



Bund
Länder
Kommunen

Nationale IT-Architekturrichtlinie

Version 1.0.0

Präambel

Motivation

Die Architekturrichtlinie hilft dabei Architekturentscheidungen systematisch, nachvollziehbar und transparent zu treffen. Sie fördert dabei die passfähige Weiterentwicklung der Informationstechnik und Digitalisierung und trägt somit zur Erreichung der strategischen und politischen Ziele in der öffentlichen Verwaltung bei. Die Architekturvorgaben sind von den betroffenen Dienststellen, Projekten, Beschaffungsstellen, Dienstleistern und Herstellern eigenverantwortlich einzuhalten.

Grundlagen

Für die Gestaltung und Anwendung der Architekturrichtlinie wurden verschiedene Modelle und Standards, insbesondere das European Interoperability Framework (EIF¹), die European Library of Architecture Principles (ELAP²), The Open Group Architecture Framework (TOGAF³), das OECD Digital Government Policy Framework und Toolkit^{4 5} berücksichtigt. Erkenntnisse aus den Indikatoren, Prinzipien und Regeln wurden in die Erarbeitung der Architekturrichtlinie einbezogen.

Struktur

Aus den Modellen und Standards wurden vier zentrale Regelungsbereiche abgeleitet:

- Allgemeine Vorgaben (AV): rahmende Prinzipien und Eigenschaften
- Geschäftliche Vorgaben (GV): Motivation, Organisation und Fähigkeiten
- Funktionale Vorgaben (FV): Gestaltung von Informationssystemen
- Technische Vorgaben (TV): Technik, Technologie und Implementierung

Die einzelnen Vorgaben sind inhaltlich nach diesen Regelungsbereichen gruppiert. Anwenderinnen und Anwender erhalten entsprechend Ihrer Rolle eine schnelle Orientierung zur Initialisierung der

¹Europäische Kommission, Mitteilung der Kommission - Europäischer Interoperabilitätsrahmen - Umsetzungsstrategie (COM/2017/0134 final), 2017, verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52017DC0134&qid=1710430918493>, zuletzt abgerufen am 14. März 2024.

²Europäische Kommission - DG Informatics - ISA² Programme, Common Assessment Method for Standards and Specifications (CAMSS) – European Library of Architecture Principles, 2023, verfügbar unter <https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elap>, zuletzt abgerufen am 18. September 2024.

³The Open Group, The TOGAF Standard Version 9-2, 2022, verfügbar unter https://publications.opengroup.org/c182?_ga=2.209896722.686744425.1649171558-784988137.1649171558, zuletzt abgerufen am 23. Mai 2022.

⁴Organisation for Economic Co-operation and Development, Going Digital Toolkit, 2024, verfügbar unter <https://goingdigital.oecd.org/>, zuletzt aufgerufen am 18. September 2024.

⁵Organisation for Economic Co-operation and Development - Observatory of Public Sector Innovation, OECD Digital Government Toolkit, 2024, verfügbar unter <https://oecd-opsi.org/toolkits/oecd-digital-government-toolkit/>, zuletzt aufgerufen am 18. September 2024.

Bewertung von Architekturfragen. Dabei richten sich allgemeine Vorgaben primär an Enterprise Architekten und Entscheider, geschäftliche Vorgaben an Auftraggeber und Behörden, funktionale Vorgaben an Projekt- und Programmverantwortliche sowie technische Vorgaben an Techniker und Dienstleister. Die Vorgaben und Regelungsbereiche sind voneinander abgegrenzt. Architekturfragen müssen aber bedarfsweise aus verschiedenen Perspektiven und damit Regelungsbereichen betrachtet werden.

In jedem der Regelungsbereiche sollen maximal 10 Vorgaben beschrieben werden. Ähnliche Themen werden zur Erhöhung der Übersichtlichkeit und Verständlichkeit gebündelt. Einem stetigen Zuwachs an Vorgaben soll vorgebeugt und eine strategische Fokussierung und Priorisierung auf wesentliche Regelungen gefördert werden.

Regelungsbereich	Vorgaben				
AV - Allgemeine Vorgaben	AV-01 Konformität	AV-02 Interoperabilität	AV-03 Nachhaltigkeit	AV-04 Datenbasiertes Handeln	AV-05 Benutzerfreundlichkeit und Barrierefreiheit
	AV-06 Kollaboration	AV-07 Open Source	AV-08 Sicherheit und Schutz	AV-09 Souveränität	AV-10 Skalierbarkeit
GV - Geschäftliche Vorgaben	GV-01 Veränderung	GV-02 Portfolio	GV-03 Grundsatz	GV-04 Planung	GV-05 Prozessmanagement
	GV-06 Daten-Governance	GV-07 Verantwortung	GV-08 Bedarf	GV-09 Geschäftsgrundlage	GV-10 Qualität
FV - Funktionale Vorgaben	FV-01 Nutzungs- und Leistungsverpflichtung	FV-02 Dienste- und Schnittstellenbeschreibung	FV-03 Darstellung	FV-04 Anwendungen für den Bundesclient	FV-05 Information und Daten
	FV-06 Fachlichkeit	FV-07 Gestaltung	FV-08 Schutz	FV-09 Entkopplung	FV-10 Leistung
TV - Technische Vorgaben	TV-01 Administration	TV-02 Schnittstellen	TV-03 Effizienz	TV-04 Monitoring	TV-05 Entwicklung
	TV-06 Testen	TV-07 Autonomie	TV-08 Protektion	TV-09 Kommunikation	TV-10 Betrieb

Abbildung 1: Vorgaben der Architekturrichtlinie (Planungsstand: 10/2024)

Fortschreibung

Die Architekturrichtlinie wird kontinuierlich unter Einbindung der Stakeholder, insbesondere den Behörden und IT-Dienstleistern, entlang methodischer und technologischer Trends fortgeschrieben. Inhalte werden grundsätzlich in weiterverarbeitbarer Form gepflegt.

Auf Basis der weiterverarbeitbaren Form werden automatisiert verschiedene Ausgabeformate bereitgestellt. Einzelne Vorgaben können unabhängig vom Gesamtdokument geändert werden.

Zur Erarbeitung unterjähriger Veröffentlichungen stehen folgende Möglichkeiten zur Verfügung:

- Patch: Änderungen redaktioneller Art.
- Minor Release: Patch und Änderungen ohne direkte Auswirkung auf die Nutzenden.
- Major Release: Minor und Änderungen mit direkter Auswirkung auf die Nutzenden.

		Major-Release	Minor-Release	Patch
direkte Auswirkung	Verschärfung Verbindlichkeitsgrad	X		
	Neuer Inhalt mit Verbindlichkeitsgrad „soll“ oder höher	X		
indirekte Auswirkung	Verminderung Verbindlichkeitsgrad	X	X	
	Neuer Inhalt mit Verbindlichkeitsgrad „kann“	X	X	
	Entfernen von Inhalt	X	X	
	Neuer Begriff im Glossar	X	X	
	Änderung von Implikationen	X	X	
	Restrukturierung, Neusortierung von Inhalten	X	X	
redaktionelle Auswirkung	Änderung von Referenzen	X	X	X
	Redaktionelle, Orthographische Änderungen	X	X	X

Abbildung 2: Matrixdarstellung der Releasetypen

Spezifikationen

Struktur, Inhalt und Umfang der Architekturrichtlinie sind strategisch übergreifend ausgerichtet. Den Anwenderinnen und Anwendern der Architekturrichtlinie wird empfohlen, für ihre Anwendungsfälle die Regeln in den Vorgaben zu detaillieren. Dazu können eigene Spezifikationen/Ergänzungen erstellt und angewendet werden. Deren Geltungsbereich, konkreter Inhalt und Grad der Konkretisierung wird vom jeweiligen Autor festgeschrieben. Zur Unterstützung kann sich an den Fragen und Prüfpunkte der einzelnen Vorgaben orientiert werden.

Inhaltsverzeichnis

1 Einführung	6
1.1 Kontext	6
1.2 Geltungsbereich	7
1.3 Zielgruppe	7
1.4 Architekturelevante strategische Ziele	7
1.5 Aufbau des Dokumentes	9
1.6 Ausblick	9
2 Architekturvorgaben	10
2.1 Allgemeine Vorgaben	10
2.2 Geschäftliche Vorgaben	27
2.3 Funktionale Vorgaben	34
2.4 Technische Vorgaben	44
3 Anhang	56
3.1 Formatvorlage für die Architekturvorgabe	56
3.2 Verbindlichkeit der Architekturvorgaben	59
3.3 Weiterentwicklung und Einhaltung von Architekturvorgaben	60
3.4 Umgang mit konkurrierenden Architekturvorgaben	61
3.5 Glossar	64
3.6 Abkürzungsverzeichnis	73
3.7 Abbildungsverzeichnis	77

1 Einführung

In diesem Kapitel wird der Kontext, der Geltungsbereich, die Zielgruppe, die architekturelevanten strategischen Ziele, der Aufbau der Architekturrichtlinie und der Ausblick für die kommenden Fortschreibungen vorgestellt.

1.1 Kontext

Die strategische Ausrichtung der IT und Digitalisierung unterliegt verschiedenen Beschlüssen, Vorgaben auf europäischer Ebene und Ergebnissen aus Projekten sowie Initiativen. Folgende zeitlich sortierte Aktivitäten sind für den Kontext der Architekturrichtlinie relevant.

Die Standards für E-Government Anwendungen (SAGA 5 aus 2011⁶) sind eine Zusammenstellung von Referenzen auf Spezifikationen und Methoden für Softwaresysteme der öffentlichen Verwaltung. Im Rahmen der IT-Konsolidierung Bund wurde SAGA mit der Fortschreibung der Architekturrichtlinie 2019 abgelöst. Konkretisierungen erfolgen in Spezifikationen zur Architekturrichtlinie.

Zur Stärkung der grenzübergreifenden Zusammenarbeit hat die Europäische Union den Europäischen Interoperabilitätsrahmen (EIF aus 2017⁷) beschlossen. Um die Interoperabilität deutscher Verwaltungen mit europäischen Diensten zu gewährleisten, sollte die Kompatibilität der Architekturrichtlinie mit dem EIF hergestellt werden.

Im Onlinezugangsgesetz (OZG⁸) verpflichten sich Bund und Länder, sämtliche Leistungen der deutschen Verwaltung vollständig digital anzubieten. Unter dem strategischen Ziel der Nutzendenfreundlichkeit soll auf vorhandenen Strukturen aufgebaut und durch die digitalen Schnittstellen Einsparungspotentiale im Bereich der Bürokratiekosten und die Verkürzung von Bearbeitungszeiten erreicht werden. Zudem sollen offene Standards prioritär verwendet und Architekturvorgaben, Qualitätsstandards und Interoperabilitätsstandards festgelegt werden.

Mit der vom IT-Rat am 25. Februar 2019 beschlossene „Netzstrategie der öffentlichen Verwaltung 2030“ (IVÖV⁹) soll die netztechnische Basis als Integrationsplattform der gesamten öffentlichen Verwaltung fortentwickelt werden.

⁶Der Beauftragte der Bundesregierung für Informationstechnik, SAGA-Modul Grundlagen 5, 2011, verfügbar unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitaler-wandel/architekturen-standard/AM_SAGA_Grundlagen.html, zuletzt abgerufen am 19. September 2024.

⁷Europäische Kommission, Mitteilung der Kommission - Europäischer Interoperabilitätsrahmen – Umsetzungsstrategie (COM/2017/0134 final), 2017, verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52017DC0134&qid=1710430918493>, zuletzt abgerufen am 14. März 2024.

⁸Bundesgesetzblatt - Bundesministerium der Justiz, Onlinezugangsgesetz vom 14. August 2017 (BGBl. I S. 3122 und 3138) zuletzt durch Artikel 1 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245) geändert, 2024, verfügbar unter <https://www.gesetze-im-internet.de/ozg/>, zuletzt abgerufen am 18. September 2024.

⁹IT-Rat, Beschluss Nr. 11/2018, Netzstrategie 2030 für die öffentliche Verwaltung, 2018, verfügbar unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/it-sicherheit-und-netze/netze/netzstrategie-2030.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 18. September 2024.

Mit dem Beschluss des Eckpunktepapiers „Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung“ des IT-Rats vom 24. März 2020 und des IT-Planungsrats vom 04. Mai 2020¹⁰ haben Bund, Länder und Kommunen sich zum Ziel gesetzt, die Digitale Souveränität der Öffentlichen Verwaltung gemeinsam und kontinuierlich zu stärken. Zu diesem übergeordneten Ziel kann mit der konsequenten Umsetzung der Architekturrichtlinie ein wesentlicher Beitrag geleistet werden.

Darüber hinaus ergänzen diverse weitere querschnittliche und fachliche Strategien, Konzepte, Projekte und Initiativen den Kontext.

1.2 Geltungsbereich

Diese Architekturrichtlinie soll in allen Projekten, Programmen und Organisationen der Informationstechnik und Digitalisierung in der deutschen öffentlichen Verwaltung angewendet werden (siehe AV-01 Konformität).

1.3 Zielgruppe

Die Architekturvorgaben richten sich an alle Akteure mit Bezug zu Informationstechnik und Digitalisierung, insbesondere

- Architekturschaffende,
- Entscheidungstragende,
- Auftraggebende und Auftragnehmende,
- Beschaffungsstellen (Einkaufende),
- Beratungsstellen und Kompetenzzentren,
- Projekt- und Programmverantwortliche,
- Planende und Controllende,
- Service und Produkt Management,
- Dienstleistende inklusive Entwicklung und Betrieb sowie
- Liefernde, Anbietende und Herstellende.

Ein geeigneter Wissenstransfer an alle relevanten Mitarbeitende ist durch die jeweiligen Behörden, Dienststellen und Einrichtungen sicherzustellen.

1.4 Architekturrelevante strategische Ziele

Mit Einhaltung der Architekturvorgaben werden folgende strategische Ziele der Informationstechnik und Digitalisierung unterstützt:

¹⁰IT-Planungsrat, Beschluss Nr. 2020/19 vom 04. Mai 2020, Stärkung der Digitalen Souveränität der öffentlichen Verwaltung, 2020, verfügbar unter https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-19_Entscheidungsniederschrift_Umlaufverfahren_Eckpunktepapier.pdf, zuletzt abgerufen am 06. April 2022.

1. **Effektivität und Qualität** - Unterstützungsleistung, Flexibilität, Standards
2. **Digitalisierte Verwaltungsvorgänge** - Zugang, Prozesse, Basisdienste
3. **Zukunftsfähigkeit und Offenheit** - Innovation, Technologie, Arbeitsweise
4. **Informationssicherheit und Datenschutz** - Gewähr, Sensibilisierung, Resilienz
5. **Attraktivität als Arbeitgeber** - Bindung, Gewinnung, Werkzeuge, Arbeitsumfeld
6. **Wirtschaftlichkeit und Kosteneffizienz** - Bündelung, Wiederverwendung, Lebenszyklus
7. **Inklusion und Barrierefreiheit** - Chancengleichheit, Zugang, Nutzbarkeit
8. **Umweltverträglichkeit und Nachhaltigkeit** - Ökonomie, Ökologie, Soziales, Lebenszyklus
9. **Kooperation** - Schnittstellen, Integration, Interoperabilität, Zusammenarbeit
10. **Kontrollfähigkeit und Steuerbarkeit** - Planung, Steuerung, Business-IT-Alignment

Die allgemeinen Vorgaben (AVn) sind eng mit den strategischen Zielen und den Erkenntnissen aus den Rahmenwerken und internationalen Modellen verknüpft. Zur Übersicht wurden jeder AV die drei relevantesten strategischen Ziele zugeordnet.

Bezeichner	Allgemeine Vorgabe	Verknüpfte strategische Ziele
AV-01	Konformität	2, 4 und 10
AV-02	Interoperabilität	1, 2 und 9
AV-03	Nachhaltigkeit	1, 6 und 8
AV-04	Datenbasiertes Handeln	1, 2 und 10
AV-05	Benutzerfreundlichkeit und Barrierefreiheit	2, 7 und 9
AV-06	Kollaboration	5, 7 und 9
AV-07	Open Source	1, 3 und 9
AV-08	Sicherheit und Schutz	4, 9 und 10
AV-09	Souveränität	1, 4 und 10
AV-10	Skalierbarkeit	1, 3 und 6

In Anbetracht der vielschichtigen und komplexen Abhängigkeiten, weiterer laufender Initiativen und Projekte, sowohl auf Bundes-, aber insbesondere auch auf EU- und Länder- wie auch kommunaler Ebene sind potenzielle Zielkonflikte zwischen einzelnen Beschlüssen sowie laufenden inhaltlichen Konzeptionen nicht ausgeschlossen.

Im Rahmen der kontinuierlichen Fortschreibung relevanter Konzepte und Beschlüsse mit Bezug zur Architekturrichtlinie sind diese Zielkonflikte zu bewerten und zur Synchronisation an die jeweils geeignete Stelle zu adressieren. Des Weiteren sind diese Zielkonflikte in die Abhängigkeiten und/oder Implikationen der betroffenen Vorgaben aufzunehmen.

1.5 Aufbau des Dokumentes

Die Inhalte des vorliegenden Dokumentes sind wie folgt gegliedert:

- Kapitel 1 „Einführung“ beschreibt den Kontext, den Anwendungsrahmen und den Ausblick.
- Kapitel 2 „Architekturvorgaben“ beinhaltet die Architekturvorgaben.
- Kapitel 3 „Anhang“ ergänzende Informationen und Hilfsmittel wie die Formatvorlage, die Verbindlichkeitsgrade, die Nutzungsgrundsätze, das Glossar und die Verzeichnisse.

1.6 Ausblick

Neue strategische und technische Entwicklungen werden reflektiert, hinsichtlich der Bedeutung und Wirkung für Vorgaben bewertet und bedarfsweise in einer Fortschreibung aufgenommen.

2 Architekturvorgaben

In diesem Kapitel werden die Architekturvorgaben beschrieben.

2.1 Allgemeine Vorgaben

Die allgemeinen Vorgaben beschreiben die grundlegenden und rahmengebenden Prinzipien sowie Eigenschaften. Sie dienen einer grundlegenden Bewertung und Einordnung von Architekturentscheidungen.

ID: V-9001-R04

AV-01 Konformität

Informationstechnik und Digitalisierung **müssen** *konform* zu den Architekturvorgaben und rechtlichen Rahmenbedingungen gestaltet sein.

Regeln

1. Die Konformität **muss** im festgelegten *Geltungsbereich* sichergestellt werden (siehe Abschnitt Geltungsbereich).
2. Die Konformität **muss** gemäß dem *Verbindlichkeitsgrad* sichergestellt werden (siehe Abschnitt Verbindlichkeit).
3. Die Konformität **muss** entsprechend den *Nutzungsgrundsätzen* sichergestellt werden (siehe Abschnitt Umgang).
4. Die Konformität **muss** durch die Einhaltung der *Rechtsgrundlagen* sichergestellt werden.

Begründung

- Die Architekturvorgaben können ihre Wirkung nur dann umfassend entfalten, wenn sie eingehalten und bei allen relevanten Entscheidungen der IT-Weiterentwicklung und IT-Neubeschaffung zugrunde gelegt werden.
- Die öffentliche Verwaltung ist in ihrer Gesamtheit verpflichtet, jederzeit alle geltenden Gesetze und Verwaltungsvorschriften umzusetzen und zu befolgen.

Abhängigkeiten

- Keine

Implikationen

1. Bei Umsetzungsvorhaben wird frühzeitig die Konformität mit und die Wirksamkeit von Architekturvorgaben beachtet.
2. Zur Umsetzung der Architekturvorgaben sind adäquate Aus- und Weiterbildungsmöglichkeiten im Rahmen eines Architekturmanagements sicherzustellen.
3. Das Zusammenspiel zwischen der IT-Governance und den Vorgaben der Architekturrichtlinie ist zu beachten.
4. Es ist notwendig, dass die mit der Umsetzung der Richtlinien betrauten Mitarbeitenden die für ihren Tätigkeitsbereich relevanten Gesetze, Verwaltungsvorschriften und Richtlinien sowie die verfolgten Ziele kennen und anwenden.
5. Aktive Steuerung der Kommunikationsflüsse zwischen der Gesetzgebung und den IT-Bereichen der Behörden sowie von Architekturentscheidungen im Rahmen eines Architekturmanagements ist anzustreben.

