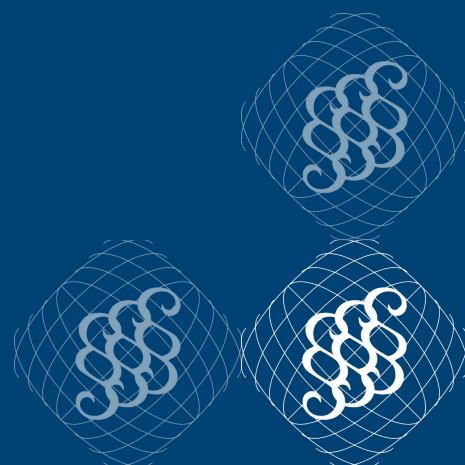




Öffentliche Konsultation - Diskussionspapier

Kriterien für Digitale Souveränität – aus messbar wird machbar

Stellungnahme von Frank Ingenrieth





1 0 Über den Autor

2 Frank Ingenrieth, LL.M. (**Gutachter**) ist Führungskraft und niedergelassener Anwalt mit über 15
3 Jahren interdisziplinärer, internationaler Erfahrung im Bereich Steuerung von Datenschutz- und
4 Regulierungsstrategien für nachhaltige, innovationsorientierte Lösungen. Sein Schwerpunkt
5 liegt im Medien-, Internet- und Datenschutzrecht, sowie verbundenen Rechtsgebieten, z.B.
6 Mietrecht, oder wechselwirkende Rechtsgebiete, etwa dem Wettbewerbs- und Kartellrecht,
7 sowie im Bereich der Fragen der Good Governance.¹

8 Seine Erfahrung sammelte Frank Ingenrieth während seines beruflichen Werdegangs, inklusive
9 seiner Ausbildung, in internationalen Großkanzleien, datenschutzrechtlicher Aufsichtsbehör-
10 den, internationaler Konzerne, gemeinnütziger Organisationen. Er veröffentlicht regelmäßig,
11 entweder im Rahmen von juristischer Fachliteratur, Fachkommentare, sowie in Form von Dis-
12 kussionsrunden und Panels².

13 Diese Stellungnahme wurde unabhängig und ohne Auftrag durch etwaige Mandant*Innen
14 erstellt. Die Stellungnahme und die Anmerkungen basieren auf der langjährigen praktischen
15 Erfahrung des Autors in der Entwicklung und Durchsetzung von Konformitätsbewertungspro-
16 grammen, inklusive solcher Prüfprogramme, die aufgrund ihrer rechtlichen Vermutungswirkun-
17 gen behördlicher Anerkennung bedürfen.

18 **Pflicht- und Kontaktinformationen des Autors**

19	Richard-Sorge-Straße 69a	24	Steuer-Nummer 14/358/01684,
20	10249 BERLIN	25	FA Friedrichshain-Kreuzberg.
21	Fon +49 30 985 387 95	26	Ich optiere gem. § 19 UstG als Kleinunterneh-
22	Fax +49 30 521 036 88	27	mer.
23	E-Mail office@ingenrieth-online.de	28	IBAN DE22 5002 4024 7497 0388 01

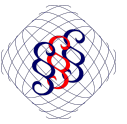
29	Zuständige Kammer	35	wesentliche berufsrechtliche Regelungen
30	Rechtsanwaltskammer Berlin, Littenstraße 9,	36	• Bundesrechtsanwaltsordnung
31	10179 Berlin	37	• Berufsordnung
32	In Deutschland verliehene	38	• Rechtsanwaltsvergütungsgesetz.
33	Berufsbezeichnung	39	Diese und weitere können auf der Webseite
34	Rechtsanwalt	40	der Rechtsanwaltskammer Berlin abgerufen
		41	werden.

1 Näheres über den Autor kann auf der Webseite der Kanzlei abgerufen werden:

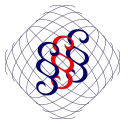
<https://ingenrieth-online.de/de/ueber>.

2 Eine Übersicht der Veröffentlichungen kann auf der Webseite der Kanzlei abgerufen werden:

<https://ingenrieth-online.de/de/publikationen>.



42	Inhaltsverzeichnis	
43	0 Über den Autor.....	2
44	Inhaltsverzeichnis.....	3
45	1 Executive Summary.....	4
46	2 Gegenstand der Stellungnahme und Struktur.....	6
47	3 Allgemeine Anmerkungen.....	7
48	3.1 konzeptionelle Überlegungen über die Potentiale von Kriterienkatalogen.....	8
49	3.1.1 theoretische Optionen und Konzepte.....	8
50	3.1.2 Übertragung der Konzepte auf das Diskussionspapier.....	9
51	3.2 Klarheit bezüglich des Gegenstands der Betrachtung.....	12
52	3.3 Existenz von und erforderliche Klarheit bezüglich der Kriterien.....	12
53	3.4 Synergiepotentiale zu anderen Souveränitätskriterien.....	13
54	3.5 Risikobetrachtung.....	14
55	4 Spezifische Anmerkungen.....	16
56	4.1 Dimension A.....	16
57	4.2 Dimension B.....	18
58	4.3 Dimension C.....	19
59	4.4 Dimension D.....	20
60	5 Fazit.....	21



1 Executive Summary

- 61
 - 62
 - 63
 - 64
 - 65
 - 66
 - 67
 - 68
 - 69
 - 70
 - 71
 - 72
 - 73
 - 74
 - 75
 - 76
 - 77
 - 78
 - 79
 - 80
 - 81
 - 82
 - 83
 - 84
 - 85
 - 86
 - 87
 - 88
 - 89
 - 90
 - 91
 - 92
 - 93
 - 94
- Gegenstand der Betrachtung ist das Diskussionspapier in der Fassung „März 2026“.
 - Die Empfehlungen betreffen sowohl generell-strukturelle Aspekte (Abschnitt 3), als auch konkrete Aspekte zu den einzelnen Dimensionen (Abschnitt 4).
 - Auf Basis der theoretischen Konzepte und Ziele von Kriterienkatalogen (Abschnitt 3.1.1) wird empfohlen den Kriterienkatalog als Reifegradmodell auszubauen (Abschnitt 3.1.2).
 - Konkret wird empfohlen ein „offenes Reifegradmodell“ zu entwickeln (Abschnitt 3.1.2). konkret wird von einer geschlossenen Ausgestaltung im Reifegradmodell für Digitale Souveränität abgeraten, obgleich sich in vielen Bereichen eine Dreistufigkeit (low/basic, essential, high) etabliert.
 - Es wird empfohlen, die Zielsetzung des Kriterienkatalogs zu klären und die Dimensionen und Kriterien streng anhand dieser Zielsetzung auszugestalten (Abschnitt 3.2).
 - Für eine objektive und vergleichbare Erfassung der Umstände müssten die Dimensionen und die Objectives in konkrete Kriterien überführt werden. Aufgrund der hohen Dynamik sollte hierbei insbesondere auch auf ergänzende Erläuterungen zurückgegriffen werden, inklusive Beispielen und Empfehlungen (Abschnitt 3.3).
 - Es sollte deutlich(er) herausgearbeitet werden, wie durch den Kriterienkatalog die Aspekte der Digitalen Souveränität ergänzt werden (Abschnitt 3.4).
 - Es sollte auf unnötige Redundanzen verzichtet werden, da diese letztlich zu einer vermeidbaren Hürde bei der Implementierung führen. Redundanzen lösen – auch ungewollt – Auslegungskonflikte aus, insbesondere soweit die Redundanz nicht wort- und kontextidentisch ist (Abschnitt 3.4).
 - Wenn und soweit Elemente des EU CSG oder der BSI C3A für förderlich aus Sicht des Diskussionspapiers erachtet werden, und eine Übernahme der Inhalte zielführend und nicht vermeidbar ist, sollte allenfalls ein (statischer) Verweis auf die jeweiligen Kriterien erfolgen und diese somit inkorporiert werden (Abschnitt 3.4).
 - Soweit Informationen bereits aufgrund anderer Kriterienkataloge objektiv und sachdienlich erfasst werden, etwa Lieferketten (Vendor Management), oder anwendbare Jurisdiktionen inklusive der implementierten Mitigationsmaßnahmen, so sollten die Kriterien des Diskussionspapiers die Öffentliche Verwaltung dahingehend ertüchtigen und messen, ob diese bereits bestehenden Kriterienkataloge bekannt und verwendet werden. Dies kann auch eine kritische Auseinandersetzung mit den jeweiligen Schwächen der existierenden Kriterienkataloge sein, mit der Folge, dass die Öffentliche Verwaltung diese Schwächen durch eigene, ergänzende Maßnahmen neutralisiert (Abschnitt 3.4).



