Der Beauftragte der Bundesregierung für Informationstechnik

IT-ARCHITEKTUR BUND

KOMPLEXITÄT MANAGEN, VERBINDUNGEN SCHAFFEN

Architekturrichtlinie für die IT des Bundes

Version v6.1

Vorwort

Erläuterung und Motivation der Änderungen der IT-Architekturrichtlinie Bund

Die Architekturrichtlinie für die IT des Bundes (IT-Architekturrichtlinie Bund) muss entsprechend der kontinuierlichen Entwicklung von Technologien, Regeln und Standards weiterentwickelt werden. Mit der vorliegenden Version wurden die systematischen Grundlagen geschaffen, um Aktualität und langfristigen Kontinuität in der Nutzbarkeit der IT-Architekturrichtlinie Bund zu gewährleisten. Bestehende Inhalte wurden neu gegliedert und die Struktur für eine zukünftige, effiziente Weiterentwicklung vorbereitet. Inhalte werden grundsätzlich in weiterverarbeitbarer Form gepflegt.

Hierfür wurden verschiedene internationale Modelle und Standards analysiert. Dazu gehören insbesondere das European Interoperability Framework (EIF), die European Library of Architecture Principles (ELAP), The Open Group Architecture Framework (TOGAF) und das OECD Digital Government Policy Framework und Toolkit. Erkenntnisse aus den Indikatoren, Prinzipien und Regeln wurden in die Erarbeitung der IT-Architekturrichtlinie Bund einbezogen. Weiterhin wurde aus der Analyse abgeleitet, dass vier zentrale Regelungsbereiche in der IT-Architekturrichtlinie Bund zu definieren sind:

- Allgemeine Vorgaben (AV): grundlegende und rahmengebende Prinzipien
- 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. Dies soll den Anwendern und Anwenderinnen der IT-Architekturrichtlinie Bund eine deutliche Abgrenzung zwischen verschiedenen Vorgaben erleichtern, auch wenn diese ähnliche Themen regeln. Zum Beispiel kann die Verwendung von Schnittstellen im funktionalen Regelungsbereich und die Ausgestaltung von Schnittstellen im technischen Regelungsbereich beschrieben werden.

In jedem der Regelungsbereiche sollen maximal 10 Vorgaben beschrieben werden. Insgesamt soll die IT-Architekturrichtlinie Bund den Umfang von 40 Vorgaben nicht überschreiten. Ähnliche Themen werden zur Erhöhung der Übersichtlichkeit und Verständlichkeit konsolidiert, einem stetigen Zuwachs an Vorgaben wird vorgebeugt und eine strategische Fokussierung und Priorisierung auf wesentliche Regelungen gefördert. In der aktuell vorliegenden Version wird die grundlegende Anpassung der Struktur vorgenommen. Inhaltliche Konsolidierung und Überarbeitung erfolgt in den folgenden Versionen.

Die Fortschreibung der IT-Architekturrichtlinie Bund wird mit der Version 6.1 in eine agile und modulare Form überführt. Dabei wird die IT-Architekturrichtlinie Bund von einer jährlich vollständig dokumentenbasierten Version auf eine unterjährig weiterverarbeitbare Version umgestellt. Auf Basis der weiterverarbeitbaren Form werden automatisiert verschiedene Ausgabeformate bereitgestellt. Künftig können einzelne Vorgaben unabhängig vom Gesamtdokument geändert werden.