ID: V-9003-R04

AV-02 Interoperabilität

Informationstechnik und Digitalisierung **sollen** *interoperabel* gestaltet sein.

Regeln

1. Die Interoperabilität **soll** durch offene *Standards* und *Profile* sichergestellt werden (u.a. XML, XÖV, ADatP-34¹¹).
2. Die Interoperabilität **soll** in den *Dimensionen* Governance, Recht, Organisation, Semantik und Technik sichergestellt werden (EIF¹²).
3. Die Interoperabilität **soll** durch etablierte organisatorische *Methoden*, *Vorgehensmodelle*, *Austauschformate* und *Fähigkeiten* umgesetzt werden (beispielsweise NAF^{TM13}, V-Modell[®] XT¹⁴, Scrum¹⁵, SAFe^{®16}, TOGAF^{®17}, ITIL^{®18}, COBIT^{®19}, PRINCE2, PMSquare).
4. Die Interoperabilität **soll** auf Basis von *Referenzarchitekturen* umgesetzt werden).
5. Die Interoperabilität **soll** hinsichtlich der *Kompatibilität* von *Betriebsumgebungen* und *Plattformen* sichergestellt werden.

Begründung

- Standardisierung fördert den medienbruchfreien Austausch von Informationen und Daten sowie die Kompatibilität von IT-Komponenten und IT-Lösungen und ermöglicht damit eine echte Ende-zu-Ende-Digitalisierung.
- Dies stellt u. a. die Interoperabilität und Wiederverwendbarkeit der IT-Komponenten und IT-Lösungen sicher.
- Des Weiteren wird eine höhere Bündelungsfähigkeit unterstützt.

¹¹NATO, NATO Interoperability Standards and Profiles, 2023, verfügbar unter <https://nhqc3s.hq.nato.int/apps/architecture/nisp/pdf/NISP-Vol1-v15-release.pdf>, zuletzt abgerufen am 19. August 2024.

¹²Europäische Kommission, Mitteilung der Kommission - Europäischer Interoperabilitätsrahmen – Umsetzungsstrategie (COM/2017/0134 final), 2017, verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52017DC0134&qid=1710430918493>, zuletzt abgerufen am 14. März 2024.

¹³NATO, NATO Architecture Framework, 2022, verfügbar unter https://www.nato.int/cps/en/natohq/topics_157575.htm, zuletzt abgerufen am 19. August 2024.

¹⁴Verein zur Weiterentwicklung des V-Modell XT eV (Weit eV), V-Modell XT - Version 2.4, 2024, verfügbar unter https://www.cio.bund.de/Webs/CIO/DE/digitaler-wandel/Achitekturen_und_Standards/V_modell_xt/v_modell_xt-node.html, zuletzt abgerufen am 11. Januar 2024.

¹⁵Scrum org, Scrum Webseite, 2022, verfügbar unter <https://www.scrum.org/>, zuletzt abgerufen am 23. Mai 2022.

¹⁶Scaled Agile Inc, SAFe - Scaled Agile Framework for Lean Enterprises, 2022, verfügbar unter <https://www.scaledagileframework.com/>, zuletzt abgerufen am 23. Mai 2022.

¹⁷The Open Group, The TOGAF Standard Version 9-2, 2022, verfügbar unter https://publications.opengroup.org/c182?_ga=2.209896722.686744425.1649171558-784988137.1649171558, zuletzt abgerufen am 23. Mai 2022.

¹⁸IT-Service Management Forum, Arbeitskreis Publikation ITIL Version 3 Translation Project, 2016, verfügbar unter https://web.archive.org/web/20160430161729/https://www.itsmf.de/fileadmin/dokumente/AK_Publikationen/20070831_ITIL_V3_Glossary_Germany.pdf, zuletzt abgerufen am 23. Mai 2022.

¹⁹ISACA, COBIT Framework, 2019, verfügbar unter <https://www.isaca.org/credentialing/cobit>, zuletzt abgerufen am 23. Mai 2022.

- In Bezug auf Methoden und Konzepte erlaubt die Standardisierung eine bessere behördenübergreifende Zusammenarbeit und gemeinsame Abstimmung.
- Die Orientierung an Referenzarchitekturen, insbesondere Domänen und Softwarearchitekturen, im Rahmen der Erstellung und Änderung der Landschaft an IT-Lösungen und damit die Anlehnung an Branchenstandards sowie gemeinschaftlich erhobener fachlicher und technischer Anforderungen, fördert die Wirtschaftlichkeit und Wartbarkeit der IT-Lösungen durch Wiederverwendung interner oder externer praxiserprobter Lösungsansätze.
- Die Interoperabilität fördert die Möglichkeit des Datenaustauschs von unterschiedlichen IT-Lösungen und damit ein ressort- und verwaltungsebenenübergreifendes medienbruchfreies Arbeiten. Die Interoperabilität ermöglicht zudem eine einfache Integration von IT-Lösungen in unterschiedliche Betriebsumgebungen und unterstützt die Kommunikationswege über alle Verwaltungsebenen (EU/ Bund/ Länder/ Kommunen) sowohl vertikal als auch horizontal und leistet einen Beitrag für die durchgängige Digitalisierung der öffentlichen Verwaltung.
- Die Interoperabilität ermöglicht den Wettbewerb und damit den Austausch von IT-Lösungen durch alternative Produkte.

Abhängigkeiten

- GV-04 Planung
- GV-05 Prozessmanagement
- TV-02 Schnittstellen
- TV-10 Betrieb

Implikationen

1. Im Zuge der (Weiter-)Entwicklung, Beschlussfassung und Umsetzung von Standardisierungen sind Standards und einheitliche Methoden zu berücksichtigen.
2. Die Schaffung notwendiger Prozesse und Strukturen, die für eine funktionsfähige Steuerung der ressortübergreifenden Strategien benötigt werden, sollte berücksichtigt werden.
3. Bei der Implementierung einer Architektur auf Basis von Referenzarchitekturen ist die Notwendigkeit der Anpassung auf behördenspezifische Bedarfe zu berücksichtigen.
4. Die Fortschreibung einer Referenzarchitektur ist stets einer behördenspezifischen Architektur zur Bedarfsabdeckung vorzuziehen.
5. Die Abstimmung notwendiger Regelungen vor der Bereitstellung von IT-Lösungen ist zu beachten.
6. Die Interoperabilität von IT-Lösungen sollte sowohl bei Neu- als auch bei Weiterentwicklungen beachtet werden.
7. Ein übergreifendes Schnittstellenmanagement sollte bereits in der Entwicklungsphase entsprechender Dienste beachtet werden.

ID: V-9012-R04

AV-03 Nachhaltigkeit

Informationstechnik und Digitalisierung **sollen** über den gesamten Lebenszyklus *nachhaltig* gestaltet sein.

Regeln

1. Die Nachhaltigkeit **soll** *ökologisch* und *sozial* umgesetzt werden (u.a. IT-Beschaffungsstrategie²⁰).
2. Die Nachhaltigkeit **soll** anhand von Kriterien aus *Zertifikaten* und *Labeln* umgesetzt werden (beispielsweise Blauer Engel²¹, u.a. Europäisches Umweltzeichen²², Energy Label²³).
3. Die Nachhaltigkeit **soll** durch *Optimierung* von *Energieverbrauch* und *Ressourcenverbrauch* umgesetzt werden (Green IT²⁴).
4. Die Nachhaltigkeit **soll** durch *Verwertung* nach Nutzungsende (Recycling, Reuse) sichergestellt werden (ElektroG²⁵).
5. Die Nachhaltigkeit **soll** *Wiederverwendbarkeit* berücksichtigen.

Begründung

- Mit der Beschaffung von umweltverträglicher IT und ressourceneffizienter Software werden die Regelungen der „Allgemeinen Verwaltungsvorschrift zur Beschaffung energieeffizienter Leistungen (AVV-EnEff²⁶)“ eingehalten.
- Die Einhaltung der Verpflichtungen aus dem Maßnahmenprogramm Nachhaltigkeit – Weiterentwicklung 2021²⁷ der Bundesregierung, aus dem Klimaschutzprogramm 2030 und dem Deutschen Ressourceneffizienzprogramm III werden gefördert.

²⁰Konferenz der IT-Beauftragten der Ressorts, IT-Beschaffungsstrategie für die zentralen IT-Beschaffungsstellen, 2018, verfügbar unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/it-rat/beschluesse/beschluss_2018_02.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 09. Januar 2024.

²¹RAL gemeinnützige GmbH, Blauer Engel - Energieeffizienter Rechenzentrumsbetrieb (DE-ZU 161), 2024, verfügbar unter <https://www.blauer-engel.de/de/produktwelt/rechenzentren>, zuletzt abgerufen am 19. August 2024.

²²RAL gemeinnützige GmbH, Über das EU Ecolabel, 2024, verfügbar unter <https://eu-ecolabel.de/eu-ecolabel-das-umweltzeichen-ihres-vertrauens/ueber-das-eu-ecolabel>, zuletzt abgerufen am 19. August 2024.

²³Europäische Kommission, Energielabel und Ökodesign, 2024, verfügbar unter https://ec.europa.eu/info/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/energy-label-and-ecodesign/about_de, zuletzt abgerufen am 19. August 2024.

²⁴IT-Planungsrat, Beschluss Nr. 2021/11 vom 17. März 2021 - KG Green IT, 2021, verfügbar unter <https://www.it-planungsrat.de/beschluss/beschluss-2021-11>, zuletzt abgerufen am 14. März 2024.

²⁵Bundesgesetzblatt - Bundesministerium der Justiz, Elektro- und Elektronikgerätegesetz vom 20. Oktober 2015 (BGBl. I S. 1739) zuletzt geändert durch Artikel 1 des Gesetzes vom 8. Dezember 2022 (BGBl. I S. 2240), 2022, verfügbar unter https://www.gesetze-im-internet.de/elektrog_2015/, zuletzt abgerufen am 14. März 2024.

²⁶Bundesanzeiger - Bundesministerium der Justiz, Allgemeine Verwaltungsvorschrift zur Beschaffung energieeffizienter Leistungen (AVV-EnEff) vom 18. Mai 2020, 2020, verfügbar unter https://www.bmwk.de/Redaktion/DE/Downloads/A/avv-eneff.pdf?__blob=publicationFile&v=8, zuletzt abgerufen am 14. März 2024.

²⁷Die Bundesregierung, Maßnahmenprogramm Nachhaltigkeit der Bundesregierung, 2021, verfügbar unter <https://www.bundesregierung.de/breg-de/themen/massnahmenprogramm-nachhaltigkeit-der-bundesregierung-427896>, zuletzt abgerufen am 14. März 2024.

- Durch eine fachgerechte Entsorgung sowie einer Zuführung von technischen Geräten zum Reuse-Markt und der daraus entstehenden Nachnutzung von Rohstoffen, kann der fortschreitenden Ressourcenknappheit entgegengewirkt sowie die Umweltbelastung reduziert werden.
- Die Wiederverwendung von IT-Komponenten und IT-Lösungen vermeidet unnötige Redundanzen und konzeptionell unterschiedliche Ausgestaltungen derselben Problemstellung und trägt damit wesentlich zur Aufwands- und Kostenreduzierung für die Entwicklung, die Wartung und den Betrieb bei.
- Durch die Umsetzung der Vorgabe wird die im Rahmen der OZG-Umsetzung geforderte Wiederverwendung und Nachnutzung als Servicestandard gefördert.²⁸

Abhängigkeiten

- Keine

Implikationen

1. Die Anschaffungskosten für Hardware können im Zusammenhang mit dieser Richtlinie steigen, da umweltfreundliche Geräte häufig preisintensiver sind.
2. Die ergänzenden Hilfestellungen des Umweltbundesamts sowie der Kompetenzstelle nachhaltige Beschaffung (KNB) sollten berücksichtigt werden.
3. Es sollte die Möglichkeit des (dynamischen) Up-/ Down-Sizing, um bedarfsgerechte Hardwarenutzung zu fördern, beachtet werden.
4. Bei der Verwertung von IT-Komponenten mit Datenspeichersystemen bei weiter bestehender Funktionsfähigkeit sollten die Regelungen des BSI für die Löschung und Vernichtung von Informationen unter CON.6²⁹ berücksichtigt werden.
5. Es sollten spezifische Maßgaben hinsichtlich des Designs von logischen Teilblöcken zur Optimierung der Wiederverwendbarkeit berücksichtigt werden.
6. Die Wiederverwendung und Wiederverwendbarkeit von IT-Komponenten sollte bei Neu- und Weiterentwicklungen im Rahmen übergreifender Architekturgremien beachtet werden.

²⁸Bundesministerium des Innern, Onlinezugangsgesetz - Prinzip 14: Wiederverwendung und Nachnutzung, 2024, verfügbar unter <https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/servicestandard/prinzip-14/prinzip-14-node.html>, zuletzt abgerufen am 14. März 2024.

²⁹Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschatz-Bausteine (Edition 2023) - OPS Betrieb, 2023, verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschatz/IT-Grundschatz-Kompodium/IT-Grundschatz-Bausteine/Bausteine_Download_Edition.html, zuletzt abgerufen am 26. August 2024.

ID: V-9080-R03

AV-04 Datenbasiertes Handeln

Informationstechnik und Digitalisierung **muss** datenbasiertes Verwaltungshandeln unterstützen.

Regeln

1. Daten **müssen** interdisziplinär für die Generierung von Information und Wissen bereitgestellt und genutzt werden.
2. Daten **müssen** zur Steigerung der Transparenz und Nachvollziehbarkeit von Entscheidungen eingesetzt werden.
3. Daten **müssen** genutzt werden, um ein proaktives Verwaltungshandeln zu fördern.

Begründung

- Der Einsatz von Daten ermöglicht das Treffen transparenter Entscheidungen und dadurch eine Stärkung des Vertrauens der Gesellschaft in die öffentliche Verwaltung. Ferner fördern Erkenntnisgewinne aus der Zusammenführung fachübergreifender Daten ein proaktives, evidenzbasiertes Verwaltungshandeln.
- Darüber hinaus ermöglicht die gezielte Bereitstellung und Verwendung von Daten verschiedene Mehrwerte für die öffentliche Verwaltung, wie unter anderem eine Reduktion des Ressourcenaufwands durch Automatisierungsmöglichkeiten.

Abhängigkeiten

- GV-06 Daten-Governance
- FV-05 Information und Daten
- TV-05 Entwicklung

Implikationen

1. Ausreichende Schulungsmöglichkeiten zu Daten und dem Aufbau von Datenkompetenz in der öffentlichen Verwaltung sind zur Verfügung zu stellen.
2. Bei der Entwicklung und Überarbeitung von Verwaltungsmaßnahmen sind weitere Einsatzmöglichkeiten von Daten zu berücksichtigen.

ID: V-9007-R04

AV-05 Benutzerfreundlichkeit und Barrierefreiheit

Informationstechnik und Digitalisierung **müssen** *benutzerfreundlich und barrierefrei* gestaltet sein.

Regeln

1. Die Nutzbarkeit **muss** durch *Benutzerfreundlichkeit* (Gebrauchstauglichkeit) sichergestellt werden (ISO 9241 110³⁰, ISO 9241 210³¹, Styleguide³²).
2. Die Nutzbarkeit **muss** durch *Barrierefreiheit* (Zugänglichkeit) sichergestellt werden (BFSG³³, BGG³⁴, BITV2³⁵, ISO 8241 171³⁶, EN 301549³⁷).

Begründung

- Die Berücksichtigung anerkannter Konzepte für die Benutzerfreundlichkeit von IT-Lösungen schafft eine höhere Akzeptanz bei den Nutzenden und fördert ein produktiveres Arbeiten, eine höhere Qualität der Arbeitsergebnisse und verringert Fehlbedienungen.
- Die Herstellung von Barrierefreiheit in IT-Lösungen schafft neben der Umsetzung geltenden Rechts auch Akzeptanz und ermöglicht, dass die Beschäftigung von Menschen mit Behinderung und somit die Attraktivität des öffentlichen Dienstes als Arbeitgeber gesteigert wird.

Abhängigkeiten

- GV-05 Prozessmanagement

³⁰Deutsches Institut für Normung eV, DIN EN ISO 9241-110 - Ergonomie der Mensch-System-Interaktion - Teil 110: Interaktionsprinzipien (ISO 9241-110:2020), 2020, verfügbar unter <https://www.din.de/de/mitwirken/normenausschuesse/naerg/veroeffentlichungen/wdc-beuth:din21:320862700>, zuletzt abgerufen am 12. März 2024.

³¹Deutsches Institut für Normung eV, DIN EN ISO 9241-210 - Ergonomie der Mensch-System-Interaktion - Teil 210: Menschzentrierte Gestaltung interaktiver Systeme (ISO 9241-210:2019), 2019, verfügbar unter <https://www.din.de/de/mitwirken/normenausschuesse/naerg/veroeffentlichungen/wdc-beuth:din21:313017070>, zuletzt abgerufen am 12. März 2024.

³²Presse- und Informationsamt der Bundesregierung, Das Corporate Design der Bundesregierung, 2024, verfügbar unter <https://styleguide.bundesregierung.de/sg-de>, zuletzt abgerufen am 12. März 2024.

³³Bundesgesetzblatt - Bundesministerium der Justiz, Barrierefreiheitsstärkungsgesetz vom 16. Juli 2021 (BGBl. I S. 2970) zuletzt geändert durch Artikel 28 des Gesetzes vom 8. Oktober 2023 (BGBl. 2023 I Nr. 272), 2023, verfügbar unter <https://www.gesetze-im-internet.de/bfsg/>, zuletzt aufgerufen am 12. März 2024.

³⁴Bundesgesetzblatt - Bundesministerium der Justiz, Behindertengleichstellungsgesetz vom 27. April 2002 (BGBl. I S. 1467f.) zuletzt geändert durch Artikel 7 des Gesetzes vom 23. Mai 2022 (BGBl. I S. 760), 2022, verfügbar unter <https://www.gesetze-im-internet.de/bgg/>, zuletzt abgerufen am 12. März 2024.

³⁵Bundesgesetzblatt - Bundesministerium der Justiz, Barrierefreie-Informationstechnik-Verordnung vom 12. September 2011 (BGBl. I S. 1843) zuletzt geändert durch Artikel 1 der Verordnung vom 24. Oktober 2023 (BGBl. 2023 I Nr. 286), 2023, verfügbar unter https://www.gesetze-im-internet.de/bitv_2_0/, zuletzt abgerufen am 12. März 2024.

³⁶Deutsches Institut für Normung eV, DIN EN ISO 9241-171 - Ergonomie der Mensch-System-Interaktion - Teil 171: Leitlinien für die Zugänglichkeit von Software (ISO 9241-171:2008), 2008, verfügbar unter <https://www.din.de/de/mitwirken/normenausschuesse/naerg/veroeffentlichungen/wdc-beuth:din21:107114575>, zuletzt abgerufen am 12. März 2024.

³⁷Deutsches Institut für Normung eV, DIN EN 301549 - Barrierefreiheitsanforderungen für IKT-Produkte und -Dienstleistungen, 2021, verfügbar unter <https://www.din.de/de/mitwirken/normenausschuesse/naerg/veroeffentlichungen/wdc-beuth:din21:353869627>, zuletzt abgerufen am 12. März 2024.

- TV-01 Administration

Implikationen

1. Die Benutzerfreundlichkeit sowie die Barrierefreiheit sollten als ein Kriterium bei der Beschaffung und Erstellung von IT-Lösungen berücksichtigt werden.
2. Die Mehraufwände, die bei der Beschaffung oder bei der Erstellung von barrierefreier Software entstehen, sollten bei der Planung berücksichtigt werden.

ID: V-9074-R03

AV-06 Kollaboration

Die digitale Kollaboration **soll** funktional ermöglicht werden.

