsrahmen für Cloud-Beschaffungen. Anbieterantworten werden durch Nachweise und öffentlich verfügbare Informationen ergänzt. Das Framework kombiniert Mindestanforderungen mit einem gewichteten Souveränitätsscore. [2]

Ziel	Inhalt	Gewicht
Strategische Souveränität	Eigentum, Kontrolle, Finanzierung und Wertschöpfung in der EU	15 %
Recht und Jurisdiktion	Anwendbares Recht und Schutz vor extraterritorialen Zugriffen	10 %

Ziel	Inhalt	Gewicht
Daten und KI	Kontrolle über Daten, Schlüssel, Verarbeitung und KI-Dienste	10 %
Operative Souveränität	Eigenständiger Betrieb, Support, Kompetenzen und Kontinuität	15 %
Lieferkette	Herkunft, Transparenz und Resilienz der Lieferkette	20 %
Technologie	Offenheit, Interoperabilität, Prüfbarkeit und Änderbarkeit	15 %
Sicherheit und Compliance	Zertifizierungen, Audits, Monitoring und autonome Sicherheitsmaßnahmen	10 %
Nachhaltigkeit	Energie, Ressourcen, Kreislaufwirtschaft und langfristige Resilienz	5 %

Die Assurance-Level reichen von SEAL 0 ohne Souveränität über SEAL 1 jurisdiktionelle Souveränität, SEAL 2 Datensouveränität und SEAL 3 digitale Resilienz bis zu SEAL 4 vollständige digitale Souveränität.

Einordnung Operationalisierbarer und nachweisorientierter Beschaffungsrahmen für Cloud-Services. Er ist kein organisationsweiter Selbsttest und kein allgemein geltendes Gesetz.

5.3 IT-Planungsrat

Der IT-Planungsrat bildet mit drei strategischen Zielen die grundlegende Referenz für viele nachfolgende Modelle:

4. Wechselmöglichkeit: Anbieter und Lösungen können mit vertretbarem Aufwand gewechselt werden.
5. Gestaltungsfähigkeit: Die Verwaltung kann Technologien, Dienste und Betriebsmodelle selbst mitgestalten.
6. Einflussnahme: Anforderungen können gegenüber Anbietern und im Markt wirksam vertreten werden.

Einordnung Grundlegendes strategisches Zielmodell. Die Ziele müssen für eine Bewertung durch konkrete Kriterien, Prüffragen, Gewichtungen und Nachweise operationalisiert werden.

6 Vergleichende Bewertung

Ansatz	Organisation	IT-Services	Auswertung	Nachweise	Transparenz
OpenDirection	Hoch	Gering	Ja	Nein	Hoch
KDN-Selbsttest	Hoch	Gering	Ja	Nein	Mittel
ÖFIT	Hoch	Gering	Ja	Nein	Hoch
Red Hat	Hoch	Mittel	Ja	Teilweise	Hoch
SUSE	Mittel	Hoch bei Cloud	Ja	Nein	Mittel bis hoch
GISA	Hoch	Gering	Ja	Nein	Mittel
Bechtle BIoS	Hoch	Hoch	Ja	Möglich	Eingeschränkt
Stadt München SDS	Mittel	Sehr hoch	Ja	Teilweise	Hoch
ZenDiS	Hoch	Hoch	Noch nicht	Vorgesehen	Hoch
EU Cloud Framework	Gering	Sehr hoch bei Cloud	Bei Anwendung	Ja	Sehr hoch
IT-Planungsrat	Zielbild	Gering	Nein	Nein	Hoch

7 Empfehlungen für eine belastbare Bewertung

Keiner der untersuchten Ansätze deckt allein alle Anforderungen an eine ganzheitliche Bewertung digitaler Souveränität ab. Für eine belastbare Beurteilung sollten drei Ebenen miteinander verbunden werden.

Ebene 1 Organisationsweite Standortbestimmung

Geeignete Grundlagen sind der OpenDirection-Selbsttest, der KDN-Selbsttest, der ÖFIT-Selbsttest und die Reifegradlogik von Red Hat. Bewertet werden Strategie, Governance, Kompetenzen, Zusammenarbeit und grundsätzliche Steuerungsfähigkeit.

Ebene 2 Kritische IT-Services und Anbieter

Geeignete Grundlagen sind der ZenDiS-Kriterienkatalog, der Münchner Score für Digitale Souveränität, das EU Cloud Sovereignty Framework und Bechtle BIoS. Bewertet werden konkrete Abhängigkeiten, Datenflüsse, Anbieter, Verträge, Betriebsmodelle, Lieferketten und Exit-Möglichkeiten.