- 95 ▪ Die Risikobetrachtung sollte eine eigene Dimension darstellen (Abschnitt 3.5).
- 96 ▪ Die Möglichkeit individueller Maßnahmen sollte aufrecht erhalten werden (Abschnitt 3.5).
- 97 ▪ Es wird empfohlen, die Dimension A stärker auf die nicht-technischen Aspekte einer orga-
98 nimatorischen Ertüchtigung zu fokussieren, und dabei die Erkenntnisse der weiteren
99 Dimensionen nutzbar zu machen (Abschnitt 4.1).
- 100 ▪ Es wird empfohlen, etwaige technische Aspekte entweder auf Basis der bereits entwickel-
101 ten weiteren Kriterienkataloge zu inkludieren, oder in eigene, noch zu entwickelnde Kriteri-
102 enkataloge auszulagern und hierdurch die Zielsetzung des Diskussionspapiers zu schär-
103 fen, und somit schnellere, und nachhaltigere Effekte zu erzielen (Abschnitt 4.1).
- 104 ▪ Generell wird für die weiteren Dimensionen (B bis D) empfohlen, Redundanzen zu reduzie-
105 ren, die Zielsetzung der Dimensionen zu schärfen, und im Ergebnis zunächst den Fokus
106 auf eine referenzielle Inklusion in Dimension A zu legen (Abschnitte 4.2, 4.3, 4.4).



2 Gegenstand der Stellungnahme und Struktur

107
108 Das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (**ZenDiS**) hat ein Diskussi-
109 onspapier zur Digitalen Souveränität der öffentlichen Verwaltung publiziert.

110 Das ZenDiS bittet um Stellungnahme. Das Diskussionspapier mit dem Titel „Kriterien für
111 Digitale Souveränität – aus messbar wird machbar“³ zielt darauf ab, Kriterien zu entwickeln,
112 die den Grad der Digitalen Souveränität in der Öffentlichen Verwaltung messbar machen.

113 Dem Diskussionspapier liegt die These zu Grunde, dass sich aus der „Messbarkeit“ eine
114 „Machbarkeit“ ergäbe oder jedenfalls erleichtere.⁴

115 Der Kriterienkatalog wurde nach eigener Angabe des ZenDiS während des Konsultationsphase
116 weiterentwickelt.⁵ Es ist aber nicht erkennbar, inwieweit dieser Workshop unmittelbare Ände-
117 rungen im Diskussionspapier zur Folge hatte. Insoweit bezieht sich diese Stellungnahme wei-
118 terhin auf das Diskussionspapier, Stand März 2026.

119 Während der dynamische und kollaborative Ansatz des ZenDiS positiv hervorzuheben ist, wäre
120 eine inhaltliche Änderung während einer Konsultationsphase auch nicht zielführend, da sich
121 die Stellungnahmen auf ein sich stets veränderndes Objekt bezögen und im Ergebnis keine
122 Vergleichbarkeit ermöglichten. Die Konsultationsphase erscheint hinreichend lang für eine
123 zielgerichtete Kommentierung und zugleich kurz genug, um eine dynamische und zeitnahe
124 Weiterentwicklung durch das ZenDiS zu ermöglichen.

125 Die Struktur der Stellungnahme gliedert sich in Allgemeine Anmerkungen (siehe Abschnitt 3)
126 und Spezifische Anmerkungen (siehe Abschnitt 4).

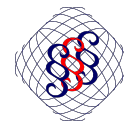
3 Abrufbar unter:

https://www.zendis.de/media/pages/newsroom/publikationen/konsultationsprozesskriterien/97c259289f-1774439296/zendis_diskussionspapier-kriterien-bewertung-digitaler-souveraenitaet.pdf

4 Siehe Kapitel 2 des Diskussionspapiers.

5 Siehe Hinweis auf einen Workshop vom 29. April 2026 auf <https://souveraenitaetscheck.de> mit Verweis auf die Ergebnisse unter

https://www.zendis.de/media/pages/newsroom/publikationen/konsultationsprozesskriterien/97c259289f-1774439296/zendis_diskussionspapier-kriterien-bewertung-digitaler-souveraenitaet.pdf



127 3 Allgemeine Anmerkungen

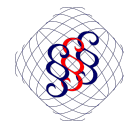
128 Allgemeine Anmerkungen beziehen sich auf strukturelle Überlegungen und adressieren somit
129 sowohl den generellen Ansatz des Diskussionspapiers sowie dessen Prämissen.

130 Eine erste abstrakte Einordnung des Diskussionspapiers durch den Autor erfolgte bereits zum
131 7. April 2026⁶. Diese Stellungnahme wird auf die dort genannten, ersten Eindrücke näher
132 eingehen.

133 Die Allgemeinen Anmerkungen beziehen sich unter anderem auf

- 134 ▪ **konzeptionelle Überlegungen** über die Potentiale von Kriterienkatalogen (siehe 3.1)
- 135 ▪ Klarheit bezüglich des **Gegenstands der Betrachtung** (siehe Abschnitt 3.2)
- 136 ▪ Existenz von und erforderliche **Klarheit bezüglich der Kriterien** (siehe Abschnitt 3.3)
- 137 ▪ **Synergiepotentiale** hinsichtlich anderer Souveränitätskriterien (siehe Abschnitt 3.4)
- 138 ▪ **Risikobetrachtung** (siehe Abschnitt 3.5)

6 Siehe *Ingenrieth*, ZenDiS calls for feedback on Digital Sovereignty Criteria - Reference and First Comment, <https://ingenrieth-online.de/de/aktuelles/detail/zendis-calls-for-feedback-on-digital-sovereignty-criteria-reference-and-first-comment>



139 3.1 konzeptionelle Überlegungen über die Potentiale von 140 Kriterienkatalogen

141 Zunächst ist zu klären, welches **Ziel der Kriterienkatalog verfolgt**. Hierzu sollten zunächst die
142 theoretischen Überlegungen der möglichen Konzepte bedacht werden und sodann auf die
143 ersichtliche Intention des Diskussionspapiers übertragen werden.