Regeln

1. Die Kollaboration **soll** durch *zentral* bereitgestellte kollaborative Dienste gefördert werden.
2. Die Kollaboration **soll** durch Nutzung innerhalb einer IT-Anwendung oder durch *Einbindung* einer Drittanwendung in die genutzte IT-Anwendung gefördert werden.
3. Die Kollaboration **soll** durch digitale behördenübergreifende Zusammenarbeit in *Echtzeit* gefördert werden.

Begründung

- Mit der Nutzung digitaler Kollaborationsdienste kann die Effizienz und Effektivität der Art der Zusammenarbeit erhöht werden. Der Einsatz aktueller technischer Möglichkeiten in der Zusammenarbeit und das Angebot mobilen Arbeitens erhöhen die Attraktivität der Arbeitsbedingungen in der öffentlichen Verwaltung. Darüber hinaus wird die Familienfreundlichkeit durch die Möglichkeit des mobilen Arbeitens³⁸ gestärkt.

Abhängigkeiten

- FV-01 Nutzungs- und Leistungsverpflichtung
- TV-10 Betrieb

Implikationen

1. Bei der Einbindung kollaborativer Dienste ist die Vermeidung von Medienbrüchen je Anwendungsgebiet (z. B. unterschiedliche Chatprogramme) zu beachten.
2. Bei der Digitalisierung bestehender Prozesse ist eine frühzeitige Berücksichtigung der Einbindung digitaler kollaborativer Funktionen zielführend. Bei bestehenden digitalen Prozessen ist eine Erweiterung um kollaborative Funktionen sinnvoll.
3. Beim Einsatz digitaler kollaborativer Dienste sind die behördeninternen Nutzungsregeln zu beachten und bedarfsweise weiterzuentwickeln.
4. Bei der Nutzung von kollaborativen Funktionalitäten ist die Einstufung der Inhalte zu beachten.

³⁸Bundesministerium des Innern, Jedes Alter zählt - Die Demografiestrategie der Bundesregierung - Arbeitsgruppenergebnisse zum Demografieipfel am 16. März 2017, 2017, verfügbar unter https://www.demografie-portal.de/DE/Politik/Bund/Dialogprozess/Arbeitsgruppen/ergebnisbericht-arbeitsgruppen-2017.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 14. März 2024.

ID: V-9075-R03

AV-07 Open Source

Open Source **soll** als Grundprinzip priorisiert werden.

Regeln

1. Open Source **soll** kontinuierlich in ihrem Einsatz ausgebaut werden.
2. Open Source und deren Weiterentwicklung **soll** durch eine aktive Beteiligung an der Open Source Community gefördert werden.
3. Open Source Software, die durch oder für die öffentliche Verwaltung entwickelt wird, **soll** auf der Open CoDE Plattform³⁹ veröffentlicht werden.

Begründung

- Open Source fördert eine transparente und offene Arbeitsweise sowie eine Kultur, die Effizienzsteigerungen bewirken und eine kontinuierliche Verbesserung unterstützen.
- Die Nutzung von Open Source sowie die öffentliche Bereitstellung tragen durch die damit geschaffene Transparenz zur Stärkung des Vertrauens in öffentliche Institutionen bei und reduzieren Abhängigkeiten von einzelnen Herstellern. Ferner ermöglicht Open Source einfachere Anpassungsmöglichkeiten.
- Durch die Erfüllung der Vorgabe wird die Umsetzung des Beschlusses 2020/39⁴⁰ des IT-Planungsrates hinsichtlich der Empfehlung im Servicestandard für die OZG-Umsetzung zur Veröffentlichung des Quellcodes aus der Realisierung digitaler Angebote der Verwaltung (Eigenentwicklung) umgesetzt.

Abhängigkeiten

- FV-05 Information und Daten

Implikationen

1. Die Vorteile, die sich aus der Nutzung von Open Source Software ergeben, sollten beim Beschaffungsprozess besonders beachtet werden.
2. Bei beschaffter Open Source Software ist das potenziell notwendige Angebot von Servicedienstleistungen zu beachten.
3. Die zu erwartenden Aufwände für eine aktive Beteiligung an der Open Source Community sollten bei der Planung von Entwicklungsprojekten berücksichtigt werden.
4. Bei der Veröffentlichung von Quellcodes sollte eine angemessene Lizenzierung beachtet werden.

³⁹Zentrum für Digitale Souveränität, Open CoDE, 2024, verfügbar unter <https://opencode.de/>, zuletzt aufgerufen am 19. August 2024.

⁴⁰IT-Planungsrat, Beschluss Nr. 2019/01 vom 12. März 2019 - OZG-Umsetzung (Digitalisierung von Verwaltungsleistungen), 2019, verfügbar unter <https://www.it-planungsrat.de/beschluss/beschluss-2019-01>, zuletzt abgerufen am 14. März 2024.

ID: V-9004-R05

AV-08 Sicherheit und Schutz

Informationstechnik und Digitalisierung **müssen** sicher gestaltet und *geschützt* werden.

Regeln

1. *Informationssicherheit* **muss** gemäß geltenden Vorgaben gewährleistet werden (insbesondere BSI 200-1 ISMS⁴¹, BSI 200-2 Grundschatz⁴², BSI 200-3 Risikoanalyse⁴³, BSIG⁴⁴, BSI Info⁴⁵, NATO Cyber Defence⁴⁶).
2. Die Anforderungen des *Geheimsschatzes* **müssen** erfüllt werden. (insbesondere Sicherheitsüberprüfung⁴⁷, personeller Geheimsschatz⁴⁸, materieller Geheimsschatz/ Verschlussachen⁴⁹).
3. Die gesetzlichen Regelungen bezüglich *Datenschutz* **müssen** beachtet werden (insbesondere DSGVO⁵⁰, BDSG⁵¹, SDM⁵²).[^]

Begründung

⁴¹Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-1 - Managementsysteme für Informationssicherheit (ISMS), 2017, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/BSI_Standards/standard_200_1.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 12. März 2024.

⁴²Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-2 - IT-Grundschatz-Methodik, 2017, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 12. März 2024.

⁴³Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-3 - Risikoanalyse auf der Basis von IT-Grundschatz, 2017, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 12. März 2024.

⁴⁴Bundesgesetzblatt - Bundesministerium der Justiz, BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821) zuletzt geändert durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982), 2021, verfügbar unter https://www.gesetze-im-internet.de/bsig_2009/, zuletzt abgerufen am 12. März 2024.

⁴⁵Bundesamt für Sicherheit in der Informationstechnik, Informationen und Empfehlungen, 2024, verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/informationen-und-empfehlungen_node.html, zuletzt abgerufen am 22. August 2024.

⁴⁶North Atlantic Treaty Organization, Cyber Defence, 2024, verfügbar unter https://www.nato.int/cps/en/natohq/topics_78170.htm, zuletzt abgerufen am 26. August 2024.

⁴⁷Bundesgesetzblatt - Bundesministerium der Justiz, Sicherheitsüberprüfungsgesetz vom 20. April 1994 (BGBl. I S. 867) zuletzt geändert durch Artikel 3 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 413), 2023, verfügbar unter https://www.gesetze-im-internet.de/s_g/, zuletzt abgerufen am 12. März 2024.

⁴⁸Bundesministerium des Innern und für Heimat, Allgemeine Verwaltungsvorschrift zum personellen Geheimsschatz und zum vorbeugenden personellen Sabotageschutz - SÜG-Ausführungsvorschrift (SÜG-AVV) vom 15. Februar 2018 (GMBl S. 270) i.d.F. der mit Rundschreiben des Bundesministeriums des Innern und für Heimat vom 8. Juni 2022 - ÖS II 5 - 54001/41#3 - bekanntgegebenen Änderungen, 2022, verfügbar unter https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_08062022_SII54001415.htm, zuletzt abgerufen am 12. März 2024.

⁴⁹Bundesministerium des Innern und für Heimat, Allgemeine Verwaltungsvorschrift zum materiellen Geheimsschatz (Verschlussachenanweisung - VSA), 2023, verfügbar unter https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_13032023_SII54001405.htm, zuletzt abgerufen am 12. März 2024.

⁵⁰Das Europäische Parlament und der europäische Rat, Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), 2016, verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679>, zuletzt abgerufen am 12. März 2024.

⁵¹Bundesgesetzblatt - Bundesministerium der Justiz, Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097) zuletzt geändert durch Artikel 10 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 414), 2023, verfügbar unter https://www.gesetze-im-internet.de/bdsg_2018/, zuletzt abgerufen am 12. März 2024.

⁵²IT-Planungsrat, Beschluss Nr. 2020/06 vom 25. März 2020 - Standard-Datenschutzmodell, 2020, verfügbar unter <https://www.it-planungsrat.de/beschluss/beschluss-2020-06>, zuletzt abgerufen am 12. März 2024.

- Einschränkungen in Grundwerten der Informationssicherheit (Vertraulichkeit, Verfügbarkeit und Integrität), dem Datenschutz und dem Geheimschutz können ernsthafte Folgen nach sich ziehen.
- Zu diesen zählen u. a. Betriebsrisiken, rechtliche Folgen, Vertrauensverlust gegenüber den Behörden, Autoritätsverlust und Angreifbarkeit des Staates.
- Durch die Einhaltung der Vorgabe kann hiergegen maßgeblich vorgebeugt werden.

Abhängigkeiten

- FV-08 Schutz
- TV-02 Schnittstellen
- TV-08 Protektion
- TV-10 Betrieb

Implikationen

1. Die Klassifikation des Schutzbedarfes von Daten, Informationen und Algorithmen ist zu beachten.
2. Die Referenzmaßnahmen des Standard-Datenschutzmodells sind nach Möglichkeit umzusetzen.

ID: V-9070-R04

AV-09 Digitale Souveränität

Informationstechnik und Digitalisierung **müssen** *digital souverän* gestaltet sein.

Regeln

1. Die digitale Souveränität **muss** durch vollumfängliche *Kontrollierbarkeit* und *Steuerbarkeit* sichergestellt werden.
2. Die digitale Souveränität **muss** durch *Flexibilität*, *Erweiterbarkeit* und *Austauschbarkeit* sichergestellt werden (insbesondere Wechsellmöglichkeiten).
3. Die digitale Souveränität **muss** durch ausreichend *interne Kompetenzen* gewährleistet sein (insbesondere Gestaltungsfähigkeit).
4. Die digitale Souveränität **soll** durch *Herstellerunabhängigkeit* und *Anbieterunabhängigkeit* (Multi-Vendor-Ansatz, IT-Sourcing-Strategie, unabhängige IT-Leistungen) sichergestellt werden.

Begründung

- Durch die Einhaltung der Vorgabe können kritische Abhängigkeiten der öffentlichen Verwaltung zu einzelnen Technologieanbietern reduziert und damit die Selbstständigkeit und Selbstbestimmtheit gewahrt werden.
- Die Vorgabe zur Stärkung der digitalen Souveränität erfüllt den Beschluss 2021/09⁵³ des IT-Planungsrates.
- Hersteller- und Anbieterunabhängigkeit ist gerade für die öffentliche Verwaltung ein wesentliches Leitprinzip zur Sicherstellung architektonischer Flexibilität, Gestaltungs- und Handlungshoheit und Vermeidung von Abhängigkeitsverhältnissen zu einzelnen Herstellern („Herstellermonopole“) und Anbietern.
- Hersteller- und Anbieterunabhängigkeit ist ein zentrales Element zur Erreichung der Digitalen Souveränität. Die Ergebnisse und abgeleiteten Maßnahmen der Studien zur Digitalen Souveränität⁵⁴ sollten bei größeren Änderungen und Neubeschaffungen beachtet werden.

Abhängigkeiten

- Keine

Implikationen

⁵³IT-Planungsrat, Beschluss Nr. 2021/09 vom 17. März 2021 - AG Cloud Computing und Digitale Souveränität, 2021, verfügbar unter <https://www.it-planungsrat.de/beschluss/beschluss-2021-09>, zuletzt abgerufen am 14. März 2024.

⁵⁴Der Beauftragte der Bundesregierung für Informationstechnik, Digitale Souveränität, 2024, verfügbar unter <https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html>, zuletzt abgerufen am 20. Oktober 2024.

1. Beim Einsatz neuer IT-Komponenten oder IT-Lösungen sind bereits bestehende Abhängigkeiten zu beachten.
2. Bei der Nutzung innovativer Technologien sind durch den unwesentlichen Grad der Verbreitung sowie die geringe Anzahl an Anbietenden mögliche entstehende Abhängigkeiten besonders zu beachten.
3. Die notwendigen Ressourcen für die Sicherstellung der Digitalen Souveränität sind bei der Planung zu berücksichtigen.
4. Die Hersteller- und Anbieterunabhängigkeit sollte nicht nur auf technischer, sondern auch auf strategischer und prozessualer Ebene Beachtung finden. Dies betrifft sowohl die Beschaffung von Standardlösungen als auch die Entwicklung von Individuallösungen und die Implementierung von Schnittstellen zwischen den IT-Lösungen.
5. Die Vorgaben des Vergaberechts, insbesondere der Grundsatz der produktneutralen Beschaffung (§31)⁵⁵, sollten beachtet und die ergänzenden Vertragsbedingungen der EVB-IT bei der Beschaffung in ihrer jeweils gültigen Fassung angewendet werden.
6. Bei der Einführung von Multi-Vendor-Strategien sollte die Einrichtung notwendiger Rollen und Prozesse beachtet werden.
7. Die Mehraufwände, die bei der Gewährleistung der Herstellerunabhängigkeit aufgrund des Verzichts auf einzelne herstellerabhängige Funktionen und des damit möglichen hohen Implementierungsaufwands entstehen können, sollten bei der Planung berücksichtigt werden.

⁵⁵Bundesgesetzblatt - Bundesministerium der Justiz, Vergabeverordnung vom 12. April 2016 (BGBl. I S. 624) zuletzt geändert durch Artikel 1 der Verordnung vom 7. Februar 2024 (BGBl. 2024 I Nr. 39), 2024, verfügbar unter https://www.gesetze-im-internet.de/vgv_2016/, zuletzt abgerufen am 14. März 2024.

ID: V-9011-R04

AV-10 Skalierbarkeit

Informationstechnik und Digitalisierung **sollen skalierbar** gestaltet sein.

Regeln

1. Die Skalierbarkeit **soll** durch *Komplexitätsreduktion* unterstützt werden. (u.a. Anzahl, Heterogenität, Abhängigkeiten, Redundanzen, fachliche Struktur).
2. Die Skalierbarkeit **soll** durch *Modularität* unterstützt (Separation of Concerns, Wirtschaftlichkeit) werden.
3. Die Skalierbarkeit **soll** durch automatische und *flexible Anpassung von Ressourcen* (insbesondere durch Cloud Computing) unterstützt werden.

Begründung

- Wesentlicher Erfolgsfaktor für den Aufbau skalierbarer IT-Architekturen und den langfristigen Betrieb umfangreicher IT-Lösungen ist die Reduzierung der Komplexität auf ein notwendiges Maß.
- Die Reduktion der Komplexität fördert die Übersichtlichkeit (z. B. für Betrieb und Wartung) und die Stabilität des IT-Betriebs (z. B. durch die Verringerung von Fehlern und einer einfacheren Fehlersuche) und damit eine Verringerung der laufenden direkten und indirekten Kosten über den gesamten Lebenszyklus hinweg.
- Modularität bietet die Möglichkeit, dass die einzelnen IT-Komponenten separat geplant, entwickelt und getestet werden können.
- Durch die Nutzung von Cloud Computing und modularer Cloud-Infrastruktur wird die Effizienz und Effektivität in Entwicklung, Inbetriebnahme und Betrieb von Anwendungen gesteigert, das Datenmanagement optimiert und die Skalierbarkeit der Infrastrukturplattformkomponenten ermöglicht. Auch deshalb wurden die Entscheidungen des IT-Planungsrats 2020/54⁵⁶ und 2021/46⁵⁷ zur DVS getroffen.

Abhängigkeiten

- FV-09 Entkopplung
- TV-01 Administration
- TV-10 Betrieb

Implikationen

⁵⁶IT-Planungsrat, Beschluss Nr. 2020/54 vom 28. Oktober 2020 - AG Cloud Computing und digitale Souveränität, 2020, verfügbar unter <https://www.it-planungsrat.de/beschluss/beschluss-2020-54>, zuletzt abgerufen am 14. März 2024.

⁵⁷IT-Planungsrat, Beschluss Nr. 2021/46 vom 29. Oktober 2021 - Deutsche Verwaltungscld-Strategie, 2021, verfügbar unter <https://www.it-planungsrat.de/beschluss/beschluss-2021-46>, zuletzt abgerufen am 12. März 2024.

1. Mechanismen zur Reduktion der Komplexität sind in strategischen, prozessualen und technischen Strukturen zu verankern.
2. Bei der Reduktion der Komplexität und Heterogenität ist darauf zu achten, dass das Risiko einer Hersteller- oder Anbieterabhängigkeit und damit einhergehender Gefährdung der digitalen Souveränität in die Abwägung einbezogen wird.
3. Durch die Umsetzung der Modularität kann es zu Performanceverlusten kommen, dies sollte berücksichtigt werden.
4. Der erhöhte Planungs- und Umsetzungsaufwand für IT-Lösungen, der durch die Entkopplung von IT-Komponenten entsteht, sollte beachtet werden.
5. Modularisierung sollte bereits bei der Architekturkonzeption und in Ausschreibungsunterlagen berücksichtigt werden.
6. Standards für die Infrastruktur- und Plattformbereitstellungen für Cloud Computing sind zu berücksichtigen.

2.2 Geschäftliche Vorgaben

Die geschäftlichen Vorgaben beschreiben die Motivation, Organisation und Fähigkeiten der geschäftlichen Aktivitäten inklusive notwendiger Managementdisziplinen und Arbeitsweisen. Sie dienen einer nachfrageseitigen sowie fachlich/ querschnittlichen Bewertung und Einordnung von Architekturentscheidungen.

ID: V-9100-R01

GV-01 Veränderung

Die Veränderung **muss** *bewertet* und *gestaltet* werden.

Regeln

1. Die Veränderung **muss** durch *Machbarkeitsprüfungen* (zeitliche, finanzielle, organisatorische Abschätzung) bewertet werden.
2. Die Veränderung **muss** durch eine *Migrationsstrategie* beschrieben sein.
3. Lösungen derselben Funktionalität **sollen** mit dem nächsten grundlegenden *Versionswechsel* zur Sicherstellung der *Überschneidungsfreiheit* abgelöst werden.
4. Veränderungen mit Auswirkungen auf Mitarbeitende **sollen** durch ein aktives Veränderungsmanagement begleitet werden.

Begründung

- Keine

Abhängigkeiten

- AV-05 Benutzerfreundlichkeit und Barrierefreiheit
- GV-04 Planung
- GV-05 Prozessmanagement

Implikationen

1. Der Rollout und die Umstellungen werden zwischen Behörde und IT-Dienstleistern abgestimmt.
2. Die Behörden entscheiden anhand der fachlich-rechtlichen Vorgaben über die IT-technische Unterstützung (mit oder ohne IT).

ID: V-9015-R04

GV-04 Planung

Die Planung **soll** *methodengestützt* durchgeführt werden.

Regeln

1. Bei der Planung **sollen** *Praxisleitfäden* beachtet werden (u.a. Projektmanagement öV⁵⁸).
2. Bei der Planung von Organisationsprojekten **soll** das *Organisationshandbuch* berücksichtigt werden (Organisationshandbuch⁵⁹).
3. Bei der Planung von Projekten **sollen** *Projektmanagementmethoden* verwendet werden (u.a. V-Modell XT⁶⁰, S-O-S-Methode⁶¹, Scrum⁶²).
4. Bei der Planung von Haushaltsmitteln für den IT-Einsatz **soll** die *IT-Rahmenplanung* verwendet werden.

Begründung

- Die Einführung von IT-Lösungen - und der entsprechenden Erhebung und Anpassung der Verwaltungsabläufe sollte im Rahmen strukturierter Projekte erfolgen.
- Zur Unterstützung dieser Projekte sind wesentliche Aspekte zum Aufbau und zur Durchführung zentral im „Praxisleitfaden Projektmanagement für die Öffentliche Verwaltung“ und im Organisationshandbuch dargestellt.