Ebene 3 Verifikation durch Nachweise

Für kritische Systeme dürfen Selbstauskünfte nicht ausreichen. Geeignete Nachweise sind insbesondere:

- Vertragsunterlagen sowie Kündigungs-, Herausgabe- und Exit-Regelungen
- Architektur-, Schnittstellen- und Betriebsdokumentationen
- Testexporte in offenen und dokumentierten Datenformaten
- Software-Stücklisten und Informationen zur Lieferkette
- Zertifizierungen, Auditberichte und Sicherheitsnachweise
- Dokumentierte Wiederanlauf-, Notfall- und Wiederherstellungstests
- Praktisch durchgeführte Datenmigrationen oder Anbieterwechsel
- Nachweise eigener und marktverfügbarer Betriebs- und Steuerungskompetenzen

8 Empfohlene Bewertungsdimensionen

Aus der Zusammenführung der betrachteten Modelle ergeben sich elf Dimensionen für eine organisationsweite Bewertung:

Nr	Bewertungsdimension
1	Strategische Souveränität
2	Datensouveränität
3	Technologische Souveränität
4	Operative Souveränität
5	Organisatorische Souveränität
6	Personelle und kompetenzbezogene Souveränität
7	Beschaffungs- und wirtschaftliche Souveränität
8	Rechtliche und regulatorische Souveränität
9	Sicherheits- und Resilienz-Souveränität
10	Prüf-, Transparenz- und Exit-Fähigkeit
11	Kooperations- und Ökosystem-Souveränität

Für die Reifegradbewertung können beispielsweise die vier Stufen Foundation, Developing, Strategic und Advanced verwendet werden. Für jede Dimension sollten sowohl Selbstauskünfte als auch überprüfbare Nachweise vorgesehen werden.

Leitender Bewertungsgrundsatz Ein Souveränitätskriterium gilt nicht allein deshalb als erfüllt, weil eine entsprechende Möglichkeit vertraglich oder technisch beschrieben wird. Entscheidend ist, ob die Organisation diese Möglichkeit organisatorisch beherrscht, vertraglich durchsetzen und im Bedarfsfall praktisch ausüben kann.

9 Quellen

[1] ZenDiS: Kriterien zur Bewertung von Digitaler Souveränität - aus messbar wird machbar. Diskussionspapier, März 2026.
https://www.zendis.de/media/pages/newsroom/publikationen/konsultationsprozesskriterien/d8b08da827-1774439296/zendis_diskussionspapier-kriterien-bewertung-digitaler-souveraenitaet.pdf

[2] Europäische Kommission: Cloud Sovereignty Framework, Version 1.2.1, Oktober 2025.
https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en

[3] OpenDirection: Selbsttest Digitale Souveränität. https://opendirection.de/selbsttest.html

[4] Kompetenzzentrum Öffentliche IT: Selbsttest zur digitalen Souveränität von Organisationen.
https://www.oeffentliche-it.de/werkstatt/selbsttest-digitale-souveraenitaet/

[5] Red Hat: Digital Sovereignty Readiness Assessment Tool, 16. Februar 2026.
https://www.redhat.com/de/blog/how-sovereign-your-strategy-introducing-red-hat-sovereignty-readiness-assessment-tool

[6] SUSE: Cloud Sovereignty Framework Self Assessment, 17. Februar 2026. https://www.suse.com/c/de/wie-souveraen-ist-ihre-it-finden-sie-es-in-20-minuten-heraus-mit-unserem-neuen-assessment-tool-das-jetzt-auf-deutsch-verfuegbar-ist/

[7] GISA: Digitale Souveränität messen und verbessern.
https://www.gisa.de/media-und-events/blog/digitale-souveraenitaet-messen-und-verbessern/

[8] Bechtle: Fünf Fragen zum Bechtle Index of Sovereignty, 30. März 2026. https://www.bechtle.com/ueber-bechtle/newsroom/it-solutions/2026/fuenf-fragen-bechtle-index-of-sovereignty

[9] Bechtle: Bechtle bringt Souveränitäts-Assessment auf den Markt, 12. März 2026.
https://www.bechtle.com/ueber-bechtle/presse/pressemeldungen/2026/bechtle-bringt-souveraenitaets-assessment-auf-den-markt

[10] Landeshauptstadt München: Digitale Souveränität und Score für Digitale Souveränität.
https://muenchen.digital/projekte/digitale-souver%C3%A4nit%C3%A4t.html