144 3.1.1 theoretische Optionen und Konzepte

145 Kriterienkataloge können unterschiedliche Zielrichtungen entfalten.⁷ Übergeordnetes Ziel ist
146 stets, die Konformität mit den Kriterien in einer vergleichbaren Form überprüfbar zu machen.
147 Hierbei kann das weitere Ziel sein, dass

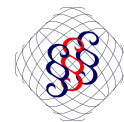
- 148 ■ eine **Eigenschaft zu einem bestimmten Zeitpunkt** bestätigt wird – etwa Produkt(-sicher-
149 heits-)zertifizierungen – und/oder sich aus diesem Umstand bestimmte Wahrscheinlich-
150 keiten einer Konformität für die Zukunft ableiten lassen – etwa in der Regel durch zertifi-
151 zierte Managementsysteme –
- 152 ■ eine **Aussage über eine Eigenschaft retrospektiv in einem bestimmten Zeitraum** getrof-
153 fen wird – in der Regel durch Audit-Programme, etwa SOC oder BSI C5.

154 Während eine Zertifizierung grundsätzlich binär pro Kriterium erfolgt (erfüllt, nicht erfüllt),
155 ermöglichen Auditberichte feingliedrige Feststellungen (erfüllt, erfüllt mit Abweichungen, nicht
156 erfüllt).

157 Neben den materiellen Anforderungen eines Kriterienkatalogs treten die prozeduralen Anforde-
158 rungen. Diese sind – im Sinne einer objektiven Vergleichbarkeit – mindestens genauso wichtig,
159 da diese unter Anderem die Unabhängigkeit und Vergleichbarkeit der Feststellungen
160 gewährleisten.

161 Neben die Kategorien der Zertifizierungen und Audits treten sogenannte **Reifegradmodelle**.
162 Hierbei werden (ungeprüfte) Eigenschaften entlang eines Gradienten verortet um letztlich eine
163 qualitative Aussage über den Prüfgegenstand zu treffen. Je höher der Reifegrad, umso höher
164 die „Reife“, also die „Qualität“, wobei sich die Aussage auf unterschiedliche Dimensionen
165 beziehen kann.

7 Siehe umfassend *Ingenrieth*, in Nink, StichwortKommentar Digitale Sicherheit, Zertifizierung, 2026.



166 3.1.2 Übertragung der Konzepte auf das Diskussionspapier

167 Die Wahl der konzeptionellen Ausgestaltung hängt von den erhofften Auswirkungen des Kriteri-
168 enkatalogs ab:

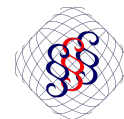
169 Eine **Momentaufnahme** (etwa „Produktzertifizierung“) erscheint für das Ziel einer Digitalen
170 Souveränität, die per definitionem eine Langzeitdimension und eine Zukunftsorientierung auf-
171 weist, **wenig zielführend**.

172 Die **Zertifizierung eines Managementprozesses** erscheint schon eher geeignet, aber weist
173 **relevante Schwächen** auf. Dies würde genügen, soweit es Ziel des Kriterienkatalogs wäre eine
174 „Souveränität per Checkbox“ zu erreichen. Allerdings dürfte eine solche Ausgestaltung der
175 Intention zuwiderlaufen, einem etwaigen Verwässern des Begriffs entgegenzutreten.⁸ Eine
176 Managementprozess-Zertifizierung könnte allenfalls sachdienlich sein, soweit hierbei sehr kon-
177 krete Kriterien und Leitlinien entwickelt würden, inklusive definierter Konsequenzen und Hand-
178 lungsalternativen. Eine derartige Granularität erscheint aber aufgrund der noch hoch-dynami-
179 schen Diskussionen bezüglich des Verständnisses von „Digitaler Souveränität“
180 höchst-herausfordernd.

181 Ist es Ziel des Kriterienkatalogs rückwirkend Missstände und Herausforderungen zu erkennen
182 und somit für die Zukunft Entwicklungspotentiale aufzuzeigen und in adaptierten Kriterien
183 nutzbar zu machen, erscheint es **zielführend, ein Audit-Programm zu entwickeln**. Audit-
184 Programme orientieren sich eher an „Dimensionen/Objectives“ und erlauben die Ausarbeitung
185 konkreter interner Kriterien bezogen auf den jeweiligen konkreten Prüfgegenstand. Hierbei
186 ist es systemimmanent, dass ein Audit Schwachstellen aufdeckt und Entwicklungspotentiale
187 aufzeigt. Entlang dieser Erkenntnisse werden sodann die internen Kriterien beständig
188 modifiziert und optimiert. Die hohe Individualität der internen Kriterien ermöglicht einerseits
189 eine hohe Flexibilität und potentielle Breitenwirkung. Andererseits **erschwert es eine**
190 **Vergleichbarkeit** der jeweils bewerteten, individuellen Prüfgegenstände.

191 Unter Berücksichtigung des erklärten Ziels, eine **Vergleichbarkeit schnell und mit verhältnis-**
192 **mäßigem Aufwand herzustellen, erscheint ein Reifegradmodell sachdienlich**. Der Kriterien-
193 katalog würde die bestehenden, diversen Herangehensweisen systematisieren und in eine die
194 Vergleichbarkeit fördernde Matrix überführen. Soweit neben der Vergleichbarkeit kurz- oder
195 mittelfristig auch eine Verlässlichkeit und Objektivität der Aussagen erzielt werden soll, **können**
196 **Reifegradmodelle mit anderen Formen der Zertifizierung und Auditierung kombiniert wer-**
197 **den**. In diesem Falle müssen alle oder einzelne Aspekte für die Erreichung eines bestimmten
198 Reifegrads durch Prüfberichte nachgewiesen werden.

8 Siehe Kapitel 2, S. 6 Diskussionspapier.



199 Eine Reifegradmodell hätte zu dem den Vorteil, dass der Kriterienkatalog zumindest vorerst die
200 **Prozeduralen Aspekte vermeiden** kann. Gerade die das Prüfverfahren betreffenden Aspekte
201 stellen häufig einen mindestens genauso umfangreichen, wenn nicht sogar umfangreicheren
202 Anteil der Konformitätsprogramme dar.

203 **Empfehlung 1:** Es wird empfohlen den Kriterienkatalog als Reifegradmodell auszubauen.