Abhängigkeiten

- AV-02 Interoperabilität

Implikationen

1. Keine

⁵⁸Bundesministerium des Innern, Praxisleitfaden Projektmanagement für die Öffentliche Verwaltung, 2013, verfügbar unter <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/moderne-verwaltung/praxisleitfaden-projektmanagement.html>, zuletzt abgerufen am 12. März 2024.

⁵⁹Bundesministerium des Innern und für Heimat, Organisationshandbuch, 2024, verfügbar unter <https://www.orghandbuch.de/>, zuletzt abgerufen am 21. August 2024.

⁶⁰Verein zur Weiterentwicklung des V-Modell XT eV (Weit eV), V-Modell XT - Version 2.4, 2024, verfügbar unter https://www.cio.bund.de/Webs/CIO/DE/digitaler-wandel/Achitekturen_und_Standards/V_modell_xt/v_modell_xt-node.html, zuletzt abgerufen am 11. Januar 2024.

⁶¹Bundesverwaltungsamt, S-O-S-Methode für Großprojekte, 2022, verfügbar unter https://www.bva.bund.de/DE/Services/Behoerden/Beratung/Beratungszentrum/GrossPM/_documents/stda_sos_methode.html, zuletzt abgerufen am 12. März 2024.

⁶²Scrum org, Scrum Webseite, 2022, verfügbar unter <https://www.scrum.org/>, zuletzt abgerufen am 23. Mai 2022.

ID: V-9016-R04

GV-05 Prozessmanagement

Prozessmanagement **muss** standardisiert etabliert, Prozessmodelle **müssen** auf standardisierten Notationen aufbauen und spezifische Austauschformate verwenden.

Regeln

1. Prozessmodelle **müssen** auf standardisierten Normen aufsetzen (u.a. DIN SPEC 90158⁶³)
2. Bei der Modellierung **müssen** *Muster- und Referenzprozesse* (Prozestemplates) beachtet werden.
3. Bei der Modellierung von Verwaltungsleistungen **soll** das *Föderale Informationsmanagement* verwendet werden (FIM⁶⁴).
4. Bei der Modellierung **müssen** *Modellierungssprachen* und *Notationen* verwendet werden (u.a. BPMN 2.0⁶⁵, CMMN 1.1⁶⁶, DMN 1.2⁶⁷, UML 2.5⁶⁸, Archimate 3.2⁶⁹).
5. Modelle **müssen** über *Austauschformate* wiederverwendbar sein (u.a. XProzess⁷⁰).

Begründung

- Die Prozesse sollen erhoben, dargestellt, bewertet und verbessert werden.
- Nach § 3 Absatz 3 EGovG⁷¹ sollen Behörden allgemeine Leistungsinformationen in standardisierter Form bereitstellen.
- Dies beinhaltet auch die Prozessdokumentation.
- Zudem gelten der Beschluss 2016/29⁷² des IT-Planungsrats zur Etablierung von FIM als Anwen-

⁶³Deutsches Institut für Normung e. V., DIN SPEC 90158:2017-08 - Handlungsleitfaden für ein strategisches und operatives Prozessmanagement in der öffentlichen Verwaltung, 2017, verfügbar unter <https://www.dinmedia.de/de/technische-regel/din-spec-90158/273163811>, zuletzt abgerufen am 21. August 2024.

⁶⁴Föderale IT-Kooperation, Föderales Informationsmanagement, 2024, verfügbar unter <https://fimportal.de/>, zuletzt aufgerufen am 21. August 2024.

⁶⁵Object Management Group, Business Process Model and Notation - Version 2.0.2, 2014, verfügbar unter <https://www.omg.org/spec/BPMN>, zuletzt abgerufen am 21. August 2024.

⁶⁶Object Management Group, Case Management Model and Notation - Version 1.1, 2016, verfügbar unter <https://www.omg.org/spec/CMMN/>, zuletzt abgerufen am 21. August 2024.

⁶⁷Object Management Group, Decision Model and Notation - Version 1.5, 2024, verfügbar unter <https://www.omg.org/spec/DMN/>, zuletzt abgerufen am 21. August 2024.

⁶⁸Object Management Group, Unified Modeling Language - Version 2.5.1, 2017, verfügbar unter <https://www.omg.org/spec/UML/>, zuletzt abgerufen am 21. August 2024.

⁶⁹The Open Group, ArchiMate® 3.2 Specification, 2023, verfügbar unter <https://pubs.opengroup.org/architecture/archimate3-doc/>, zuletzt aufgerufen am 21. August 2024.

⁷⁰Geschäfts- und Koordinierungsstelle Föderales Informationsmanagement - Baustein Prozesse (GK_FIM), XProzess - Version 2.0.1, 2024, verfügbar unter <https://www.xrepository.de/details/urn:xoev-de:mv:em:standard:xprozess>, zuletzt aufgerufen am 21. August 2024.

⁷¹Bundesgesetzblatt - Bundesministerium der Justiz, E-Government-Gesetz vom 25. Juli 2013 (BGBl. I S. 2749) zuletzt geändert durch Artikel 2 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245), verfügbar unter <http://www.gesetze-im-internet.de/egovg/EGovG.pdf>, zuletzt abgerufen am 30. Januar 2024.

⁷²IT-Planungsrat, Beschluss Nr. 2016/29 vom 13. Oktober 2016 - Steuerungsprojekt Föderales Informationsmanagement (FIM), 2016, verfügbar unter <https://www.it-planungsrat.de/beschluss/beschluss-2016-29>, zuletzt abgerufen am 14. März 2024.

derung bzw. Produkt des IT-Planungsrats und der Beschluss 2019/01⁷³ des IT-Planungsrats zur Nutzung von FIM im Rahmen von OZG.

- Mit vollständig modellierten Prozessen lassen sich Entscheidungen bezüglich der IT-Ausrichtung und der Anpassung organisatorischer Rahmenbedingungen schneller und effizienter treffen.
- Die aufgeführten Vorgaben sind Standards in Lehre und Forschung und sind erprobt und verlässlich.
- Die Verwendung gemeinsamer Konventionen und Standards in Bezug auf die Modellierung fördert darüber hinaus die Austauschbarkeit der Ergebnisse und schafft damit Synergien z. B. durch gemeinsame Prozessbibliotheken.
- Um einen reibungslosen Austausch von Prozessmodellen über verschiedene Nutzende, IT-Anwendungen und Behörden zu ermöglichen, ist es notwendig, Austauschformate zu definieren. Durch die Nutzung von einheitlichen, offenen Austauschformaten können Prozessmodelle ohne Abhängigkeiten zu Herstellern oder Technologien ausgetauscht werden.
- Laut Beschluss des IT-Planungsrats 2019/14⁷⁴ ist dafür der Standard XProzess zu verwenden.

Abhängigkeiten

- AV-02 Interoperabilität

Implikationen

1. Da bis 2025 in den von der IT-Konsolidierung betroffenen Bereichen von den zentralen IT-Dienstleistern jeweils nur noch maximal zwei Basisdienste bzw. Querschnittsdienste für gleiche Funktionalitäten bereitgestellt werden sollen, enthält das IT-Rahmenkonzept 2023 das Projekt „Prozessmanagementtool“.
2. Den entsprechenden Modellierern müssen geeignete IT-Anwendungen und Schulungen zur Verfügung gestellt werden.
3. Die genutzten IT-Anwendungen müssen die entsprechenden Austauschformate unterstützen und geeignete Schnittstellen bereitstellen.

⁷³IT-Planungsrat, Beschluss Nr. 2019/01 vom 12. März 2019 - OZG-Umsetzung (Digitalisierung von Verwaltungsleistungen), 2019, verfügbar unter <https://www.it-planungsrat.de/beschluss/beschluss-2019-01>, zuletzt abgerufen am 14. März 2024.

⁷⁴IT-Planungsrat, Beschluss Nr. 2019/14 vom 12. März 2019 - XÖV-Standard für FIM: XProzess, 2019, verfügbar unter <https://www.it-planungsrat.de/beschluss/beschluss-2019-14>, zuletzt abgerufen am 14. März 2024.

ID: V-9081-R03

GV-06 Daten-Governance

Die Daten-Governance soll ausgebaut werden.

Regeln

1. Die Daten-Governance **soll** den Rahmen für einen effektiven und effizienten Umgang mit Daten legen und bildet somit die Grundlage für eine *datenorientierte* Organisation in der öffentlichen Verwaltung.
2. Für die Daten-Governance **sollen** *Richtlinien und Regeln* (z.B. Hausanordnungen) sowie anzuwendende *Standards* festgelegt sein.
3. Die Daten-Governance **soll** *Rollen und Verantwortlichkeiten* definieren.
4. In der Daten-Governance **sollen** *Verhaltensregeln, Prozesse und Best-Practices* aufgestellt sein.

Begründung

- Der Ausbau der Daten-Governance ist ein wesentlicher Bestandteil zur Steigerung von Datenkompetenzen, zum Umgang mit Daten, zu datenbasierten Entscheidungsprozessen und zum Aufbau von Datenökosystemen, wodurch gleichzeitig datenorientierte Innovationen innerhalb des bestehenden Rechtsrahmens ermöglicht werden.
- Gemäß dem Vorschlag der Europäischen Kommission für einen gemeinsamen europäischen Data Governance Act⁷⁵ soll die Gewährleistung von Datenzugangsneutralität, Übertragbarkeit und Interoperabilität von Daten sowie die Vermeidung von Lock-in-Effekten sichergestellt werden, welches für die Schaffung eines europäischen Datenraumes berücksichtigt werden soll.

Abhängigkeiten

- AV-04 Datenbasiertes Handeln
- FV-05 Information und Daten
- TV-05 Entwicklung

Implikationen

1. Bei der Einführung einer Daten-Governance sind auch Vorgaben für die Datenqualität zu berücksichtigen.

⁷⁵Das Europäische Parlament und der Rat, Verordnung (EU) 2022/868 vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), 2022, verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R0868>, zuletzt abgerufen am 12. März 2024.

2. Für die Etablierung, Weiterentwicklung und Einhaltung einer Daten-Governance werden Ressourcen benötigt.
3. Bei der Überprüfung bestehender und der Einführung zukünftiger datengestützter Leistungsangebote sind die in der Daten-Governance festgelegten Rahmenbedingungen zu beachten.

2.3 Funktionale Vorgaben

Die funktionalen Vorgaben beschreiben die Anforderungen und Bedingungen zur Gestaltung sowie Umsetzung von Informationssystemen und Digitalisierungsaktivitäten. Dabei beinhalten diese funktionale, datenbasierte und logische Perspektiven (Dienste). Sie dienen einer umsetzungsbezogenen Bewertung und Einordnung von Architekturentscheidungen.

ID: V-9019-R04

FV-01 Nutzungs- und Leistungsverpflichtung

Die allgemeine Nutzungs- und Leistungsverpflichtung **soll eingehalten** werden.

Regeln

1. Die gemeinsam zu nutzende Basis-, Querschnitts- und Infrastruktur-IT **soll** anhand der *IT-Rahmenarchitektur* festgelegt werden.
2. Die Verpflichtung zur Nutzung und Leistung **soll** durch *Wirtschaftlichkeit* nachgewiesen werden (u.a. WiBe⁷⁶).

Begründung

- Die Nutzung gemeinsamer Basis-, Querschnitts- und Infrastrukturdienste dient der Harmonisierung und Konsolidierung der IT.

Abhängigkeiten

- Keine

Implikationen

1. Für alle Funktionen und Anwendungsbereiche, für die Basis-, Querschnitts- und Infrastrukturdienste bereitgestellt werden, werden die evtl. vorhandenen eigenen Lösungen zukünftig abgelöst.
2. Anwendungen und Dienste, die die entsprechenden Funktionen nutzen, werden entsprechend umgestellt.
3. Mit der Eintragung eines Dienstes im Produktkatalog als angekündigter Dienst führt die nutzende Behörde notwendige Vorbereitungsmaßnahmen mit Prüfung der späteren Nutzung anhand der eigenen Anforderungen und Bedarfe durch.
4. Nutzende Behörden und IT-Dienstleister stimmen sich im Rahmen von Projekten und Aufträgen über die gegenseitige Nutzungs- und Leistungsverpflichtung ab.
5. Für Behörden mit Bedarf zur Nutzung von geplanten oder angekündigten Diensten vor der Produktivsetzung werden durch die Maßnahmen entsprechende Transitionspapiere (Zwischen- / Übergangslösung) bereitgestellt.

⁷⁶Rat der IT-Beauftragten der Ressorts, Beschluss Nr. 2015/3 vom 19. Februar 2015 (WiBe-Fachkonzept) - Version 5.0, 2015, verfügbar unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/it-beschaffung/wirtschaftlichkeitsbetrachtung/wibe5-0/wibe-fachkonzept-5-0.pdf?__blob=publicationFile&v=4, zuletzt abgerufen am 21. August 2024.

ID: V-9025-R04

FV-02 Dienste- und Schnittstellenbeschreibung

Die Beschreibung von Diensten und Schnittstellen **muss standardisiert** dokumentiert sein.

Regeln

1. Die Beschreibung von Diensten und Schnittstellen **muss** spezifisch hinsichtlich *Utility* (Funktions- und Leistungsumfang), *Warranty* (Leistungsqualität) und *Service Design Aspekten* (u.a. Organisation, technischer Aufbau) gestaltet sein.
2. Die Beschreibung von Diensten und Schnittstellen **muss** vorhandene *Regelungen* und *Templates* (u.a. Steckbriefe, Muster) berücksichtigen.
3. Die Beschreibung von Schnittstellen **muss** *Ein- und Ausgabeparameter* sowie *Verhalten* detailliert umfassen.
4. Die Beschreibung **muss** *alle* Funktionen und Schnittstellen umfassen (vollumfänglich, keine versteckten und undokumentierten).

Begründung

- Sowohl die Merkmale eines Dienstes aus Kundinnen- und Kunden- bzw. Nutzendensicht (*Utility*, *Warranty*, *Schnittstellen*) als auch aus Dienstleistersicht (*Service Design Aspekte*, *Schnittstellen*) sind für die Modularisierung, die lose Koppelung, die Interoperabilität und die Reduzierung der Komplexität entscheidend.
- Weiterhin kann eine effektive Zugriffskontrolle und -steuerung nur dann etabliert werden, wenn sämtliche Schnittstellen und Funktionen bekannt sind.
- Die Sicherheit wird gestärkt, da keine versteckten Funktionen bestehen.

Abhängigkeiten

- GV-05 Prozessmanagement

Implikationen

1. Es sind übergreifende Vorgaben für die Dokumentation von Diensten und Schnittstellen festzulegen.
2. Diese Vorgaben für die standardisierte Dokumentation sind bei Entwurf, Entwicklung und Bereitstellung von Diensten zu berücksichtigen.

ID: V-9040-R04

FV-05 Information und Daten

Information und Daten **sollen** standardisiert *beschrieben, ausgetauscht, gemanagt* und *bereitgestellt* werden.

Regeln

1. Informationen und Daten (inklusive Metadaten) **sollen** anhand einheitlicher *Standards, Formate* und *Zeichensätze* beschrieben, verlinkt und ausgetauscht werden (u.a. FAIR⁷⁷).
2. Informationen und Daten **sollen** für die Nutzung hinsichtlich *Kosten* und *Aufwand* bewertet werden.
3. Informationen und Daten **sollen** einheitlich *gemanagt* (insbesondere Erhebung, Analyse, Verarbeitung, Speicherung, Archivierung, Löschung, Nutzung) werden.
4. Daten **müssen** zum elektronischen Abruf öffentlich *bereitgestellt* werden (EGovG⁷⁸, Sunlight⁷⁹).
5. Die öffentliche Bereitstellung von Daten **muss** anhand § 12a – Gesetz zur Förderung der elektronischen Verwaltung erfolgen.

Begründung

- Der Einsatz von einheitlichen Austauschformaten erleichtert die Kooperation der beteiligten Organisationen.
- Damit geht eine höhere Effektivität in der Aufgabenerfüllung der Behörden einher.
- Der Einsatz von standardisierten Zeichensätzen und -kodierungen erleichtert die Kooperation der beteiligten Organisationen, insbesondere bei der Erfassung von Namen zur korrekten Identifikation von Personen.
- Damit geht eine höhere Effektivität in der Aufgabenerfüllung der Behörden einher.
- Die einheitliche Abbildung von Metadaten in verschiedenen Kontexten erleichtert die automatisierte Zuordnung und Auswertung von Metadaten.
- Fast alle Behörden arbeiten mit Daten, die einen räumlichen Bezug aufweisen (Geodaten).

⁷⁷Scientific Data, The FAIR Guiding Principles for scientific data management and stewardship, 2016, verfügbar unter <https://www.nature.com/articles/sdata201618>, zuletzt abgerufen am 14. März 2024.

⁷⁸Bundesgesetzblatt - Bundesministerium der Justiz, E-Government-Gesetz vom 25. Juli 2013 (BGBl. I S. 2749) zuletzt geändert durch Artikel 2 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245), verfügbar unter <http://www.gesetze-im-internet.de/egovg/EGovG.pdf>, zuletzt abgerufen am 30. Januar 2024.

⁷⁹GovData, Die zehn Open-Data-Kriterien der Sunlight-Foundation, 2014, verfügbar unter https://www.govdata.de/documents/10156/18448/GovData_Open-Data-Kriterien_der_Sunlight_Foundation.pdf/dca8fea0-8e04-4de0-8531-2bc3e8d4abc0, zuletzt abgerufen am 14. März 2024.

- Das Architekturkonzept der GDI-DE stellt insbesondere unter Beachtung der gesetzlichen Pflichten sicher, dass gängige Standards im Geoinformationswesen einheitlich und kompatibel innerhalb der Verwaltung in Deutschland angewendet werden können.
- Nur durch eine konsequente Umsetzung der organisationsinternen Regelungen hinsichtlich des Umgangs mit Daten können die sich daraus ergebenden Mehrwerte, wie z. B. die Steigerung der Datenqualität und das Treffen datengestützter Entscheidungen, voll ausgeschöpft werden.
- Zudem ermöglicht das operative Datenmanagement die Betrachtung von Daten hinsichtlich ihres gesamten Lebenszyklus.
- Die (semantische) Verknüpfung von Daten mittels Linked Data erhöht die Verwendbarkeit der Daten und fördert unter anderem die Möglichkeit des Einsatzes im Rahmen von Anwendungen der Künstlichen Intelligenz.
- Open Data fördert ein offenes Regierungs- und Verwaltungshandeln und stärkt die Ziele aus der europäischen Datenstrategie⁸⁰ wie z. B. der Aufbau eines gemeinsamen Daten-Ökosystems, die verstärkte Datennachnutzung, die Innovationsförderung und die Stärkung des Wirtschaftsstandorts Deutschland.
- Das E-Government-Gesetz⁸¹ und Datennutzungsgesetz⁸², bilden die Grundlage und Verpflichtung für die Bereitstellung von offenen Verwaltungsdaten und im Grundsatz auch von Forschungsdaten.
- Die Bereitstellung offener Verwaltungsdaten durch den formalen Austauschstandard für offene Verwaltungsdaten DCAT-AP.de im nationalen Metadatenportal GovData erleichtert den Datenzugang auf sämtlichen Verwaltungsebenen und unterstützt gleichzeitig den Aufbau eines europäischen Datenbinnenmarktes, ein Ziel aus der Europäischen Datenstrategie⁸³, indem die Daten in das Europäische Metadatenportal (EDP) überführt werden.

Abhängigkeiten

- AV-04 Datenbasiertes Handeln

⁸⁰Europäische Kommission, Eine europäische Datenstrategie - Die EU zum Vorbild für eine digitale Gesellschaft machen, 2024, verfügbar unter https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de, zuletzt abgerufen am 14. März 2024.

⁸¹Bundesgesetzblatt - Bundesministerium der Justiz, E-Government-Gesetz vom 25. Juli 2013 (BGBl. I S. 2749) zuletzt geändert durch Artikel 2 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245), verfügbar unter <http://www.gesetze-im-internet.de/egovg/EGovG.pdf>, zuletzt abgerufen am 30. Januar 2024.