204 Das Reifegradmodell ermöglicht es die Vielzahl der sachdienlichen Maßnahmen zur
205 Erreichung einer Digitalen Souveränität zu systematisieren. Durch ein Reifegradmodell
206 wird eine **Bewertung einer Konformität im Sinne des „richtig / falsch“ vermieden**.
207 Insoweit besteht ein geringeres Risiko der Ablehnung durch Verantwortliche und
208 einzelnen Sektoren, nur weil einzelne Wertungen nicht geteilt werden oder die
209 Umsetzung dessen abgelehnt wird. Zudem sind **hohe Mitnahme-Effekte** zu erwarten.
210 Die Verantwortlichen für die Implementierung und Steuerung werden nicht dem
211 unnötigen Eindruck eigener Schlechtleistung unterworfen, während ihnen zugleich –
212 aufgrund der möglichen Feingliedrigkeit der Aspekte – unmittelbare und leicht
213 implementierbare Verbesserungen an die Hand gegeben werden. Gerade in hoch-
214 interdependenten Themen, wie der Digitalen Souveränität, ist ein Handlungshemmnis
215 die vermeintliche „Größe“ der zu bewältigen Aufgabe. Eine **durch das Reifegrad-**
216 **Modell angeleitete Aufteilung in (kleinst-)Projekte kann derartige Hemmnisse bei**
217 **den Verantwortlichen überwinden**. Zugleich erleichtert es die Kommunikation,
218 Präsentation und Finanzierung im Rahmen von internen Freigabeprozessen, da die
219 Maßnahmen und die Auswirkungen greifbarer werden.

220 **Empfehlung 2:** Es wird empfohlen den Kriterienkatalog als offenes Reifegradmodell
221 auszugestalten.⁹

222 Obgleich sich in vielen Bereichen eine Dreistufigkeit (low/basic, essential, high) eta-
223 bliert, wird von einer derartigen Ausgestaltung im Reifegradmodell für Digitale Souverä-
224 nität abgeraten.

225 Der Begriff der Digitalen Souveränität ist höchst-dynamisch. Die in Rede stehenden
226 Maßnahmen und Kriterien sind interdependent und somit von unterschiedlichen Inter-
227 essen geleitet. Es wird daher bereits eine Herausforderung darstellen, je Dimension
228 einzelne Umstände hierarchisch in einen Reifegradgradienten zu überführen. Müssten
229 sich diese Aspekte zudem in **definierte Stufen eingliedern, droht dies erheblichen**

9 „Offene Reifegradmodelle“ zeichnen sich dadurch aus, dass je Dimension/Objective unterschiedlich viele Aspekten existieren können und sich diese Aspekte nicht in ein vordefiniertes Schema von Reifestufen eingliedern müssen; vgl. exemplarisch das „Reifegradmodell zur Abbildung von technisch-organisatorischen Maßnahmen bei der Auftragsverarbeitung“, entwickelt und herausgegeben durch bitkom in 2024. Das Modell zeigt zudem auch auf, wie externe Validierungen in ein Reifegradmodell eingebunden werden können. abrufbar unter <https://www.bitkom.org/sites/main/files/2024-11/241104-LF-Datenschutz-Reifegradmodell-Bitkom.pdf>.



230 **Blockade-Haltungen zu begegnen.** Derartige Stufen würden letztlich den Vorteil eines
231 an sich wertungsneutralen Reifegrad-Modells zu Nichte machen. Vielmehr würde der
232 **Eindruck** entstehen, dass durch bestimmte Reifegradstufen bereits **korrespondie-**
233 **rende „Konformitäten“** erreicht seien. Es ist aus der Erfahrung mit ähnlich gelagerten
234 Vorhaben zu erwarten, dass **Stakeholder auf solche Automatismen hinwirken**
235 würden.

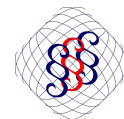
236 Im Ergebnis würden bei einer vorgegebenen (Drei-)Stufigkeit Chancen verloren gehen,
237 jedenfalls (1) eine ergebnisoffene Sammlung von Maßnahmen und (2) ein Fokus auf
238 Effektivität und objektive Vergleichbarkeit.

239 Stakeholder werden im Falle eines engen und zu erwartenden Konformitätskorsetts
240 nicht gewillt sein, ergebnisoffen Maßnahmen vorzutragen. Diese Zurückhaltung begrün-
241 det sich etwa weil einzelne Maßnahme eventuell aus anderen Überlegungen als der
242 Digitalen Souveränität umstritten sind¹⁰, (hohe oder anderenfalls entfallene) Aufwände
243 bedeuten würden, oder lediglich in besonderen Konstellationen¹¹ erforderlich scheinen.
244 Allerdings ist diese **Offenheit gerade die Intention eines Reifegrad-Modells.** Die
245 Aspekte werden entlang eines Gradienten verortet entsprechend der erwarteten positi-
246 ven Auswirkungen. Es ist dann Aufgabe derjenigen, die den **konkreten Einsatzzweck**
247 kennen, die erforderliche „Reife“ je Dimension anhand der **eigenen Risiko- und Anfor-**
248 **derungsanalyse** zu definieren. Da es gerade keinen Automatismus zur Konformität
249 oder zu einer Implementierungspflicht gibt, können Reifegradmodelle ohne unmittel-
250 bare Konsequenzen auch höchst seltene, ausgefallene oder aufwändige Maßnahmen
251 aufnehmen und somit den (gedanklichen und entwicklungstechnischen) Rahmen und
252 Ausblick auf mögliche künftige Optionen aufzeigen.

253 **Fehlt eine solche Ergebnisoffenheit** können andere Überlegungen überwiegen, die
254 dazu führen könnten, dass am Ende lediglich die Erreichbarkeit einer bestimmten „**Rei-**
255 **fegradstufe“ durch die Mehrheit der etablierten Stakeholder** garantiert ist. Diese
256 könnten sodann leicht die relevante Stufe erreichen, und im Falle etwaiger Automatis-
257 men resultiert der Kriterienkatalog dann in einer möglichen **Verwässerung des**
258 **Begriffs der Digitalen Souveränität.** Denn in diesem Falle stünde nicht mehr die im
259 konkreten Anwendungsfall erforderliche Effektivität im Fokus, sondern ausschließlich
260 die Absicherung der eigenen Verantwortlichkeiten durch **Nachweise der richtigen**
261 **„Checkbox“.**

10 Etwa, weil diese nicht von eigenen Produkten bereits umgesetzt sind, weil diese möglicherweise Konkurrenten eher befähigt, oder in Widerspruch zu bisherigen politischen oder werblichen Aussagen stehen.

11 Z.B. in höchst-sensiblen Kontexten der nationalen Sicherheit.



262 3.2 Klarheit bezüglich des Gegenstands der Betrachtung

263 Derzeit ist nicht klar, was Gegenstand der Betrachtung (**Prüfgegenstand**) des Kriterienkatalogs
264 sein soll. Einerseits weist das Diskussionspapier daraufhin, dass gerade nicht einzelne Pro-
265 dukte oder Systeme betrachtet werden sollen, sondern die Öffentliche Verwaltung als Ganzes,
266 inklusive des gesamten digitalen Stacks.

267 Gleichzeitig soll die Öffentliche Verwaltung (durch den Kriterienkatalog) in die Lage versetzt
268 werden, IT-Lösungen, Komponenten und Anbieter flexibel auszuwählen und bei Bedarf mit ver-
269 tretbarem Aufwand zu wechseln.¹²

270 Hierbei sollte zunächst klar sein, was die Zielsetzung des Kriterienkatalogs ist. Es ist auch vor-
271 stellbar, dass es mehrere Zielsetzungen bereits hinsichtlich des Prüfgegenstands gibt. In die-
272 sem Falle sollte der Kriterienkatalog in unterschiedliche Kataloge bzw. Sub-Kataloge aufgeteilt
273 werden.

274 **Empfehlung:** Es wird empfohlen, die Zielsetzung des Kriterienkatalogs zu klären und die
275 Dimensionen und Kriterien streng anhand dieser Zielsetzung auszugestalten.

276 Bestehen Unwägbarkeiten hinsichtlich der Zielsetzung wird dies die weitere Entwick-
277 lung verzögern, da unterschiedliche Stakeholder die Unwägbarkeiten nutzen könnten,
278 um deren eigenen Interessen zu sichern.

279 3.3 Existenz von und erforderliche Klarheit bezüglich der 280 Kriterien

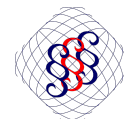
281 Bisher weist das Diskussionspapier lediglich Dimensionen, allenfalls Objectives auf. Konkrete
282 Kriterien sind nicht ersichtlich, geschweige denn Empfehlungen oder Beispiele zu den
283 Kriterien.¹³

284 Inwieweit die konkreten Dimensionen bzw. Objectives geeignet sind bzw. ergänzt werden
285 müssten, hängt von dem beabsichtigten Prüfgegenstand ab. Im weiteren wird als Prüfgegen-
286 stand die Öffentliche Verwaltung beziehungsweise derer Organisationseinheiten vorausgesetzt.

287 **Empfehlung:** Für eine objektive und vergleichbare Erfassung der Umstände müssten die
288 Dimensionen und die Objectives in konkrete Kriterien überführt werden. Aufgrund der hohen
289 Dynamik sollte hierbei insbesondere auch auf ergänzende Erläuterungen zurückgegriffen wer-
290 den, inklusive Beispielen und Empfehlungen.

12 Kapitel 3, S. 9 Diskussionspapier.

13 Weitergehend zu den Begrifflichkeiten *Ingenrieth*, in Nink, StichwortKommentar Digitale Sicherheit, Zertifizie-
rung, 2026.



291 3.4 Synergiepotentiale zu anderen Souveränitätskriterien

292 Es ist zu begrüßen, dass das Diskussionspapier die Kriterien des European Cloud Sovereignty
293 Framework (**EU CSF**)¹⁴ sowie die BSI Criteria Enabling Cloud Computing Autonomy (**BSI C3A**)¹⁵
294 in Bezug nimmt. Generell sollte sichergestellt werden, dass eine sachdienliche Kompatibilität
295 aufrecht erhalten wird.

296 Insoweit ist ebenfalls auf den Prüfgegenstand abzustellen. Das EU CSF und die BSI C3A-Krite-
297 rien stellen im Wesentlichen die jeweiligen Digitalen Dienste in den Fokus. Das Diskussions-
298 papier scheint aber sehr bewusst einen anderen Fokus setzen zu wollen. Soweit die **Fähigkei-**
299 **ten und Implementierungsfortschritte der Öffentlichen Verwaltung** betrachtet werden sollen,
300 erscheinen das EU CSF und die BSI C3A-Kriterien nicht geeignet.

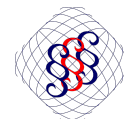
301 Es erscheint indessen **höchst sachdienlich, mit dem Diskussionspapier einen anderen Fokus**
302 **zu setzen**. Nicht alle Fachverfahren und digitalen Prozesse, inklusive der damit verbundenen
303 Datenverarbeitung, Speicher- und Netzwerkinfrastruktur, sind durch oder müssen durch Cloud-
304 Dienste realisiert werden. Jedwede **Prozesse und Infrastruktur, die nicht über Cloud-Dienste**
305 **realisiert werden, verblieben somit in einem „Blinden Fleck“**. Hierzu zählen auch etwaige
306 (mobile) Endgeräte und deren Firmware, Betriebssysteme und sonstiger Software. Auch
307 digitale Gebäude- und Bereichssicherungssysteme sind möglicherweise digitale Verfahren.
308 Diese kurze Darstellung zeigt bereits, warum die Kriterien-Kataloge mit reinem Cloud-Fokus
309 einer Ergänzung bedürfen.

310 Zugleich erscheint es nicht sachdienlich, in angemessener Zeit, einen Rundumschlag zu reali-
311 sieren. Vielmehr wirkt es förderlicher und effizienter, die Zielrichtungen der Prüfgegenstände
312 strikt zu trennen und hierdurch ein **Souveränitäts-Netz** zu spannen. Einzelne Dimensionen
313 können sich somit sowohl **horizontal ergänzen, als auch vertikal aufeinander aufbauen**.

314 Hierdurch ergeben sich allgemeine Anforderungen an die Informationsbeschaffung, Dokumen-
315 tation sowie hinsichtlich der Fertigkeiten der Öffentlichen Verwaltung. Hierbei umfassen die
316 Fertigkeiten die finanziellen und sachlichen Ressourcen, und das notwendige Fachwissen die
317 sachlichen Ressourcen sachdienlich einzusetzen und eine **angemessene und unabhängige**
318 **Risikoanalyse** durchführen zu können.

14 https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?file-name=Cloud-Sovereignty-Framework.pdf

15 Download at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/C3A_Cloud_Computing_Autonomy.pdf; First analysis, e.g. *Ingenieth*, BSI C3A:v1 on Cloud Autonomy published by Federal Office for Information Security : <https://ingenieth-online.de/de/aktuelles/detail/bsi-c3av1-on-cloud-autonomy-published-by-federal-office-for-information-security>



319 **Empfehlung 1:** Es sollte deutlich(er) herausgearbeitet werden, wie durch den Kriterienkatalog
320 die Aspekte der Digitalen Souveränität ergänzt werden.

321 **Empfehlung 2:** Es sollte auf unnötige Redundanzen verzichtet werden, da diese letztlich zu
322 einer vermeidbaren Hürde bei der Implementierung führen. Redundanzen lösen – auch unge-
323 wollt – Auslegungskonflikte aus, insbesondere soweit die Redundanz nicht wort- und kontexti-
324 dentisch ist.

325 **Empfehlung 3:** Wenn und soweit Elemente des EU CSG oder der BSI C3A für förderlich aus
326 Sicht des Diskussionspapiers erachtet werden, und eine Übernahme der Inhalte zielführend
327 und nicht vermeidbar ist, sollte allenfalls ein (statischer) Verweis auf die jeweiligen Kriterien
328 erfolgen und diese somit inkorporiert werden.

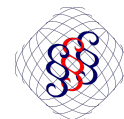
329 **Empfehlung 4:** Soweit Informationen bereits aufgrund anderer Kriterienkataloge objektiv und
330 sachdienlich erfasst werden, etwa Lieferketten (Vendor Management), oder anwendbare Juris-
331 diktionen inklusive der implementierten Mitigationsmaßnahmen, so sollten die Kriterien des
332 Diskussionspapiers die Öffentliche Verwaltung dahingehend ertüchtigen und messen, ob diese
333 bereits bestehenden Kriterienkataloge bekannt und verwendet werden. Dies kann auch eine
334 kritische Auseinandersetzung mit den jeweiligen Schwächen der existierenden Kriterienkata-
335 loge sein, mit der Folge, dass die Öffentliche Verwaltung diese Schwächen durch eigene, ergän-
336 zende Maßnahmen neutralisiert.