⁸²Bundesgesetzblatt - Bundesministerium der Justiz, Datennutzungsgesetz vom 16. Juli 2021 (BGBl. I S. 2941f. und 4114), 2021, verfügbar unter <https://www.gesetze-im-internet.de/dng/>, zuletzt abgerufen am 14. März 2024.

⁸³Europäische Kommission, Eine europäische Datenstrategie - Die EU zum Vorbild für eine digitale Gesellschaft machen, 2024, verfügbar unter https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de, zuletzt abgerufen am 14. März 2024.

- AV-09 Souveränität
- GV-06 Daten-Governance
- TV-05 Entwicklung

Implikationen

1. Für die Umsetzung der Vorgabe ist die regelmäßige Prüfung der Mindestanforderungen von genutzten Austauschformaten zu berücksichtigen.
2. Für eine Nutzung von Geodaten und Geodatendiensten sind u. U. Änderungen bei den Einstellungen in Grundanwendungen wie z. B. im Browser notwendig.
3. Eine Nichtumsetzung der verbindlichen Vorgaben aus den europäischen INSPIRE-Regelungen kann zu einem Vertragsverletzungsverfahren seitens der Europäischen Kommission gegenüber der Bundesrepublik Deutschland führen.
4. Die bei der Umsetzung gemachten Erfahrungen sind bei der Weiterentwicklung der Regelungen zu beachten.
5. Es ist zu beachten, dass schutzbedürftige Daten entsprechend ihres Schutzbedarfs veröffentlicht werden.
6. Es ist zu beachten, dass keine personenbezogenen Daten für einen unberechtigten Empfängerkreis veröffentlicht werden.
7. Die Einführung und Befolgung von funktionalen und organisatorischen Strukturen und Prozessen zur öffentlichen Bereitstellung von Daten sind wichtige Bausteine zur Einhaltung der Vorgabe.
8. Die öffentliche Bereitstellung der Daten sollte bereits bei der Datenerhebung mit dem „Open by default“-Prinzip beachtet werden.

ID: V-9028-R05

FV-08 Schutz

Der Schutz von sensiblen Informationen **muss** durch bedarfsgerechte *Schutzmechanismen* gewährleistet werden.

Regeln

1. Der Schutz **muss** für *Identitätsinformationen* inklusive *identitätsbeschreibender Attribute* (u.a. Rollen) und *Berechtigungsrichtlinien* (u.a. Access Control Policies) gewährleistet werden.
2. Zum Schutz **muss** jeder *Zugriff* auf Ressourcen durchgängig sichergestellt werden (Access Management).
3. Zum Schutz **muss** ein *Informationssicherheitskonzept* gemäß BSI Grundschutz erstellt, umgesetzt und regelmäßig auditiert werden.
4. Zum Schutz **müssen** *Schutzbedarf* und *Quality of Service* von IT-Lösungen und Ressourcen festgelegt, überprüft und gewährleistet werden.
5. Zum Schutz **müssen** passfähige *Trennungs- und Vertrauensmechanismen* (inklusive Separierung, Segmentierung und Mandantentrennung) sichergestellt werden.
6. Zum Schutz **müssen** *Sicherheitseinstellungen* aktiviert und regelmäßig auditiert werden (Systemgrundkonfiguration, Audits).

Begründung

- Eine Integration von IAM-System und -Dienst ist nur dann möglich, wenn alle für die Zugangs- und Zugriffssteuerung des Dienstes benötigten Informationen auch extern abfragbar sind.
- Identity und Access Management muss ganzheitlich gesehen werden und bezogen auf Zugang und Zugriff auf eine Ressource einen durchgängigen Schutz bieten.
- Dies gilt ebenfalls für privilegierte Identitäten, wie z. B. die Administrierenden.
- Integraler Bestandteil der Sicherheitskonzeption im Sinne des ISM.
- Die Festlegung von Schutzbedarf und Quality of Service ist die Basis für die Sicherheitskonzeption.
- „Security by Design“ ist das zentrale Element einer ganzheitlichen Sicherheitskonzeption, um über alle Lebenszyklen eines IT-Verfahrens die passenden Informationssicherheitsanforderungen zu berücksichtigen.
- Separierung/ Mandantentrennung ist ein wichtiges Element, um komplexen Angriffen in einer gemeinsam genutzten IT-Umgebung zu begegnen.
- Eine sichere Grundkonfiguration von IT-Lösungen stellt sicher, dass Nutzende keine eigenständigen Sicherheitseinstellungen vornehmen müssen und die IT-Lösung bereits in einem sicheren Zustand bereitgestellt wird.
- Ferner erhöht eine sichere Grundkonfiguration den Schutz der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität.

Abhängigkeiten

- AV-08 Sicherheit und Schutz

Implikationen

1. Die Etablierung zentraler Sicherheitsdienste, welche durch Querschnittsdienste genutzt werden, stellt besondere Anforderungen an deren Sicherheit, Performance und Verfügbarkeit.
2. Selbst wenn nicht die Komponenten des IAM zur Zugriffssteuerung genutzt werden, sondern auf die im jeweiligen Dienst integrierte Access Control Funktionalität zurückgegriffen wird, muss die Einhaltung der Anforderung sichergestellt werden.
3. Entsprechende Prozesse und Maßnahmen sind bezogen auf die Einführung zu definieren (z. B. Penetration Testing der Anwendung oder Code Reviews).
4. Ein Informationssicherheitskonzept unterstützt das Compliance-Management von IT-Verfahren.
5. Die Festlegung von Schutzbedarf und Quality of Service ist maßgeblich für die zu ergreifenden IT-Sicherheitsvorkehrungen bei der Entwicklung und Implementierung von IT-Verfahren^{84 85 86}.
6. Aspekte der Informationssicherheit sind bereits beim Entwurf von IT-Verfahren zu berücksichtigen. U. a. sind die Implikationen aus technischen Anhängen zu beachten.
7. Bei übergreifend konzipierten IT-Verfahren ist bereits zum Zeitpunkt der Konzeption eine Separierung/ Mandantentrennung nach Anforderungen der Nutzerbehörde zu berücksichtigen.
8. Vor Inbetriebnahme neuer IT-Systeme sollten notwendige Schutzmaßnahmen (wie z. B. die Konfigurationsempfehlungen des BSI⁸⁷) evaluiert und durch entsprechende Sicherheitseinstellungen beachtet werden.
9. Es ist zu beachten, dass die Sicherheitseinstellungen, die die höchste Sicherheit gewährleisten, der Nutzerfreundlichkeit entgegenstehen können.
10. Bei der Aktivierung der Sicherheitseinstellungen sollte der zur Bewältigung der Aufgabenstellung benötigte Funktionsumfang beachtet werden.

⁸⁴Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-1 - Managementsysteme für Informationssicherheit (ISMS), 2017, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 12. März 2024.

⁸⁵Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-2 - IT-Grundschutz-Methodik, 2017, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 12. März 2024.

⁸⁶Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-3 - Risikoanalyse auf der Basis von IT-Grundschutz, 2017, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 12. März 2024.

⁸⁷Bundesamt für Sicherheit in der Informationstechnik, SiSyPHuS Win10: Empfehlung zur Härtung von Windows 10 mit Bordmitteln, 2022, verfügbar unter https://www.bsi.bund.de/Service-Navi/Publicationen/Studien/SiSyPHuS_Win10/AP11/SiSyPHuS_AP11_node.html, zuletzt abgerufen am 14. März 2024.

ID: V-9024-R04

FV-09 Entkopplung

Die Entkopplung (lose Kopplung) **soll** *optimiert* werden.

Regeln

1. Zur Entkopplung (losen Kopplung) von Diensten und IT-Komponenten **sollen** *offene Standards* und *Datenmodelle* eingesetzt werden.
2. Bei Entkopplung (loser Kopplung) **sollen** *Abhängigkeiten* zwischen IT und insbesondere zu spezifischen Laufzeitumgebungen und Software-Komponenten minimiert werden.
3. Zur Entkopplung (loser Kopplung) **soll** die Bereitstellung von IT *serverbasiert*, der Zugriff über den *Webbrowser* und die *clientseitige Integration* nur im Einzelfall erfolgen.

Begründung

- Wesentliche Voraussetzung für die lose Koppelung von Diensten sind wohl definierte und standardisierte Schnittstellen, welche die gesamte Interaktion eines Dienstes mit der Umgebung abdecken.
- Die spezifischen Details der Implementierung eines Dienstes müssen damit in der Umgebung (z. B. bei anderen Diensten) nicht bekannt sein.
- Weiterhin wird die Wiederverwendung und Wartung sowie die Zugriffskontrolle und -steuerung erleichtert.
- Damit werden Effizienz- und Standardisierungsvorteile realisiert.
- Die lose Kopplung ermöglicht durch die geringe Abhängigkeit zwischen einzelnen Komponenten eine schnelle und flexible Anpassung von IT-Lösungen und vereinfacht ihre Verwaltung, Erprobung, Weiterentwicklung und Wartung.

Abhängigkeiten

- AV-10 Skalierbarkeit

Implikationen

1. Die Vorgabe soll beim Entwurf, der Entwicklung und der Bereitstellung von Diensten berücksichtigt werden, wobei ein übergreifendes Schnittstellenmanagement unterstützend zu etablieren ist.
2. Bei der Umsetzung der losen Kopplung sollten gängige Architektur und Entwurfsmuster berücksichtigt werden.⁸⁸

⁸⁸Institute of Electrical and Electronics Engineers, Design patterns in object oriented analysis and design, 2011, verfügbar unter <https://ieeexplore.ieee.org/abstract/document/5982229>, zuletzt abgerufen am 14. März 2024.

3. Die bei der Umsetzung der losen Kopplung entstehende Komplexität sollte beachtet werden.
4. Der erhöhte Planungs- und Umsetzungsaufwand, der durch die Entkopplung von Diensten entsteht, sollte beachtet werden.

2.4 Technische Vorgaben

Die technischen Vorgaben beschreiben die technische Realisierung von Informationstechnik und Digitalisierung inklusive der relevanten Technologien, Entwicklungs- und Implementierungsaktivitäten sowie technischen Daueraufgaben und Infrastrukturaspekten. Sie dienen einer Bewertung und Einordnung von Architekturentscheidungen bezogen auf die technische Umsetzbarkeit und dienstleisterseitige Leistungserbringung.

ID: V-9034-R04

TV-01 Administration

Die Administration **soll** über standardisierte *Prozesse* erfolgen.

Regeln

1. Die Administration **soll** über automatisierte *kontinuierliche Bereitstellung* (Continuous Integration, Deployment, Delivery - DevOps) erfolgen.

Begründung

- keine

Abhängigkeiten

- AV-10 Skalierbarkeit
- TV-10 Betrieb

Implikationen

1. Keine

ID: V-9071-R04

TV-02 Schnittstellen

Die Schnittstellen **sollen** *standardisiert* implementiert und genutzt werden.

Regeln

1. Die Schnittstellen **sollen** *reduziert* und auf Basis offener *Standards* implementiert und genutzt werden.
2. Die Schnittstellen **müssen** *dokumentiert* werden.
3. Die Schnittstellen **müssen** hinsichtlich der *Protokolldaten* zugänglich sein.

Begründung

- Die Komplexität der IT-Landschaft und der Aufwand für das Management steigen mit der Anzahl an IT-Lösungen und Verbindungen zwischen diesen.
- Zur Minimierung soll die Standardisierung gestärkt werden und die Komplexität kontrolliert gemanagt werden.
- Für die Ausgestaltung sind die Festlegungen in den Architekturen und für die Standardisierung die verfügbaren Standards in den technischen Vorgaben und technischen Spezifikationen zu verwenden.
- Die Stärkung der Entkopplung und Informationssicherheit wird durch eine überschaubare Anzahl an standardisierten Schnittstellen befördert.

Abhängigkeiten

- AV-02 Interoperabilität
- AV-08 Sicherheit und Schutz
- AV-09 Souveränität
- AV-10 Skalierbarkeit

Implikationen

1. Die Behörden verbinden die in ihrer Hoheit liegenden Dienste oder IT-Lösungen über die wenigen Standardschnittstellen und -APIs.
2. Individualanbindungen müssen begründet, im Architekturmanagement begleitet und gepflegt sowie gesondert beauftragt und finanziert werden.
3. Die Anzahl der bilateralen und individuellen Schnittstellen wird sinken.
4. Die Integrationstiefe wird auf ein in Architekturen definiertes Standardniveau festgelegt.

ID: V-9032-R04

TV-05 Entwicklung

Die Entwicklung **soll** *standardisiert* erfolgen.

Regeln

1. Die Entwicklung **soll** quelloffene standardisierte *Entwicklungswerkzeuge* mit adäquatem Support (Programme, Frameworks, Bibliotheken) verwenden.
2. Die Entwicklung **soll** standarisierter *Programmiersprachen* sowie *Entwicklungs- und Laufzeitumgebungen* verwenden.
3. Die Entwicklung **muss** einem standardisierten *Qualitätsmanagement* unterliegen.
4. Die Entwicklung **muss** *Quellcode* und *Artefakte* versionieren und *Entwicklungswissen* dokumentieren.
5. Die Entwicklung **muss** *Analyse* und *Tests* berücksichtigen (insbesondere Codeanalyse, Softwaretests, Lasttests, Vulnerability Scans).

Begründung

- Die Standardisierung ermöglicht eine Vereinfachung der Programmierung durch einheitliche Sprache und Reduzierung des Schulungsaufwandes sowie bessere Portierbarkeit bei einem Wechsel des DBS.
- Durch die Verwendung standardisierter Cloud-Entwicklungsumgebungen wird die Herstellerabhängigkeit reduziert und die Koordination von internen und externen Entwickelnden erleichtert.
- Des Weiteren bleibt die Hoheit über die Anwendungen bei den Auftragenden ebenso erhalten wie die Offenheit für moderne Entwicklungsansätze wie zum Beispiel agile Vorgehensweisen, Lean Management und DevOps.
- Ein hoher Grad an Automatisierung soll die Qualität der Entwicklungen zusätzlich fördern.
- Durch die Verwendung standardisierter Programmiersprachen und Entwicklungs- und Laufzeitumgebungen wird die Herstellerabhängigkeit reduziert und IT-Personal kann flexibler für unterschiedliche Aufgaben eingesetzt werden.
- Mit der Verwendung quelloffener Entwicklungswerkzeuge wird die Betriebsfähigkeit der Verfahren dauerhaft sichergestellt.
- Durch einen kontinuierlichen Prozess des Qualitätsmanagements werden Fehler im Entwicklungsprozess frühzeitig erkannt.
- Nötige Änderungen können schneller eingearbeitet werden.

- Außerdem wird die Sicherheit der Anwendung erhöht.
- Insgesamt wird die Qualität der Anwendungen verbessert.

Abhängigkeiten

- AV-04 Datenbasiertes Handeln
- GV-06 Daten-Governance
- TV-02 Schnittstellen

Implikationen

1. Die IT-Dienstleister stellen in deren Standardkatalogen Empfehlungen von offenen Elementen, Entwicklungswerkzeugen, Bibliotheken und Standards vor.

ID: V-9047-R04

TV-08 Protektion

Die Protektion **muss** durch technische *Sicherheitssysteme* sichergestellt werden.

Regeln

1. Die Protektion **muss** durch *kryptografische Verfahren* nach dem Stand der Technik sichergestellt werden (BSI TR-02102 Empfehlungen und Schlüssellängen inklusive TLS, IPsec und SSH⁸⁹, BSI TR-03116 Vorgaben⁹⁰).
2. Die Protektion **muss** durch *Protokollierung* von Ereignissen und *Detektion* von Cyberangriffen sichergestellt werden (u.a. BSI Mindeststandard Protokollierung und Detektion⁹¹, BSI OPS.1.1.5 Protokollierung⁹², BSI DER.1 Detektion⁹³).
3. Die Protektion **muss** durch *Virenschutz* und *Schadprogrammabwehr* nach aktuellem Stand der Technik sichergestellt werden (u.a. OPS.1.1.4 Schadprogramme⁹⁴).

Begründung

- Kryptografische Verfahren sind ein zentrales Instrument, um die Schutzziele „Vertraulichkeit“ und „Integrität“ der verarbeiteten Informationen angemessen und wirksam sicherzustellen.
- Zielgerichtete Handlungen gegen die Informationssicherheit lassen sich nur durch die detaillierte Analyse von Protokollierungsdaten erkennen.
- Die Sicherstellung der Schadprogrammabwehr ist ein integraler Bestandteil der Sicherheitskonzeption im Sinne des ISM.

Abhängigkeiten

⁸⁹Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 2024, verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html, zuletzt abgerufen am 26. August 2024.

⁹⁰Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, 2024, verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03116/TR-03116_node.html, zuletzt abgerufen am 26. August 2024.

⁹¹Bundesamt für Sicherheit in der Informationstechnik, Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 29. Juni 2023, 2023, verfügbar unter https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/PDCA/PDCA_node.html, zuletzt abgerufen am 12. März 2024.

⁹²Bundesamt für Sicherheit in der Informationstechnik, OPS.1.1.5: Protokollierung (Edition 2023), 2023, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_1_1_5_Protokollierung_Edition_2023.pdf?__blob=publicationFile&v=3, zuletzt abgerufen am 26. August 2024.

⁹³Bundesamt für Sicherheit in der Informationstechnik, DER.1: Detektion von sicherheitsrelevanten Ereignissen (Edition 2023), 2023, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/IT-GS-Kompendium_Einzel_PDFs_2023/05_DER_Detektion_und_Reaktion/DER_1_Detektion_von_sicherheitsrelevanten_Ereignissen_Edition_2023.pdf?__blob=publicationFile&v=3, zuletzt abgerufen am 26. August 2024.

⁹⁴Bundesamt für Sicherheit in der Informationstechnik, OPS.1.1.4: Schutz vor Schadprogrammen (Edition 2022), 2022, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/IT-GS-Kompendium_Einzel_PDFs_2022/04_OPS_Betrieb/OPS_1_1_4_Schutz_vor_Schadprogrammen_Edition_2022.pdf?__blob=publicationFile&v=3, zuletzt abgerufen am 26. August 2024.

- AV-08 Sicherheit und Schutz

Implikationen

1. Die für IT-Verfahren umgesetzten kryptographischen Verfahren sind stets unter Beachtung der Technischen Richtlinien des BSI auf dem aktuellen Stand der Technik zu halten.
2. Die Konzeption muss turnusmäßig überprüft werden.
3. Bereits bei der Konzeption von IT-Verfahren ist ein Protokollierungskonzept zu erstellen und im Weiteren zu berücksichtigen.
4. Die Meldepflichten gemäß § 4 Abs. 6 BSIG i. V. m. der AVV zum BSIG sind zu beachten.
5. Um dem nachzukommen, ist ein Prozess für ein Sicherheitsvorfallmanagement zu etablieren.
6. Umfang und Leistung der o. g. Schutzsysteme sind an die aktuellen Bedrohungsszenarien anzupassen. Weiterhin ist dies auch in Bezug auf Clients zu berücksichtigen.

ID: V-9036-R05

TV-09 Kommunikation

Die Kommunikation **soll** über *zentral bereitgestellte Verbindungen* genutzt werden.

Regeln

1. Die Kommunikation **soll** über zentral bereitgestellte gesicherte *Netze, Netzanschlüsse, Netzzugänge, Netzkopplungen* und *Netzübergänge* erfolgen (u.a. IVÖV⁹⁵, KTN⁹⁶).
2. Die Kommunikation **soll** durch *netznahe Dienste* (u.a. E-Mail, PKI, X500) unterstützt werden.
3. Die Kommunikation **muss** innerhalb der definierten *Netzzonen* (u.a. Grundschatz, Hoch) oder entlang des *Sicherheitsgefälles* erfolgen.
4. Die Kommunikation **muss** vollständig über *IPv6* funktionsfähig sein (u.a. LIR de.government⁹⁷, IPv6 Netzinfrastrukturen⁹⁸, IPv6 Adresskonzept⁹⁹, IPv6 Routing¹⁰⁰).