337 3.5 Risikobetrachtung

338 Positiv ist hervorzuheben, dass das Diskussionspapier die Diversität der zugrundeliegenden
339 Sachverhalte anerkennt. Soll die Effektivität in den Fokus gestellt werden, erscheint eine kon-
340 zeptionell individualisierte Vorgehensweise nachvollziehbar.

341 Es ist zu beachten, dass eine **konzeptionelle Individualisierung** trotzdem einen **hohen Grad**
342 **an Synergien** ermöglicht. Hierzu sollte parallel zu den Kriterien ein interner Austausch der Ver-
343 antwortlichen in der Öffentlichen Verwaltung etabliert werden. Ein solcher Austausch kann –
344 und sollte – die jeweils getroffenen Maßnahmen dokumentieren und für andere zugänglich
345 machen. Die so gewonnenen „good practices“ ermöglichen letztlich einen hohen Effizienz-
346 gewinn auf Basis einer de facto Standardisierung, erhält aber den hohen Grad der individuel-
347 len Flexibilität.

348 Ein zu hoher – **zentral vorgegebener – Grad der Standardisierung könnte der Digitalen Sou-**
349 **veränität auch zuwiderlaufen.** Souveränität ist in erster Linie die Fähigkeit, eigenständig in
350 Kenntnis der Umstände entscheiden zu können. Faktische Abhängigkeiten entstehen insbe-
351 sondere, wenn einzelne Lösungen und Maßnahmen auf Ebene der Implementierung so
352 dominant werden, dass diese als „too big/important to fail“ gelten. Eine **zentrale**



353 **Standardisierung von Maßnahmen fördert derartige Dominanzen.** Im Ergebnis könnte somit
354 eine Abhängigkeit A lediglich in eine Abhängigkeit B verlagert werden. Die Möglichkeit individu-
355 elle Maßnahmen implementieren zu können, erscheint daher ein zentraler Aspekt, die notwen-
356 dige Diversität der getroffenen Maßnahmen zu erreichen. Eine **Diversität der getroffenen**
357 **Maßnahmen** ermöglicht zudem auch einen **Vergleich der Maßnahmen** und der sich aus der
358 Maßnahme ergebenden **Potentiale**. Diese vielfältigen Erfahrungen können wiederum für die
359 Weiterentwicklung und Optimierung der individuellen Maßnahmen genutzt werden.

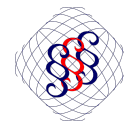
360 **Empfehlung 1:** Die Risikobetrachtung sollte eine eigene Dimension darstellen.

361 Es ist zwar zutreffend, dass die Risiken sich über die jeweiligen Dimensionen – auch –
362 als Querschnittsmaterie realisieren, jedoch existieren vorgelagert wichtige Aspekte, die
363 sichergestellt werden sollten. Dies betrifft etwa die Fähigkeiten und Maßnahmen, Risi-
364 ken erkennen und bewerten zu können, die etwaige kaskadierte kollateral-Folgen
365 erkennen zu können oder eben die (un-)mittelbaren Auswirkungen durch Sicherungs-
366 maßnahmen in nachgelagerten Verfahren adressieren zu können.

367 **Empfehlung 2:** Die Möglichkeit individueller Maßnahmen sollte aufrecht erhalten werden.

368 Die hierdurch mögliche Diversität erhöht den Erfahrungsgewinn, der wiederum in alle
369 Maßnahmen ausstrahlt. Zudem birgt eine zu große Standardisierung das inhärente
370 Risiko, dass am Ende eine Abhängigkeit von der standardisierten Maßnahme etabliert
371 wird.¹⁶

16 Sicherheitstechnische Betrachtungen bleiben vorliegend außer Acht. Standardisierung ist stets auch aus einer sicherheitstechnischen Betrachtung in einem Spannungsfeld: einerseits erleichtert die Standardisierung die Aufrechterhaltung eines hohen Niveaus in der Fläche; andererseits vergrößert Standardisierung auch den Angriffsvektor, soweit eine Lücke in der Sicherheitsarchitektur erkannt wird, da Angreifer diese nun flächen-deckend vorfinden.



372 4 Spezifische Anmerkungen

373 Spezifische Anmerkungen beziehen sich auf die Elemente der jeweiligen Dimensionen, soweit
374 dies nicht bereits Gegenstand der allgemeinen Betrachtung war.

375 Hierbei sind zwei Prämissen besonders wichtig:

- 376 ■ entwickelt sich das Diskussionspapier zu einem offenen Reifegradmodell, stellen die zu
377 entwickelnden Kriterien lediglich individuelle Aspekte der Reife dar;
- 378 ■ verbleibt das Diskussionspapier in einem Konzept der (binären) Konformität, so sollten die
379 Kriterien in ihrer Struktur optimiert und weiter systematisiert werden.

380 Hierbei sind auch Kombinationen möglich, wobei es oberste Priorität sein muss, die Zielset-
381 zung des Kriterienkatalogs zu schärfen.

382 4.1 Dimension A

383 Die Dimension A erscheint sachdienlich und die primäre Dimension zur Ertüchtigung der
384 Öffentlichen Verwaltung.

385 Es erscheint sachdienlich, die weiteren – teils technischen – Dimensionen stärker an die
386 Dimension A anzubinden.

387 Der Prüfgegenstand ist bisher unklar. Die Digitale Souveränität der Verwaltung für den gesam-
388 ten Stack inkludiert sowohl die technische Dimension als auch die organisatorische
389 Dimension.

390 Wie bereits zuvor erwähnt, erscheint der Kriterienkatalog alle Dimensionen und Aspekte des
391 digitalen Stacks zu umfassen. Sowohl die Erstellung, als auch die weitere Pflege würde enorme
392 Ressourcen beanspruchen. Die Vermischung der Prüfgegenstände würde zudem zu einer Ver-
393 wässerung der Zielsetzungen führen, da neben einem Fokus auf Digitale Souveränität andere
394 **politische und wirtschaftliche Überlegungen** die Entwicklung beeinflussen könnten.

395 Eine solche **Verwässerung und Ablenkung** kann **ergebnisorientierter begegnet** werden, wenn
396 der **Prüfgegenstand klar und fokussiert** ist.

397 Insofern ist es unbenommen, dass auch technische Aspekte entlang des digitalen Stacks der
398 Öffentlichen Verwaltung betrachtet werden müssen. Die jetzige Ausgestaltung und Zielsetzung
399 des Diskussionspapiers scheint es aber aufzudrängen, diese technische Betrachtung auszula-
400 gern in eigene Kriterienkataloge.



401 Konzeptionell würde somit die Dimension A bedeuten:

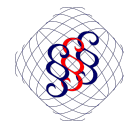
- 402 ▪ Aufbau und Erhalt von **(Fach-)Expertise**
- 403 ▪ Aufbau und Erhalt von **Erkenntnis- und Dokumentationsverfahren**
- 404 ▪ Aufbau und Erhalt von **Evaluations- und Reaktionsmechanismen**
- 405 ▪ Aufbau und Erhalt von **Beschaffungs- und Entscheidungsstrukturen** zum Aufbau und
- 406 Erhalt digitaler Souveränität
- 407 ▪ Aufbau und Erhalt von (internen) **Austauschplattformen** zur Entwicklung und Weitergabe
- 408 von „good practises“ im Rahmen genutzter Mechanismen
- 409 ▪ Aufbau und Erhalt übergeordneter **Transparenzstrukturen** zur Vermeidung ungewollter
- 410 und indirekter Abhängigkeiten
- 411 ▪ Aufbau und Erhalt von **Experimentalverfahren und Sprint-Umgebungen**

412 Soweit Fachexpertise betroffen ist, kann diese in unterschiedlicher Granularität erforderlich
413 sein und sollte somit auch graduell ertüchtigt werden. Die notwendige Fachexpertise reicht von
414 verständigem Bewusstsein bis hin zu der Fähigkeit, eigene (technische) Elemente eigenständig
415 und autonom entwickeln zu können. **Entlang dieses Gradienten können auch ergänzende**
416 **Kriterienkataloge unterstützen.** Insoweit ist es Teil der Ertüchtigung der Öffentlichen Verwal-
417 tung, diese Kriterienkataloge bekannt zu machen, die Vor- und Nachteile zu kennen, und letzt-
418 lich in angemessenen Umfang bei eigenen Entscheidungen und der Beschaffung zu
419 berücksichtigen.¹⁷

420 Insbesondere erscheint neben der individuellen Fachexpertise eine **Überwindung der Silo-**
421 **Strukturen** erforderlich. Einerseits beschleunigt ein Fachaustausch die Ertüchtigung, da die
422 Fachbereiche aus wechselseitigen Erfahrungen eigene Entscheidungen ableiten können. Es
423 kann von einem hohen Synergiepotential ausgegangen werden. Zudem kann hierdurch vermie-
424 den werden, dass sich **(ungewollt und indirekt) entlang des digitalen Stacks einzelne**
425 **digitale Dienste verdichten** und somit zu einer unbeabsichtigten, **schleichenden Abhängig-**
426 **keit** führen.

427 Diese **Synergien** gehen einher mit der **positiven Konnotation**, dass auch fremde Fachbereiche
428 sachdienliche und ggf. optimierte Mechanismen etabliert haben können, deren **Übertragung**
429 **auf die eigenen Fachverfahren** förderlich ist. Hierzu erscheint es sachdienlich, die Gemein-
430 samkeiten der Verfahren in den Mittelpunkt der Betrachtung zu stellen, und auf deren Basis
431 modular die Besonderheiten zu adressieren. Hierzu erscheint es konzeptionell förderlich, dass

17 Zu relevanten Fragen bei der Bewertung und Evaluation von (externen) Prüfverfahren, siehe auch *Ingenrieth*, in Nink, StichwortKommentar Digitale Sicherheit, Zertifizierung, 2026. Zu relevanten Fragen wie die Unabhängigkeit bzw. das Gleichgewicht der berücksichtigten Interessen ermittelt werden kann, siehe etwa *Ingenrieth*, in Nink, StichwortKommentar Digitale Sicherheit, Ko-Regulierung, 2026.



432 auch die **Vorteile einer dynamischen Entwicklung** in den Vordergrund gestellt werden. Im
433 Falle einer **sachdienlichen Trennung der Hintergrundprozesse und Hintergrundsysteme von**
434 **deren Bedienungsoberflächen** führt eine Umstellung dieser Hintergrundprozesse zu geringen
435 bis keinen Schulungsbedarfen der Endnutzer*Innen.

436 Die obig genannten Aspekte der Dimension A können zudem sehr gut in Reifegraden darge-
437 stellt werden.

438 **Empfehlung 1:** Es wird empfohlen, die Dimension A stärker auf die nicht-technischen Aspekte
439 einer organisatorischen Ertüchtigung zu fokussieren, und dabei die Erkenntnisse der weiteren
440 Dimensionen nutzbar zu machen.

441 **Empfehlung 2:** Es wird empfohlen, etwaige technische Aspekte entweder auf Basis der bereits
442 entwickelten weiteren Kriterienkataloge zu inkludieren, oder in eigene, noch zu entwickelnde
443 Kriterienkataloge auszulagern und hierdurch die Zielsetzung des Diskussionspapiers zu schär-
444 fen, und somit schnellere, und nachhaltigere Effekte zu erzielen.

445 4.2 Dimension B

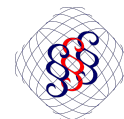
446 Insgesamt wirkt diese Dimension **teils redundant und in sich un schlüssig**, obgleich die einzel-
447 nen Elemente einer Digitalen Souveränität zuträglich sein können.

448 So erscheint „Transparenz und Dokumentation“ Redundant zur Dimension A der IT-Gover-
449 nance und des Managements. Die Dokumentation und Transparenz ist hierzu eine *conditio*
450 *sine qua non*. Dies gilt auch für ein Risikomanagement. Ohne Kenntnis der Umstände ist ein
451 Risikomanagement nicht zielführend. Dies inkludiert auch die Dokumentation über getroffene
452 Entscheidungen und die damit verbundenen, akzeptierten Risiken. Denn nur so können künf-
453 tige Entscheidungen nachhaltig und verständlich getroffen werden.

454 Soweit Dimension B technische Aspekte betrifft, sollte dies in eine Fähigkeits- und Berücksich-
455 tungsmatrix überführt werden, während die eigentlichen technischen Aspekte in kontextuali-
456 sierte Kriterienkataloge überführt werden.

457 Hierbei ist zu beachten, dass die Fähigkeits- und Berücksichtigungsmatrix sehr gut in ein Reife-
458 gradmodell überführt werden kann. Technische Aspekte, je nach deren Detailgrad, erscheinen
459 sachdienlicher in konkreten Konformitätsprogrammen. Obgleich auch in diesem Kontext sind
460 Reifegrade vorstellbar.

461 Soweit auf **Standards und Schnittstellen** abgestellt wird, sollte der Kriterienkatalog klarstel-
462 len, was hierdurch adressiert werden soll. Positiv ist sicherlich, wenn die Öffentliche Verwal-
463 tung deren **digitale Verfahren stärker in Modulen organisiert** und den **Austausch von Inhal-**
464 **ten stärker über Schnittstellen** realisiert. Im Sinne der Organisations- und



465 (Weiter-)Entwicklungscompetenzen erscheint ein **Fokus auf Open Source nahe liegend**. Hier-
466 bei sollte aber unterschieden werden, was durch Open Source tatsächlich erreicht werden
467 kann. **Automatismen hinsichtlich der positiven Bewertung von Open Source sollten vermie-**
468 **den werden**. Ein „öffentlich verfügbarer Source Code“ bedeutet nicht notwendigerweise, volle
469 Nutzungs- und Verwertungsrechte. Umgekehrt verlangen umfassende Nutzungs- und Verwer-
470 tungsrechte nicht die Veröffentlichung des Source Codes.

471 **Empfehlung:** Redundanzen reduzieren, Zielsetzung der Dimension schärfen, und im Ergebnis
472 zunächst den Fokus auf eine referenzielle Inklusion in Dimension A legen.