Begründung

- Die Nutzung der Protokollversion 4 (IPv4) wird weltweit durch die Version 6 (IPv6) abgelöst, da IPv4 langfristig mangels verfügbarem Adressraum keine Zukunftsfähigkeit bietet.
- IPv4-Adressen, die aus dem Internet angesprochen werden können, sind für die öffentliche Hand nur noch zu ständig steigenden Preisen und in kleinen Mengen verfügbar.
- Die Unterstützung von IPv4 in Netzwerken sowie herstellerseitig in IT-Komponenten und zugehörigen Serviceverträgen schwindet.

Abhängigkeiten

- Keine

Implikationen

⁹⁵Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, Informationsverbund der öffentlichen Verwaltung, 2024, verfügbar unter https://www.bdbos.bund.de/DE/Aufgaben/IVOEV/ivoev_node.html, zuletzt abgerufen am 27. August 2024.

⁹⁶Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, Kerntransportnetz des Bundes, 2024, verfügbar unter https://www.bdbos.bund.de/DE/Aufgaben/KTN-Bund/ktn-bund_node.html, zuletzt abgerufen am 27. August 2024.

⁹⁷Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, Local Internet Registry de.government, 2024, verfügbar unter https://www.bdbos.bund.de/DE/Aufgaben/LIRdeGovernment/lirdegovernment_node.html, zuletzt abgerufen am 27. August 2024.

⁹⁸Konferenz der IT-Beauftragten der Ressorts, Beschluss Nr. 2020/14 vom 11. November 2020 - Zukunftsfähige Netzinfrastrukturen auf Basis von funktionsfähigem IPv6, 2020, verfügbar unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/cio-bund/steuerung-it-bund/beschluesse_cio-board_KoITB/2020_14_Beschluss_Konferenz_IT_Beauftragte.pdf?__blob=publicationFile&v=3, zuletzt abgerufen am 12. März 2024.

⁹⁹IT-Planungsrat, Beschluss Nr. 2011/04 vom 3. März 2011 - IPv6 für die öffentliche Verwaltung Deutschlands - Adresskonzept und Eckpunkte der Organisation, 2011, verfügbar unter https://www.it-planungsrat.de/fileadmin/beschluesse/2011/Beschluss2011-04_Bericht_IpV6.pdf, zuletzt abgerufen am 27. August 2024.

¹⁰⁰IT-Planungsrat, Beschluss Nr. 2016/43 vom 13. Oktober 2016 - IP-Adressverwaltung, 2016, verfügbar unter https://www.it-planungsrat.de/fileadmin/beschluesse/2016/Beschluss2016-43_24_Anlage1_IP_Adressverwaltung.pdf, zuletzt abgerufen am 27. August 2024.

1. Unter Berücksichtigung des Schutzbedarfes der verarbeiteten Informationen und der Netzwerkinfrastruktur soll eine entsprechende Segmentierung der lokalen Netze der Nutzenden realisiert werden.
2. Die Implikationen der flächendeckenden Einführung von IPv6 sind aufgrund der vielfachen Abhängigkeiten sehr groß und werden dramatisch größer, je länger dessen Einführung hinausgezögert wird. Neben dem finanziellen Aufwand sind Ressourcenengpässe bei Dienstleistern und Schulung zu erwarten, sodass dann eine kurzfristige Umsetzung bei akutem Bedarf nicht realistisch ist.¹⁰¹
3. Bei der Einführung von IPv6 muss beispielsweise berücksichtigt werden, ob
 - Der Netzbereich und seine Anwendung weitgehend autark sind und somit auf IPv4 vollständig verzichtet werden kann (IPv6 only). Beispiele:
 - VoIP innerhalb einer Behörde
 - MPLS WAN Netz zwischen Behörden mit IPSec Tunnelverschlüsselung
 - Für den technischen Übergang der parallele Einsatz von IPv6 und IPv4 notwendig ist.
 - Normalfall in der öffentlichen Verwaltung
 - Technologiefestlegung IT-PLR: Dual Stack
 - Von IPv6 als Standardprotokoll und IPv4 als in Teilen notwendiger Lösung für den Bestandsschutz ausgegangen werden muss, bezogen auf:
 - IT-Konzepten, inkl. Sicherheitskonzepten
 - IT-Hardwarekomponenten
 - IT-Softwarekomponenten (insbesondere Einzelentwicklungen – Fachverfahren für Behörden)

¹⁰¹Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, Local Internet Registry de.government, 2024, verfügbar unter https://www.bdbos.bund.de/DE/Aufgaben/LIRdeGovernment/lirdegovernment_node.html, zuletzt abgerufen am 27. August 2024.

ID: V-9078-R03

TV-10 Betrieb

Der Betrieb **muss** *standardisiert* erfolgen.

Regeln

1. Der Betrieb **muss** die Kriterien für die Nutzung *externer (Cloud) IT-Leistungen* einhalten (u.a. Inhouse und Kauf First, LockIn¹⁰², externe Cloud-Dienste¹⁰³).
2. Der Betrieb **muss** *standardisierte (Cloud) Betriebsumgebungen* bereitstellen, *Kompatibilität* sicherstellen und *Cloud* priorisieren (u.a. DVS¹⁰⁴, DVC¹⁰⁵, GaiaX¹⁰⁶, SCS¹⁰⁷, BSI IT-Grundschutz OPS: Betrieb¹⁰⁸, HV-Benchmark¹⁰⁹).
3. Der Betrieb **soll** *standardisierte Prozessorarchitekturen* und *Serverbetriebssysteme* für *Hostrechner* nutzen.
4. Der Betrieb **soll** *einheitliche Technologien* für *Server* und *Laufzeitumgebungen* verwenden.
5. Der Betrieb **muss** in der Beschaffung die *ergänzenden Vertragsbedingungen Cloud* anwenden (EVB-IT Cloud¹¹⁰).

Begründung

- Durch Befolgen der Kriterien und Anforderungen wird der Regelbetrieb einschließlich angemessener Maßnahmen für Planung, Protokollierung und Überwachung von Ereignissen sowie der Umgang mit Störungen, Fehlern, Schwachstellen und Sicherheitsupdates sichergestellt.
- Ziel ist eine weitgehende Standardisierung und Ausrichtung aller Infrastrukturkomponenten im Sinne der Rechenzentrumskonsolidierung.

¹⁰²Rat der IT-Beauftragten, Beschluss Nr. 2015/5 vom 29. Juli 2015 - Kriterien für die Nutzung von Cloud-Diensten der IT-Wirtschaft, 2015, verfügbar unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/it-rat/beschluesse/beschluss_2015_05.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 12. März 2024.

¹⁰³Bundesamt für Sicherheit in der Informationstechnik, Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG zur Nutzung externer Cloud-Dienste in der Bundesverwaltung, 2022, verfügbar unter https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html, zuletzt abgerufen am 12. März 2024.

¹⁰⁴IT-Planungsrat, Beschluss Nr. 2021/46 vom 29. Oktober 2021 - Deutsche Verwaltungscloud-Strategie, 2021, verfügbar unter <https://www.it-planungsrat.de/beschluss/beschluss-2021-46>, zuletzt abgerufen am 12. März 2024.

¹⁰⁵govdigital eG, Deutsche Verwaltungscloud (DVC), 2024, verfügbar unter <https://deutsche-verwaltungscloud.de/>, zuletzt abgerufen am 27. August 2024.

¹⁰⁶Gaia-X Hub Germany c/o acatech - Deutsche Akademie der Technikwissenschaften, Gaia-X Hub Germany, 2024, verfügbar unter <https://gaia-x-hub.de/>, zuletzt abgerufen am 27. August 2024.

¹⁰⁷Open Source Business Alliance - Bundesverband für digitale Souveränität e.V., Sovereign Cloud Stack, 2024, verfügbar unter <https://scs.community/de/>, zuletzt abgerufen am 27. August 2024.

¹⁰⁸Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Bausteine (Edition 2023) - OPS Betrieb, 2023, verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition.html, zuletzt abgerufen am 26. August 2024.

¹⁰⁹Bundesamt für Sicherheit in der Informationstechnik, Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG zum HV-Benchmark kompakt 5.0 Version 2.0, 2023, verfügbar unter https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/HV-Benchmark-kompakt/HV-Benchmark-kompakt_node.html, zuletzt abgerufen am 12. März 2024.

¹¹⁰Der Beauftragte der Bundesregierung für Informationstechnik, Aktuelle EVB-IT, 2024, verfügbar unter <https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/it-beschaffung/evb-it-und-bvb/evb-it/evb-it-node.html>, zuletzt abgerufen am 27. August 2024.

- Eine standardisierte Prozessorarchitektur ermöglicht die Entwicklung von Software und den Einsatz von Systemkomponenten gegen eine definierte Plattform.
- Die Kompatibilität und Interdependenzen zu anderen eingesetzten Technologien und Infrastrukturen aus dem Standardkatalog sind notwendig, um die Ziele der IT-Konsolidierung bestmöglich zu verfolgen.
- Weiterhin wird der Betrieb durch die Nutzbarkeit von einheitlichen Installations- und Administrationswerkzeugen erleichtert und eine Reduzierung des Schulungsaufwandes erreicht.
- Durch die Konzentration auf standardisierte Funktionalitäten wird es möglich, Applikationen über unterschiedliche Serverlandschaften zu migrieren, zu konsolidieren und wirtschaftlicher zu betreiben.
- Mit der Nutzung von Cloud Computing geht eine Verlagerung der Datenhaltung und Datenverarbeitung einher, der durch die Umsetzung der Vorgabe geeignet Rechnung getragen wird.
- Die Einhaltung der Anforderungen, Kriterien und Standards gewährleistet die Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) für Daten und deren Verarbeitung und schafft somit Rechtssicherheit beim Einsatz von Cloud Computing.
- Durch die Nutzung von Cloud Computing und modularer Cloud-Infrastruktur wird die Effizienz und Effektivität in Entwicklung, Inbetriebnahme und Betrieb von Anwendungen gesteigert, das Datenmanagement optimiert und die Skalierbarkeit der Infrastrukturplattformkomponenten ermöglicht. Auch deshalb wurden die Entscheidungen des IT-Planungsrats 2020/54¹¹¹ und 2021/46¹¹² zur DVS getroffen.

Abhängigkeiten

- AV-08 Sicherheit und Schutz
- AV-10 Skalierbarkeit
- TV-01 Administration

Implikationen

1. Bereits vor der Inbetriebnahme sind die benannten Kriterien, Anforderungen und Standards zu überprüfen.
2. Vor einer Beauftragung ist festzulegen, auf welcher Betriebsumgebung und mit welchen damit verbundenen Standards und Referenzen die IT-Lösungen und Verfahren betrieben werden.
3. Beschaffte IT-Lösungen müssen mit der Prozessorarchitektur sowie dem Serverbetriebssystem kompatibel sein.

¹¹¹IT-Planungsrat, Beschluss Nr. 2020/54 vom 28. Oktober 2020 - AG Cloud Computing und digitale Souveränität, 2020, verfügbar unter <https://www.it-planungsrat.de/beschluss/beschluss-2020-54>, zuletzt abgerufen am 14. März 2024.

¹¹²IT-Planungsrat, Beschluss Nr. 2021/46 vom 29. Oktober 2021 - Deutsche Verwaltungscloud-Strategie, 2021, verfügbar unter <https://www.it-planungsrat.de/beschluss/beschluss-2021-46>, zuletzt abgerufen am 12. März 2024.

4. Ergänzend zu den Verpflichtungen des Cloud-Anbieters ist auch der Cloud-Nutzer für den sicheren Einsatz der Cloud mitverantwortlich (shared responsibility).
5. In der Gewährleistung der Sicherheit von Cloud-Infrastrukturen stellt deren Komplexität gegenüber herkömmlichen Infrastrukturen eine fachliche und technische Herausforderung dar, die auch auf organisatorischer Ebene zu berücksichtigen ist.
6. Das Cloud Computing ist im Informationssicherheitsmanagement (ISM) des Cloud-Nutzers zu berücksichtigen.
7. Die konsequente Nutzung von Cloud Computing hat Auswirkungen auf bestehende Betriebs- und Organisationskonzepte, deren Anpassung entlang der Indikatoren wie der Verfügbarkeit, Skalierbarkeit, Wirtschaftlichkeit und Automatisierung zu prüfen ist.

3 Anhang

Der Anhang enthält die Formatvorlage, die verwendeten Verbindlichkeiten, die Nutzungsgrundsätze, das Glossar und die Verzeichnisse.

3.1 Formatvorlage für die Architekturvorgabe

Um die praktische Arbeit mit den Architekturvorgaben zu erleichtern, wird jede Architekturvorgabe im Folgenden durch einen eindeutigen Bezeichner, einen aussagekräftigen Titel sowie den Verbindlichkeitsgrad gekennzeichnet.

Für eine einheitliche Darstellung und Lesbarkeit der in diesem Dokument beschriebenen Architekturvorgaben wurde die folgende, aus dem TOGAF® Framework¹¹³ adaptierte, Formatvorlage genutzt.

¹¹³The Open Group Library. The TOGAF Standard Version 9.2. Unter https://publications.opengroup.org/c182?_ga=2.209896722.686744425.1649171558-784988137.1649171558 zuletzt abgerufen am 05. April 2022.

ID: V-xxxx-Rxx (Revisions sichere Identifikationsnummer)

xV-xx xyz (Titel der Architekturvorgabe bestehend aus VorgabeID und Kernelement)

Kernvorgabe inklusive des Verbindlichkeitsgrades

Regeln

1. Konkretisieren und vervollständigen die Kernvorgabe durch einzelne eindeutige und widerspruchsfreie Regeln.
2. ...

Begründung

- Beschreibt die geschäftlichen und technologischen Vorteile der Architekturvorgabe aus fachlicher Perspektive.

Abhängigkeiten

- Beschreibt die Beziehung zu anderen Architekturvorgaben.

Implikationen

1. Beschreiben eindeutig und wertungsfrei die geschäftlichen und technologischen, teilweise nur potenziellen Auswirkungen der Architekturvorgabe auf die Stakeholder der Architekturrichtlinie (z. B. in Bezug auf Ressourcen, Kosten und Aktivitäten/ Aufgaben).
2. ...

Ergänzende Hinweise zur Formatvorlage

Im Folgenden werden die einzelnen Elemente der Vorgaben noch einmal im Detail erläutert:

Die **ID** als revisionssichere Identifikationsnummer identifiziert Änderungen an einzelnen Architekturvorgaben. Die Nummerierung erfolgt fortlaufend, wobei das Präfix V zur Kennzeichnung der Zugehörigkeit zu den Architekturvorgaben der Architekturrichtlinie vorangestellt wird. Der Mittelteil wird fortlaufend und dadurch für jede Vorgabe einmalig vergeben. Der Revisionsstand der Architekturvorgabe wird durch das Suffix gekennzeichnet, wobei R01 die initiale Version der Vorgabe kennzeichnet und bei jeder künftigen Revision der Wert um eins erhöht wird. R04 bedeutet also beispielsweise, dass die vorliegende Vorgabe die dritte Revision der initialen Version ist.

Der **Titel** ergibt sich aus dem Regelungsbereich (AV, GV, FV, TV), einer fortlaufenden Nummer (zusammen VorgabeID) und dem Kernelement der Kernvorgabe. Die Anzahl der Architekturvorgaben **muss** zur Gewährleistung der Anwendbarkeit pro Regelungsbereich auf zehn Vorgaben begrenzt sein.

Die **Kernvorgabe** wird zur schnellen Erfassbarkeit und Verständlichkeit als einzelner grammatikalisch gleich aufgebauter Satz formuliert. Die Kernvorgabe repräsentiert den Kern der Regeln.

Die **Regeln** werden zur Bewertung der Anwendbarkeit der Architekturrichtlinie einheitlich strukturiert. Die Nummerierung dient der Identifikation der einzelnen Regel und nicht der Priorisierung von Regeln untereinander. Die Identifikation einer einzelnen Regel setzt sich zusammen aus der VorgabeID und der Nummerierung in der Liste (Schema xV-xx-Rxx). Die Anzahl der Regeln **soll** zur Gewährleistung der Anwendbarkeit pro Architekturvorgabe auf fünf Regeln begrenzt sein. Die Regel **soll** in einem einzelnen und einfach verständlichen Satz geschrieben sein. Die Regeln können durch Architekturartefakte, Prüfelemente und Referenzen unterlegt werden. Diese werden für Verzeichnisse in der Architekturrichtlinie sowie als Basis für ein Architekturcontrolling verwendet. Um die Einhaltung von Architekturvorgaben und den Gesamtfortschritt überwachen zu können, sollen die Architekturvorgaben mithilfe von Kennzahlen messbar gemacht werden. Die Kennzahlen orientieren sich an den in der Beschreibung definierten Architekturartefakten, Prüfelementen und Referenzen.

Die **Begründung** beschreibt die Vorteile in der Anwendung der Architekturvorgabe. Ziel ist insbesondere die Unterstützung der Kommunikation bei den Stakeholdern und der Verknüpfung mit Zielen in relevanten Strategien und Konzepten.

Die **Abhängigkeiten** beschreiben die Beziehungen der Architekturvorgaben untereinander und damit deren Zusammenhang. Die Beziehung wird mit einem Typ der Beziehung versehen (z.B. Konkretisierung). Die einzelnen Beziehungen können ob bestehender Konkurrenz untereinander mit einer Priorisierung versehen werden.

Die **Implikationen** beschreiben die Auswirkungen auf die Stakeholder, insbesondere die Anwendenden, der Architekturrichtlinie entsprechend Abschnitt 1.3 Zielgruppe, insbesondere bei den Behörden und Dienstleistern, in der Anwendung der Architekturvorgabe. Die Anwendung und Bewertung unterliegen dabei den jeweiligen Anwendenden. Die Bewertung der Implikationen sollte sich auch auf die Regeln beziehen. Die Nummerierung dient der Identifikation der einzelnen Implikation und nicht

der Priorisierung von Implikationen untereinander. Die Identifikation einer einzelnen Implikation setzt sich zusammen aus der VorgabeID und der Nummerierung in der Liste (Schema xV-xx-Ixx). Die Anzahl der Implikationen **soll** zur Gewährleistung der Anwendbarkeit pro Architekturvorgabe auf fünf Implikationen begrenzt sein. Die Implikation **soll** in einem einzelnen und einfach verständlichen Satz geschrieben sein. Bedarfsweise können diese Bewertungen für Prozesse des Architekturcontrollings oder für Entscheidungsprozesse herangezogen werden und von diesen Stakeholdern analysiert werden.

3.2 Verbindlichkeit der Architekturvorgaben

Zur Verringerung des Interpretationsspielraums und somit besseren Verständlichkeit für die Anwenderin und den Anwender der Architekturrichtlinie wird zur Beschreibung der Architekturvorgaben eine einheitliche Beschreibungssemantik verwendet. Diese orientiert sich an RFC 2119¹¹⁴ und sieht zur Beschreibung des Verbindlichkeitsgrads einer Architekturvorgabe vier Abstufungen vor, die in der nachfolgenden Auflistung verdeutlicht werden.

Muss: kennzeichnet eine Aussage mit dem Charakter einer verbindlichen Festlegung. Anmerkungen: Der Spezifikation liegt eine verbindliche Entscheidungs-, Beschluss- oder Rechtslage oder eine einstimmige Einigung im Ressortkreis zugrunde.

Soll: kennzeichnet eine verbindliche Aussage, von der bei Vorliegen wesentlicher Gründe abgewichen werden kann. Die aus der Abweichung resultierenden Auswirkungen sind sorgfältig abzuwägen. Die Abweichungen sind zu dokumentieren. Anmerkungen: Beschreibung einer Vorgabe, von der u. a. dann abgewichen werden kann, wenn die fachliche Aufgabenerfüllung der Ressorts beeinträchtigt wäre. Abweichungen von der Vorgabe erfordern die Abwägung von Vor- und Nachteilen und die Dokumentation.

Kann: kennzeichnet eine Aussage mit dem Charakter einer gestatteten Option. Anmerkungen: Beschreibung einer zulässigen rechtlichen/ technischen Option.