473 4.3 Dimension C

474 Diese Dimension beschäftigt sich mit der Perspektive „Daten“. Auch hier sind teilweise Redun-
475 danzen erkennbar.

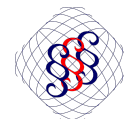
476 Die Datenstruktur ist eng mit der Entwicklung und Ausgestaltung von (Daten-)Schnittstellen
477 verbunden.

478 Die Datensicherheit wird in der Regel durch IT-Sicherheitskriterien adressiert. Insoweit sollte
479 klargestellt werden, **an welchen Stellen die durch das Diskussionspapier angedachten Krite-**
480 **rien gegenüber den etablierten IT-Sicherheitsstandards einen Mehrwert bieten**. Denkbar
481 erscheint auch hier ein Rückgriff auf die Dimension A dahingehend, dass die Verantwortlichen
482 in der Öffentlichen Verwaltung ertüchtigt werden, die etablierten Standards sowohl zu kennen,
483 als auch deren Aussagen in den eigenen Entscheidungen verständlich einfließen zu lassen.

484 Soweit **Datenlokation** betroffen ist, sollte klargestellt werden, dass bei einer Verarbeitung von
485 Daten in öffentlichen Netzen, bzw. in Netzen, die eine Anbindung an öffentliche Netze haben,
486 die **Lokation nur eine sekundäre Sicherheit** bietet. Eine Verarbeitung „in Europa“ garantiert
487 nicht, dass die hiesigen Rechtsnormen eingehalten werden. Es erleichtert allenfalls deren
488 Durchsetzung. Zugleich ist eine Datenlokation außerhalb von Europa nicht gleichzusetzen mit
489 einem garantierten Missbrauch der Daten durch Dritte.

490 Es sollte hierbei eine **differenzierte und zielorientierte Betrachtung** stattfinden. Eine räumli-
491 che Konzentration der digitalen Dienste erhöht das Risiko eines Single-Point-Of-Failures. Das
492 gleiche gilt für die Nationalitäten und Wohnsitze der mit der Datenverarbeitung betrauten Per-
493 sonen. Beide Aspekte sind ein **ungeeigneter Proxy und eine Verwässerung einer effektiven**
494 **Risikomitigation**. Das Risiko ist der Single-Point-Of-Failure. Der Proxy verleitet zu einer Risiko-
495 Ignoranz aufgrund einer positiven „Checkbox“.¹⁸ Die Intention des Diskussionspapiers,

18 Siehe hierzu etwa die initiale Analyse der BSI C3A Kriterien, *Ingenieth*, BSI C3A:v1 on Cloud Autonomy publis-
hed by Federal Office for Information Security,
<https://ingenieth-online.de/de/aktuelles/detail/bsi-c3av1-on-cloud-autonomy-published-by-federal-office-for-information-security>.



496 derartigen **Verwässerungen und Fehlanreizen entgegenzuwirken**, sollte durch eine sachdien-
497 liche Schärfung des Regelungsziels und der damit verbundenen Kriterien und Erwartungen
498 befördert und effektuiert werden.

499 **Empfehlung:** Redundanzen reduzieren, Zielsetzung der Dimension schärfen, und im Ergebnis
500 zunächst den Fokus auf eine referenzielle Inklusion in Dimension A legen.

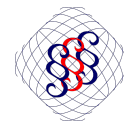
501 4.4 Dimension D

502 Hierbei sind einige Redundanzen mit den weiteren Dimensionen festzustellen.

503 Datenschutz inkludiert Datensicherheit und IT-Sicherheit, wobei hierdurch auch zwingend Über-
504 legungen im Bereich des Business Continuity Managements und sowie der Sicherheit und
505 Compliance im Betrieb anzustellen sind.

506 Denkbar erscheint eine **Schärfung der Dimension**, oder eine **referenzielle Inklusion** in andere
507 Dimensionen. Letzteres wäre dem primären Zweck des Diskussionspapier förderlich und
508 könnte in ein Reifegradmodell überführt werden. Die weiteren, detaillierten Anforderungen
509 wären in diesem Fall in ergänzenden Kriterienkatalogen und Konformitätsbewertungsprogram-
510 men zu etablieren und zu pflegen.

511 **Empfehlung:** Redundanzen reduzieren, Zielsetzung der Dimension schärfen, und im Ergebnis
512 zunächst den Fokus auf eine referenzielle Inklusion in Dimension A legen.



513 5 Fazit

514 Das Diskussionspapier liefert einen guten Überblick über den aktuellen Sachstand bezüglich
515 der „Digitalen Souveränität“. Die Definition des Begriffs ist nach wie vor nicht abgeschlossen
516 und somit ist auch eine Entwicklung von klaren Kriterien schwierig.

517 Der **Dynamik des Themenfelds** geschuldet, erscheint es somit sachdienlich, zunächst eine
518 **ergebnisoffene und wertungsneutrale Matrix** zu entwickeln, etwa in Form eines
519 Reifegradmodells.

520 Aus dem **Reifegradmodell** können sodann konkrete Anforderungen (Reifegrade) für bestimmte
521 **horizontale oder vertikale Anwendungsfälle** extrahiert werden.

522 Wichtig erscheint, dass sich der zu entwickelnde Kriterienkatalog einerseits in die Logik der
523 bereits anderweitig ausgearbeiteten Kriterienkataloge einbinden lässt. Andererseits erscheint
524 es sachdienlich, die **Effektivität und Individualität** aufrecht zu erhalten.

525 Ebenfalls erscheint ein konkreter Bedarf gegeben, da die bisherigen Kriterienkataloge entwe-
526 der nur einen Ausschnitt der digitalen Dienste bzw. des digitalen Stacks der Öffentlichen Ver-
527 waltung abbilden; oder weil die bisherigen Kriterienkataloge eine Verwässerung der Effektivität
528 und der eigenen, verständigen Entscheidung befördern könnten.

529 Hierbei sollte insbesondere darauf geachtet werden, **Fehlanreize und Fehlwirkungen zu ver-**
530 **meiden**. Zugleich sollte vermieden werden, Verantwortliche in der Verwaltung dem Anschein
531 anzusetzen, dass diese bisher ausschließlich fehlerhafte Entscheidungen getroffen haben.
532 Stattdessen sollten die Kriterien und das empfohlene Format eines offenen Reifegradmodells
533 eine **selbstkritische aber ansonsten wertungsneutrale Auseinandersetzung mit dem Status**
534 **Quo** ermöglichen und zugleich **niederschwellige Entwicklungs- und Optimierungspotentiale**
535 **aufzeigen**. Eine **konsistente und kontinuierliche Berücksichtigung** der Entscheidungsdimen-
536 sion „Digitale Souveränität“ wird im Ergebnis **nachhaltigere und zeitnähere Effekte** begrün-
537 den können, als medial-politische Großprojekte. Einerseits ist die Finanzierung derartiger **Groß-**
538 **projekte schwieriger**, andererseits ist die Umsetzung von Großprojekten **vergleichsweise**
539 **träge** und daher dem Risiko ausgesetzt, dass sich die Anforderungen im hoch-dynamischen
540 Themenfeld der Digitalen Souveränität bereits verändert haben, bevor das Großprojekt über-
541 haupt Wirkung entfalten kann.