Darf nicht: kennzeichnet eine Aussage mit dem Charakter eines absoluten Verbots. Anmerkungen: Beschreibung einer Vorgabe, die einen ausdrücklichen Ausschluss einer Spezifikation erfordert.

Die vorhergehende Auflistung verdeutlicht, dass der Verbindlichkeitsgrad einer Architekturvorgabe eng an das Vorliegen einer klaren Entscheidungslage gekoppelt ist. Diese kann in Form entsprechender Beschlüsse/ Rechtsnormen vorliegen bzw. im Rahmen der Ressortabstimmung zur Architekturrichtlinie getroffen worden sein.

Dies hat zwei wesentliche Implikationen auf die Architekturrichtlinie und die Beschreibung der Architekturvorgaben:

¹¹⁴Internet Engineering Task Force - Network Working Group, Request for Comments 2119 - Key words for use in RFCs to Indicate Requirement Levels, 1997, verfügbar unter <https://tools.ietf.org/html/rfc2119>, zuletzt abgerufen am 20. September 2024.

- Die Beschreibung der Architekturvorgabe wird um einen Verweis auf die entsprechende Entscheidungs-, Beschluss- oder Rechtslage (im Idealfall auf das jeweilige Quelldokument) ergänzt. Dies gilt insbesondere für Architekturvorgaben, die mit einem „MUSS“ oder einem „DARF NICHT“ als verbindlich festgelegt oder verboten sind.
- Zudem sind die dargestellten Verbindlichkeitsgrade keinesfalls als statisch zu betrachten, sondern werden entsprechend der sich ändernden rechtlichen und technologischen Rahmenbedingungen kontinuierlich angepasst.

3.3 Weiterentwicklung und Einhaltung von Architekturvorgaben

Zur Erstellung, fortlaufenden Überprüfung und bedarfsbezogenen Weiterentwicklung der in diesem Dokument dargelegten Architekturvorgaben wird der im Governance Framework COBIT 5¹¹⁵ definierte Richtlinien-Lebenszyklus herangezogen. COBIT 5 wird innerhalb des TOGAF Frameworks als Referenzwerk für IT-Governance genutzt, da es einen offenen Standard zur Steuerung der IT darstellt. Der Richtlinien-Lebenszyklus dieser Architekturrichtlinie orientiert sich an den in der folgenden



Abbildung 3: Richtlinien-Lebenszyklus COBIT 5

Abbildung erkennbaren Phasen: Jede der im COBIT Framework aufgeführten Phasen beinhaltet definierte Vorgehensweisen, die zur Erarbeitung von Prüfungs- und Steuerungsmechanismen berücksichtigt wurden. Aus diesen Mechanismen wurden anschließend die folgenden Grundsätze abgeleitet, die bei der Nutzung und Einhaltung der Architekturrichtlinie zu berücksichtigen sind:

1. Die Beachtung der in diesem Dokument aufgeführten Architekturvorgaben ist gemäß Geltungsbereich (vgl. Kapitel 1.2 Geltungsbereich) verbindlich.
2. Die Sicherstellung und Überprüfung der Einhaltung der Architekturrichtlinie ist durch das jeweilige Ressort/ die Behörde und der dort verorteten Projekte und Programme selbst vorzu-

¹¹⁵ISACA. COBIT Framework. 2019 unter <http://www.isaca.org/COBIT/Pages/default.aspx>; zuletzt abgerufen am 24. April 2019.

nehmen (z. B. durch entsprechende Kommunikations- und Schulungsmaßnahmen der zuständigen Mitarbeitenden). Abweichungen bei der Anwendung der (SOLL-) Architekturvorgaben werden die jeweils zuständigen Bereiche konsultiert, welche den Ressorts/Behörden beratend zur Seite stehen. Die hinreichende Berücksichtigung der Architekturvorgaben wird im Rahmen des zukünftigen Architekturcontrolling mithilfe von Eigenbewertungen (Self-Assessment) und Kennzahlen ermittelt. Die Erkenntnisse aus der Bewertung der Architekturvorgaben werden bedarfsweise den relevanten Entscheidungsgremien zur Verfügung gestellt.

3. Die Behörden sollten einen permanenten Feedbackprozess etablieren, um eine regelmäßige Prüfung und proaktive Anpassung und Ergänzung der Vorgaben aus ihrer operativen Aufgabenerfüllung heraus zu gewährleisten. Sollten bei Prüfung und Anwendung der Architekturvorgaben Unklarheiten oder Abweichungen auftreten, so ist der entsprechende Sachverhalt bei den jeweils zuständigen Bereichen anzuzeigen. Die im Rahmen der Fortschreibung zuständigen Bereiche werden somit in Kenntnis gesetzt¹¹⁶ und können auf dieser Basis Anpassungsbedarfe ableiten.
4. Dieses Dokument wird kontinuierlich fortgeschrieben, um ein Höchstmaß an Aktualität und einen optimalen Umfang zu gewährleisten. Hierbei wird insbesondere auf eine kontinuierliche Synchronisation der weiteren Konzepte im Zusammenhang zur Architekturrichtlinie geachtet. Die Fortschreibung und Aktualisierung dieser Architekturrichtlinie ist eine strategische und damit ministerielle Aufgabe und liegt aktuell in der Organisation des Beauftragten der Bundesregierung für Informationstechnik. Eine Beteiligung der relevanten Stakeholder wird sichergestellt.

3.4 Umgang mit konkurrierenden Architekturvorgaben

Bei der Umsetzung von IT-Vorhaben ist es möglich, dass Zielkonflikte und/oder konkurrierende Vorgaben auftreten. Zur Evaluation geeigneter Umsetzungsalternativen sollen diese konkurrierenden Ziele/Vorgaben anhand eines systematischen Entscheidungsprozesses gegeneinander abgewogen und bewertet werden. Die dazugehörige Dokumentation schafft gleichzeitig Transparenz und Vergleichbarkeit in Bezug auf die angestrebte Lösung. Im Folgenden soll eine mögliche (jedoch unverbindliche) Entscheidungsmethode vorgestellt werden. Die Methode ist immer dann anwendbar, wenn die folgenden Ausgangsbedingungen gegeben sind: Zum einen muss ein Zielkonflikt bestehen – das heißt es müssen mindestens zwei konkurrierende Vorgaben existieren. Zum anderen müssen verschiedene Alternativen zur Umsetzung des IT-Vorhabens gegeben sein. Die Umsetzung der priorisierten Vorga-

¹¹⁶Es besteht explizit keine Genehmigungspflicht auf Seiten der Projektleitung des BMI bzw. des jeweils zuständigen Bereiches des jeweils zuständigen Bereiches.

ben basiert auf einer Nutzwertanalyse¹¹⁷, welche mit dem Entscheidungsprozess der Satisfizierung¹¹⁸ kombiniert wird.

Nachfolgend werden die notwendigen Prozessschritte zur Auflösung von Zielkonflikten kursorisch dargestellt (vergleiche auch Abbildung 3).

1. Gewichtung

- Nach erfolgter Prüfung und Identifizierung der konkurrierenden Vorgaben erfolgt deren Priorisierung in Form einer **Gewichtung**. Die Vorgaben werden dafür paarweise verglichen (z. B.: Ist Vorgabe A im Vergleich zu Vorgabe B wichtiger oder weniger wichtig?), woraus sich die Gewichtungen für die Nutzwertanalyse ergeben. Dies erfolgt unabhängig von den zur Verfügung stehenden Alternativen.
- Im Anschluss wird jeder Vorgabe ein **Mindestmaß an Erfüllungsgrad** zugewiesen. Dieses Mindestmaß entspricht dabei einer selbst identifizierten Kenngröße, die angibt, zu welchem Grad die betrachtete Vorgabe mindestens erfüllt werden muss. Die Kenngröße wird als (prozentualer) Anteil vom Idealzustand angegeben. Keine Vorgabe, unabhängig von der betrachteten Gewichtung und Alternative, darf dieses Mindestmaß – beziehungsweise diese Satisfizierungs-Bedingung – unterschreiten.

2. Vorauswahl

- Im nächsten Schritt erfolgt die **Vorauswahl**. Der tatsächliche Erfüllungsgrad einer jeden Vorgabe wird geschätzt. Hierfür muss für jede Alternative bestimmt werden, inwiefern sie die Erfüllung der Vorgabe gewährleistet. Die Schätzung wird als (prozentualer) Anteil vom Idealzustand angegeben. Wird für eine Alternative das Mindestmaß einer oder mehrerer Vorgaben unterschritten, so ist die Alternative obsolet und wird nicht weiter betrachtet.

3. Auswahl

- Verbleibt mehr als eine Alternative zur Auswahl, so ist im Schritt der **Entscheidung** die Alternative mit dem größten Nutzen zu identifizieren. Der Nutzen einer Alternative errechnet sich aus dem Summenprodukt des Erfüllungsgrades mit der jeweiligen Gewichtung einer jeden Vorgabe. Falls zwei oder mehr Alternativen den gleichen Nutzen versprechen, wird die Alternative bevorzugt, die die wichtigste (und demnach am stärksten gewichtete) Vorgabe besser erfüllt.

¹¹⁷Die Nutzwertanalyse ist eine Methode, die durch Quantifizierung von Entscheidungskriterien bei der Entscheidungsfindung unterstützt. Den Entscheidungskriterien wird für jede Alternative ein eigener Wert (Einzelwert) zugeordnet. In der Regel wird die Alternative gewählt, die die höchste Summe an Einzelwerten aufweist.

¹¹⁸Die Satisfizierung ist eine Methode zur Entscheidungsfindung, bei der für Entscheidungskriterien ein Mindestmaß an Erfüllungsgrad definiert wird, welches nicht unterschritten werden darf. Sollte keine der zur Verfügung stehenden Alternativen diesen im Vorfeld definierten Anspruchsniveaus genügen, so ist eine Senkung des oder der Mindestmaße möglich.

Die Analyse löst dabei keinen Zielkonflikt auf, sondern zeigt im Ergebnis, welche Alternative unter den gewählten Rahmenbedingungen am sinnvollsten ist und somit den am größten errechneten Nutzen liefert. Durch den Zwischenschritt der Satisfizierung wird für alle relevanten Vorgaben ein zu erfüllendes Anspruchsniveau definiert. Eine Alternative muss das Anspruchsniveau einer jeden Vorgabe erfüllen, ansonsten ist die Alternative obsolet und kommt bei der Umsetzung der Vorgabe nicht infrage. Hiermit wird sichergestellt, dass auch Vorgaben mit geringem Gewicht, die trotzdem für den Entscheidungsprozess relevant sind, berücksichtigt bleiben.

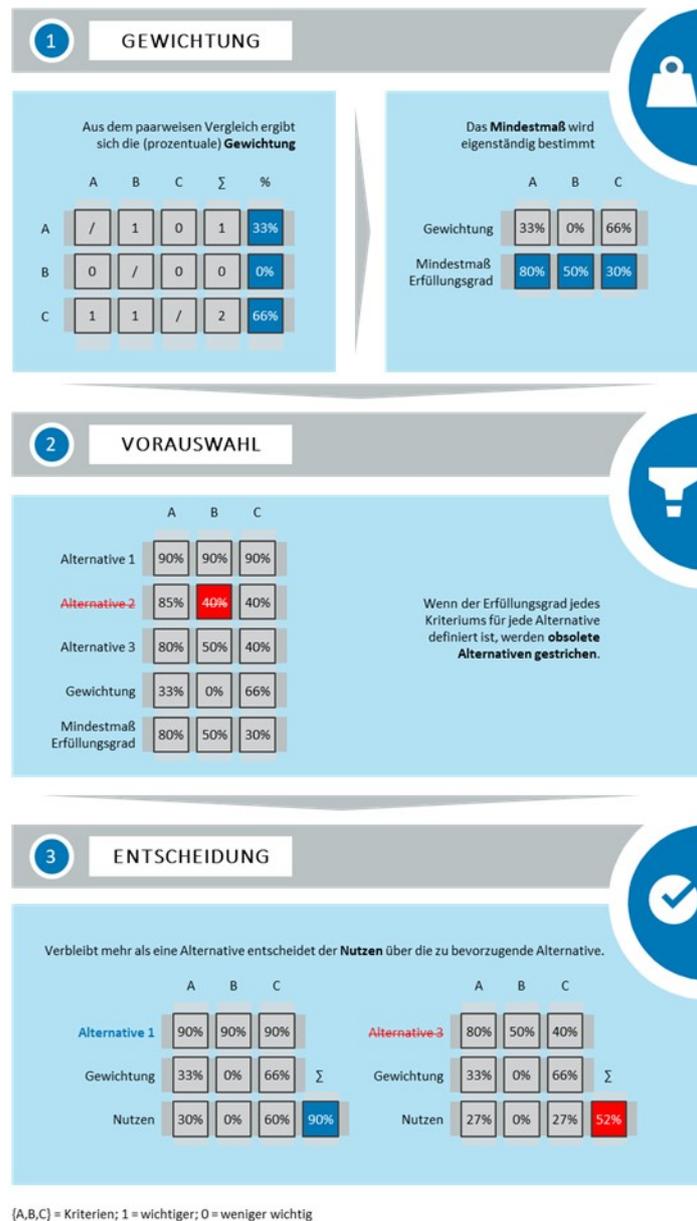


Abbildung 4: Beispielhafte Darstellung der Nutzwertanalyse mit Satisfizierung

3.5 Glossar

Architekturrichtlinie

Eine Architekturrichtlinie stellt die Gesamtheit aller Architekturvorgaben dar, die innerhalb des Geltungsbereichs verbindlich eingehalten werden müssen.

Architekturvorgabe

Eine Architekturvorgabe definiert die spezifische Ausprägung eines Aspektes, der entsprechend des Verbindlichkeitsgrades verbindlich eingehalten wird.

Auslands-IT

Die Auslandsinformations- und -kommunikationstechnik umfasst die Informations- und Kommunikationstechnik des Geschäftsbereichs des Auswärtigen Amtes im In- und Ausland sowie die Informationstechnik der unmittelbaren Bundesverwaltung im Ausland. Die IT Ausstattung der Bundeswehr-Dienststellen im Ausland verantwortet die Bundeswehr in eigener Zuständigkeit.

Basisdienst

Ein Basisdienst ist ein grundlegender IT-Dienst, der die Bereitstellung von Fach- und Querschnittsdiensten unterstützt und auf Infrastrukturdiensten aufbaut.

Basis-IT

Die Basis-IT baut auf der IT-Infrastruktur auf und umfasst IT-Lösungen, die zum Betrieb von Basisdiensten benötigt werden.

Betriebshoheit

Die Betriebshoheit beschreibt alle Befugnisse, die für die dauerhafte Sicherstellung der vollumfänglichen Kontrolle und Steuerung von IT-Lösungen notwendig sind.

Betriebsumgebung

Eine Betriebsumgebung beschreibt die Umgebung, auf der die IT-Lösungen betrieben werden, die den Geschäfts- und Dienstzwecken dienen.

Cloud Computing

Cloud Computing ermöglicht über ein Netz den Zugriff auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste), die mit einem geringen Managementaufwand sowie geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können.¹¹⁹, ¹²⁰ Cloud Computing bildet die Alternative zur traditionellen On-Premises Nutzung

¹¹⁹Bundesamt für Sicherheit in der Informationstechnik. Cloud Computing Grundlagen. 21. Januar 2021 unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen_node.html; zuletzt abgerufen am 9. März 2022.

¹²⁰IT-Planungsrat. Beschluss 2021/46 Deutsche Verwaltungscloud-Strategie: Rahmenwerk der Zielarchitektur. 13. August 2021 unter https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-46_Deutsche_Verwaltungscloud-Strategie_AL1.pdf; zuletzt abgerufen am 10. März 2022.

von Rechnerressourcen, die lokal erfolgt und mit einem hohen Managementaufwand sowie intensiver Serviceprovider-Interaktion verbunden ist.

Continuous Delivery

Continuous Delivery ist ein Software-Engineering-Ansatz, bei dem Software in kurzen Zyklen produziert und die Freigabe zuverlässig und automatisiert erfolgt. Ziel ist es, Software schneller und häufiger zu erstellen, zu testen und freizugeben.

Daten

Mit Daten werden einzelne Werte innerhalb eines Datensatzes bezeichnet. In der Literatur wird unter Daten jedwede Art von Elementen verstanden, die durch einen Computer interpretierbar sind. Der Datenbegriff umfasst im Allgemeinen elektronisch und nicht-elektronisch gespeicherte Zustände und Wiedergaben von Sachverhalten. Die Interpretation von Daten schafft Informationen, deren gemeinsame Verknüpfung Wissen generiert. In der Architekturrichtlinie wird der Ausdruck Daten primär im digitalen Sinne verstanden.

Daten-Governance

Daten-Governance beschreibt die übergreifenden Rahmenbedingungen und organisatorischen Strukturen, die für das Datenmanagement und eine datenorientierte Verwaltung notwendig sind.¹²¹

Datenmanagement

Das Datenmanagement umfasst alle Methoden und Maßnahmen, die sich mit der Erhebung, Verarbeitung, Qualität und Analyse von Daten beschäftigen.

DevOps

Der Begriff DevOps ist von den englischen Worten Software Development und IT-Operations abgeleitet und beschreibt die enge Kollaboration der Entwicklung (Development) und des Betriebs (Operations). Dies soll zu einer effizienteren Software-Entwicklung führen, indem durch Automatisierung und Kooperation Qualität kontinuierlich analysiert wird und Produkte nutzungsorientierter und schneller (weiter-)entwickelt werden können.

Dienst (IT-Dienst)

Ein Dienst ist eine logische und konzeptionelle Einheit, die einen definierten Umfang an funktionalen Anforderungen erfüllt. Das Konzept des Dienstes wird zur Strukturierung des IT-Angebots genutzt. Es ist weiterhin dazu geeignet, Nachfrage auf einer groben Beschreibungsebene zu identifizieren, die bereits einen Abgleich mit dem IT-Angebot erlaubt.

Digitalisierung

¹²¹Die Bundesregierung. Datenstrategie der Bundesregierung. 27. Januar 2011 unter <https://www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf>; zuletzt abgerufen am 11. April 2022.

Digitalisierung ist die Transformation und Umsetzung von Information und Kommunikation durch technische Systeme. Damit werden im Rahmen von Digitalisierung die geschäftlichen und methodischen Fähigkeiten durch Informations- und Kommunikationstechnik gestaltet.

Digitale Kollaboration

Digitale Kollaboration bezeichnet die kooperative Zusammenarbeit von Personen, die durch IT-Anwendungen realisiert wird. Die Verteilung von Informationen zur Kollaboration stellt ein zentrales Element dar.¹²²

Digitale Souveränität

Digitale Souveränität bezeichnet die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.¹²³

Einsatz-IT

Die Einsatz-IT umfasst IT-Lösungen, die für die aufgabengemäße Durchführung von Tätigkeiten der Einsatzorganisation der Bereiche Äußere sowie Innere Sicherheit zur Anwendung kommen. Hierbei umfasst sie stationäre, transportable oder mobile IT-Lösungen. Dabei muss, je nach Auftrag und Einsatz, auch ein autonomer und krisenresilienter Betrieb möglich sein. Die Bereiche Äußere sowie Innere Sicherheit sind Nutzer und auch Betreiber von Einsatz-IT.

E-Government

E-Government oder elektronische Behördendienste bezeichnen alle Prozesse der öffentlichen Willens- und Entscheidungsbildung in Politik, Staat und Verwaltung unter Nutzung von Informations- und Kommunikationstechnologien.¹²⁴

Fachdienst

Ein Fachdienst ist ein IT-Dienst, der die Funktionalität für einen spezifischen Anwendungsbereich einer Behörde beschreibt. In Kontrast zu Querschnittsdiensten haben Fachdienste einen fachspezifischen Charakter.

Fach-IT

Die Fach-IT baut auf der IT-Infrastruktur und den Basisdiensten auf und umfasst IT-Lösungen, die zum Betrieb von Fachdiensten benötigt werden. Die Fach-IT beschreibt einen fachlogischen, eigenständigen und auf eine Behörde zugeschnittenen Anwendungsbereich.

¹²²ITWissen. Kollaboration. September 2019 unter <https://www.itwissen.info/Kollaboration-collaboration.html>; zuletzt abgerufen am 21. März 2021.

¹²³Kompetenzzentrum Öffentliche IT. Digitale Souveränität. November 2017, Seite 3 unter <https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t>; zuletzt abgerufen am 5. April 2022.

¹²⁴IT-Planungsrat; Föderale IT-Kooperation Jahresbericht 2020/2021. 26. März 2021 unter https://www.it-planungsrat.de/fileadmin/it-planungsrat/der-it-planungsrat/Jahresbericht_IT-PLR_FITKO.pdf; zuletzt abgerufen am 11. März 2022.

Forschungs-IT

Die Forschungs-IT umfasst IT-Lösungen, die für die Erkenntnis- und Wissensgewinnung im Rahmen von Forschungsprojekten notwendige Tätigkeiten und Prozesse unterstützen.

Gemeinsame IT (des Bundes)

Informationstechnik welche gemeinsam genutzt wird.

Informationstechnik (IT)

Die Informationstechnik umfasst die technische (elektronische) Verarbeitung von Daten und Informationen. Dazu bedient sich Informationstechnik Software, Hardware und entsprechender Infrastrukturen sowie dazugehöriger Methoden und Arbeitsweisen für das Management und die Anwendung der technischen Informationssysteme.

Informations- und Kommunikationstechnik (IKT)

Die Informations- und Kommunikationstechnik umfasst die Informationstechnik und Kommunikationstechnik.

Informationstechnik des Bundes (IT des Bundes)

Die Informationstechnik des Bundes umfasst alle informationstechnischen Bestandteile, die die Handlungsfähigkeit der Bundesverwaltung gewährleisten. Sie wird durch den Beauftragten der Bundesregierung für Informationstechnik und den IT-Rat politisch und strategisch gesteuert und soll den Service der Verwaltung verbessern, Innovationen fördern und die Effizienz der Verwaltung sicherstellen.¹²⁵ Die Informationstechnik des Bundes umfasst üblicherweise auch Kommunikationstechnik und die Digitalisierungsaktivitäten. Die Informationstechnik des Bundes schließt die Verwaltungs-IT ein.

Infrastrukturdienst

Ein Infrastrukturdienst ist ein IT-Dienst, der Basis-, Fach- und Querschnittsdienste unterstützt, indem er technische Basisfunktionalitäten bereitstellt und der Entkopplung von der zugrunde liegenden technischen Infrastruktur der IT-Dienstleister dient.¹²⁶

Interoperabilität

Interoperabilität bezeichnet die Fähigkeit von unterschiedlichen IT-Lösungen nahtlos zu interagieren.¹²⁷

IT-Anwendung

¹²⁵Bundesministerium des Innern und für Heimat. Informationstechnik des Bundes. Unter <https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-des-bundes/it-des-bundes-node.html>; zuletzt abgerufen am 7. April 2022.

¹²⁶CIO Bund. Strategie Dienstekonsolidierung 2018-2025. Beschluss Nr. 2018/3. 24. Januar 2018 unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/it-rat/beschluesse/beschluss_2018_03.pdf?__blob=publicationFile&v=1; zuletzt abgerufen am 10. Januar 2024.

¹²⁷Der Beauftragte der Bundesregierung für Informationstechnik. Architekturen, Standards und Methoden unter https://www.cio.bund.de/Webs/CIO/DE/digitaler-wandel/Achitekturen_und_Standards/architekturen_und_standards-node.html; zuletzt abgerufen am 10. Januar 2024.

Eine IT-Anwendung beschreibt eine IT-Lösung, die mit Anwendern kommuniziert und interagiert.

IT-Architektur

Eine IT-Architektur beschreibt, auf welcher technischen Basis IT-Lösungen zur Umsetzung der Anforderungen bereitgestellt werden.

IT-Dienstleistung

Eine IT-Dienstleistung beschreibt eine auf dem Einsatz der Informationstechnologie basierende Dienstleistung, die von einem Anbieter für Kunden zur Verfügung gestellt wird. Eine IT-Dienstleistung besteht aus Personen, Prozessen und Technologie, deren Umfang mit dem Kunden definiert wird.¹²⁸

IT-Infrastruktur

Eine IT-Infrastruktur umfasst alle materiellen Bestandteile, die für die Entwicklung und den Einsatz von IT-Lösungen erforderlich sind.

IT-Komponente

Eine IT-Komponente ist in der Softwarearchitektur eine eigenständig einsetzbare Einheit mit Schnittstellen nach außen, die Entwurf und Implementierung kapselt und mit anderen IT Komponenten verbunden werden kann. Sie ist sowohl fachlich als auch technisch unabhängig und besitzt eine gewisse Größe (im Sinne eines wirtschaftlichen Wertes).

IT-Landschaft

Im Rahmen dieser Architekturrichtlinie umfasst eine IT-Landschaft sämtliche IT-Lösungen, die im Kontext der verwaltungsspezifischen Aufgabenbewältigung genutzt werden.

IT-Lösung

Eine IT-Lösung stellt die informationstechnische Realisierung eines definierten Leistungsumfangs an IT-Unterstützung durch ein (technisches) System bestehend aus mehreren IT-Komponenten dar. Das IT-System wird synonym verwendet.

IT-Sourcing-Strategie

Eine IT-Sourcing-Strategie bezeichnet die strategische, detaillierte und auf die Aufgabenstellung zugeschnittene Planung von Rahmenbedingungen zur Beschaffung von externen IT-Lösungen und IT-Dienstleistungen.

IT-Umgebung

Die IT-Umgebung modelliert eine Arbeits- und Interaktionsumgebung, in der verschiedene IT Komponenten, IT-Lösungen und IT-Dienstleistungen für die zweckmäßigen Bedarfe funktional adressiert werden.

¹²⁸IT-Service Management Forum. Arbeitskreis Publikation ITIL Version 3 Translation Project. 17. März 2016 unter https://web.archive.org/web/20160430161729/https://www.itsmf.de/fileadmin/dokumente/AK_Publikationen/20070831_ITIL_V3_Glossary_Germany.pdf; zuletzt abgerufen am 11. März 2022.

IT-Wirtschaft

Die IT-Wirtschaft umfasst Unternehmen, die Dienstleistungen, die auf dem Einsatz von Informationstechnologie basieren, anbieten.

IT-Verfahren

IT-Verfahren beschreiben spezifische IT-Anwendungen, die zur Bearbeitung regelmäßig anfallender strukturierter Prozesse zur Verfügung gestellt werden.

Kollaborative Funktionalität

Die kollaborative Funktionalität einer IT-Lösung ermöglicht die gemeinsame, ortsunabhängige und zeitgleiche Bearbeitung von Daten.

Kommunikationstechnik

Die Kommunikationstechnik umfasst die technische (elektronische) Verarbeitung von Kommunikation und Nachrichten. Dazu bedient sich Kommunikationstechnik Software, Hardware und entsprechender Infrastrukturen sowie dazugehöriger Methoden und Arbeitsweisen für das Management und die Anwendung der technischen Kommunikationssysteme.

Lose Kopplung

Die Lose Kopplung bezeichnet die Unabhängigkeit von Komponenten untereinander, wodurch Änderungen an einzelnen Komponenten einfacher durchgeführt werden können.¹²⁹

Markdown

Ist eine leicht lesbare und verständliche Auszeichnungssprache für Inhalt. Die Inhalte der Architekturrichtlinie werden in dieser Auszeichnungssprache gepflegt.

Modul

Ein Modul bezeichnet eine IT-Komponente, die bei einer Modularisierung entsteht und somit die Eigenschaft der Modularität beinhaltet.

Modularisierung

Modularisierung stellt ein Prinzip dar, in der während der Entwicklung IT-Komponenten in eigenständige Bausteine gegliedert werden, die unabhängig nutzbar sind.

Modularität

Die Modularität bezieht sich auf die flexible Austauschbarkeit von IT-Komponenten und Anwendun-

¹²⁹Diese Definition orientiert sich an der AV-03

gen¹³⁰, sofern diese als Baustein eigenständig und unabhängig nutzbar sind.¹³¹

Multi-Vendor-Strategie

Eine Multi-Vendor-Strategie beschreibt die strategische Beschaffung von IT-Dienstleistungen und IT Lösungen von mehr als einem Anbieter, um Abhängigkeiten zu vermeiden.

Nachrichtendienst-IT

Die Nachrichtendienst-IT umfasst IT-Lösungen, die für nachrichtendienstliche Zwecke im Kontext der Aufklärung, Informationsgewinnung und Überwachung sowie der dafür notwendigen Unterstützung bereitgestellt werden.

Open Source

Open Source bezeichnet frei zur Verfügung gestellte Inhalte mit dem Ziel der kollaborativen Weiterentwicklung sowie allgemeinen Nutzung. Open Source adressiert in diesem Zusammenhang die Transparenz, Meritokratie und Gemeinschaft als einzuhaltende Werte, die während der Entwicklung erfüllt werden sollten.¹³²

Quality of Service

Quality of Service bezeichnet die Erfüllung der Anforderungen an einen Kommunikationsdienst aus Nutzendensicht, um eine anwendungsgerechte Qualität sicherzustellen.

Querschnittsdienst

Ein Querschnittsdienst ist ein IT-Dienst, der in unterschiedlichen Verwaltungseinheiten stets in ähnlicher oder gleicher Form anfallende Aufgaben unterstützt und auch von Fachdiensten genutzt wird. Beispielhaft seien hier Personalverwaltung, Beschaffung und Haushaltswesen genannt.

Querschnitts-IT

Die Querschnitts-IT baut auf der IT-Infrastruktur und den Basisdiensten auf und umfasst IT Lösungen, die zum Betrieb von Querschnittsdiensten benötigt werden.

Referenzarchitektur

Eine Referenzarchitektur baut auf der Architekturrichtlinie auf und definiert Leitlinien und Vorgaben für eine standardisierte Umsetzung eines spezifischen Anwendungsfeldes.¹³³

¹³⁰Der Beauftragte der Bundesregierung für Informationstechnik. Zentrum für Digitale Souveränität in der Öffentlichen Verwaltung (ZenDis). 2023 unter <https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/zentrum-fuer-digitale-souveraenitaet/zentrum-fuer-digitale-souveraenitaet-node.html>; zuletzt abgerufen am 10. Januar 2024.

¹³¹IT-Planungsrat. Beschluss 2021/37 Föderale Architekturrichtlinien Version 0.99. 9. September 2021 unter https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-37_IT-Architekturboard_AL1_Architekturrichtlinien.pdf; zuletzt abgerufen am 11. März 2022.

¹³²Der Beauftragte der Bundesregierung für Informationstechnik. Glossar. https://www.cio.bund.de/Webs/CIO/DE/service/lexikon/functions/bmi-lexikon.html?cms_lv2=18094664; zuletzt abgerufen am 10. Januar 2024.

¹³³CIO Bund. Referenzarchitektur Portale und Integration. 2019 unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitaler-wandel/architekturen-standard/portale-und-integration.pdf?__blob=publicationFile&v=1; zuletzt abgerufen am 10. Januar 2024.

Self-Assessment

Das Self-Assessment ist ein Fragebogen zur Eigenbewertung eines Sachverhaltes.

„Separation of Concerns“-Prinzip

Das “Separation of Concerns“-Prinzip besagt, dass IT-Komponenten eine klar definierte Aufgabe erfüllen sollen. IT-Komponenten bilden somit modulare Teillösungen für IT Lösungen. Sie können leicht weiterentwickelt, eingesetzt und ausgetauscht werden. Die Einhaltung des „Separation of Concerns“-Prinzips erleichtert somit die Weiterentwicklung von IT-Lösungen und ermöglicht die Wiederverwendung von IT-Komponenten.

Sichere Systemkonfiguration

Eine sichere Systemkonfiguration beschreibt die Anpassung der Standardkonfiguration von IT-Lösungen mit dem Ziel, die zu betreffenden Dienste und IT-Lösungen vor Angriffen zu schützen.¹³⁴

Verbindlichkeitsgrad (RFC 2119)

Zur Beschreibung des Verbindlichkeitsgrads einer Architekturvorgabe wird sich zur Verringerung des Interpretationsspielraums und somit besseren Verständlichkeit an den Request For Comments (RFC) 2119¹³⁵ orientiert. Im Rahmen der Architekturrichtlinie werden folgende vier Abstufungen verwendet:

- „MUSS“ kennzeichnet die Vorgabe als verbindlich fest
- „SOLL“ kennzeichnet die Vorgabe als verbindlich fest, sofern keine wesentlichen Gründe für eine Abweichung bestehen
- „KANN“ kennzeichnet die Vorgabe als eine unverbindliche Option
- „DARF NICHT“ kennzeichnet die Vorgabe absolutes Verbot.

Der Verbindlichkeitsgrad einer Architekturvorgabe ist eng am Prozess der Entscheidungsfindung gekoppelt.

Verwaltungs-IT

Die Verwaltungs-IT, bzw. die IT der öffentlichen Verwaltung, umfasst alle informationstechnischen Bestandteile, über die die öffentliche Verwaltung zur Unterstützung ihres Auftrages verfügt. Dies schließt alles von der verwendeten Hardware bis hin zu internen Fach- und Querschnittsdiensten sowie IT-Dienstleistungen für Externe ein.

VS-IT

VS-IT umfasst die IT, die für die Handhabung von Verschlusssachen (VS) eingesetzt wird.

¹³⁴BSI. IT-Grundschutz-Kompendium. 2021 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6; zuletzt abgerufen am 14. März 2022.

¹³⁵Network Working Group. Datentracker. 1997 unter <https://datatracker.ietf.org/doc/html/rfc2119>; zuletzt abgerufen am 11. März 2022.

VSV-IT

VSV-IT umfasst die IT, die für die Handhabung von VS-VERTRAULICH oder höher eingestuften Verschlusssachen eingesetzt wird. Zur Sicherstellung der Geheimhaltung von VS-VERTRAULICH oder höher eingestuften Verschlusssachen beim Einsatz von IT ist ein Informationssicherheitskonzept mit Aussagen zu Sicherheitsfunktionen wie Zugangs- und Zugriffskontrollsysteme, sowie zur Abstrahlsicherheit der Hardware zu erstellen und umzusetzen.¹³⁶

¹³⁶BSI. Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz. 13. März 2023 unter https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_13032023_SII554001405.htm; zuletzt abgerufen am 10. Januar 2024.

3.6 Abkürzungsverzeichnis

Abkürzung	Bedeutung
ADatP	Allied Data Publication
ADMBw	Architekturdatenmodell der Bundeswehr
API	Application Programming Interface
AV	Allgemeine Vorgabe
AVV-EnEff	Allgemeine Verwaltungsvorschrift zur Beschaffung energieeffizienter Produkte und Dienstleistungen
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGG	Behindertengleichstellungsgesetz
BITV	Barrierefreie Informationstechnik Verordnung
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Innern und für Heimat
BP	Beschreibungspunkt
BPML	Business Process Modeling Language
BPMN	Business Process Model and Notation
BQI-Dienst	Basis-, Querschnitts- und Infrastrukturdienst
BSCW	Basic Support for Cooperative Work
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
BVA	Bundesverwaltungsamt
BVN	Bundesverwaltungsnetz
CIO	Chief Information Officer
CMMN	Case Management Model and Notation
CNP	Netze der Polizei / Corporate Network der Polizei
COBIT	Control Objectives for Information and Related Technologies
DBS	Datenbanksystem
DER	Detektion und Reaktion
DevOps	Software Development and IT Operations
DIN	Deutsches Institut für Normung
DK	Dienstekonsolidierung
DMN	Decision Model and Notation

Abkürzung	Bedeutung
DNS	Domain Name System
DOI	Deutschland Online Infrastruktur
DSGVO	Datenschutz-Grundverordnung
DVS	Deutsche Verwaltungscloud-Strategie
EDP	Europäisches Metadatenportal
EGovG	E-Government-Gesetz
EIF	European Interoperability Framework
EN	Europäische Norm
EPK	Ereignisgesteuerte Prozesskette
EU	Europäische Union v
EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von IT-Lösungen
FAIR	Findable, Accessible, Interoperable, and Re-usable
FIM	Föderales Informationsmanagement
FMN	Federated Mission Networking
FV	Funktionale Vorgabe
GDI-DE	Geodateninfrastruktur Deutschland
GV	Geschäftliche Vorgabe
IAM	Identity Access Management
ID	Identifikationsnummer
IEEE	Institute of Electrical and Electronical Engineers
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISi-LANA	Sichere Anbindung von lokalen Netzen an das Internet
ISMS	Informationssicherheitsmanagementsystem
IKT	Informations- und Kommunikationstechnologie
IMS	Integrated Management System
INSPIRE	Infrastructure for Spatial Information in the European Community
ISM	Informationssicherheitsmanagement
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
IT-BPB	IT-Bebauungsplan der Bundeswehr
IT-K	IT-Konsolidierung Bund
IT-PLR	IT-Planungsrat
IT-Rat	Rat der IT-Beauftragten der Ressorts

Abkürzung	Bedeutung
IVBB	Informationsverbund Berlin-Bonn
IVBV	Informationsverbund der Bundesverwaltung
IVÖV	Informationsverbund der öffentlichen Verwaltung
ITZBund	Informationstechnikzentrum Bund
KG	Koordinierungsgruppe
KI	Künstliche Intelligenz
KNB	Kompetenzstelle nachhaltige Beschaffung
KoITB	Konferenz der IT-Beauftragten der Ressorts
LAN	Local Area Network
MPLS WAN	Multiprotocol Label Switching Wide Area Network
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NdB	Netze des Bundes
NdB-VN	Netze des Bundes-Verbindungsnetz
NISP	Interoperability Standards and Profiles
NMO	Nachfragemanagementorganisation
OMG	Object Management Group
OPS	Betrieb
OZG	Onlinezugangsgesetz
PKI	Public key infrastructure
R	Regel
RFC	Request for Comments
RZ	Rechenzentrum
SAF	Scaled Agile Framework
SAGA	Standards und Architekturen für E-Government-Anwendungen
SCS	Sovereign Cloud Stack
SiSyPHuS Win10	Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10
STANAG	Standardization Agreement
S-O-S	Strategische Ausrichtung, Organisatorisches Umfeld, Systematisches Vorgehen
SÜG	Sicherheitsüberprüfungsgesetz
SÜG-AVV	Sicherheitsüberprüfungsgesetz- Ausführungsvorschrift

Abkürzung	Bedeutung
TESTA-ng	Trans-European Services for Telematics between Administrations - New Generation
TLS	Transport Layer Security
TV	Technische Vorgabe
TOGAF	The Open Group Architecture Framework
UML	Unified Modelling Language
UN	United Nations
UP	Umsetzungsplan
V	Vorgabe
VgV	Vergaberechtliche Vorschrift
VS	Verschlusssache
VN	Bund-Länder-Verbindungsnetz nach IT-NetzG
VSA	Verschlusssachenanweisung
VS-NfD	Verschlusssache-Nur für den Dienstgebrauch
WKD	Wertschöpfungskettendiagramm
XML	Extensible Markup Language
XÖV	XML in der öffentlichen Verwaltung
XPDL	XML Process Definition Language

3.7 Abbildungsverzeichnis

Abbildung	Titel der Abbildung
Abbildung 1	Vorgaben der Architekturrichtlinie (Planungsstand: 09/2024)
Abbildung 2	Matrixdarstellung der Releasetypen
Abbildung 3	Richtlinie Lebenszyklus COBIT 5
Abbildung 4	Beispielhafte Darstellung der Nutzwertanalyse mit Satisfizierung

Impressum**Herausgeber**

Der Beauftragte der Bundesregierung für Informationstechnik
Bundesministerium des Innern und für Heimat, Alt-Moabit 140, 10557 Berlin
Internet: www.bmi.bund.de ; www.cio.bund.de

Stand

Februar 2025

Bildnachweis

Titelbild: vs148 / shutterstock.com

Diese Publikation wird von der Bundesregierung im Rahmen ihrer Öffentlichkeitsarbeit herausgegeben. Die Publikation wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Bundestags-, Landtags- und Kommunalwahlen sowie für Wahlen zum Europäischen Parlament.