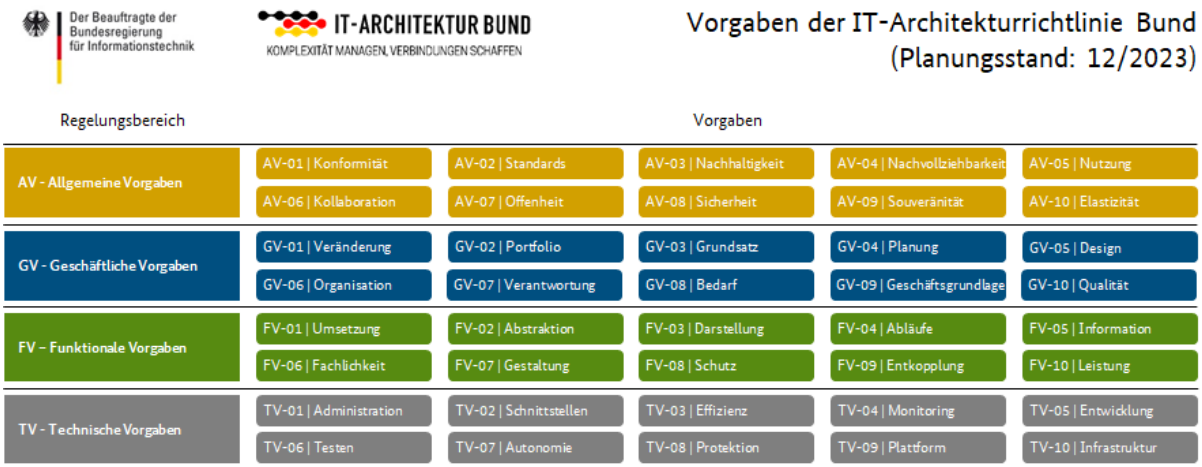

Abbildung 1: Vorgabe der IT-Architekturrichtlinie Bund (Planungsstand: 12/2023)

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.

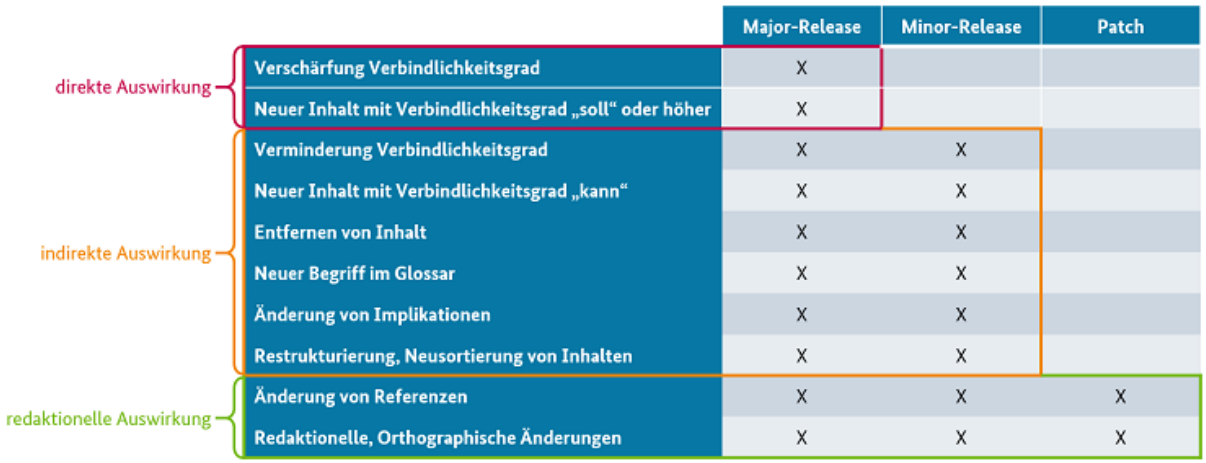

Abbildung 2: Matrixdarstellung der Releasetypen

Struktur, Inhalt und Umfang der IT-Architekturrichtlinie Bund sind strategisch übergreifend ausgerichtet. Den Anwendern und Anwenderinnen der IT-Architekturrichtlinie Bund wird empfohlen, für ihre Anwendungsfälle die Regeln in den Vorgaben zu detaillieren. Dazu sollten eigene Spezifikationen abgeleitet oder bestehende Spezifikationen angewendet werden. Die Spezifikationen leiten anhand der Vorgaben aus der IT-Architekturrichtlinie Bund detaillierte Regeln ab. Deren Geltungsbereich, konkreter Inhalt und Grad der Konkretisierung wird vom jeweiligen Autor in der Spezifikation festgeschrieben.

Releasenotes v6.1

In Releasenotes werden sehr kurz und in einer einheitlichen Form die Änderungen seit der letzten Version des Produktes zusammengefasst.

Zusammenfassung

Diese Releasenotes beschreiben die Veränderungen von Version 6.0 zu Version 6.1 (minor release).
Die Version 6.1 beinhaltet die Neugruppierung der Vorgaben in die vier Regelungsbereiche allgemeine, geschäftliche, funktionale und technische Vorgaben.
Die Änderung stärkt die Orientierung an den Architekturebenen gemäß The Open Group Architecture Framework (TOGAF) und Rahmenarchitektur der IT-Steuerung Bund.

- Die grundlegenden Prinzipien, Vision, Anforderungen und Bedingungen werden in den allgemeinen Vorgaben gebündelt.
- Die Motivation, Organisation und Fähigkeiten werden in den geschäftlichen Vorgaben gebündelt.
- Die funktionalen, datenorientierten und logischen Perspektiven der Gestaltung von Informationssystemen werden in den funktionalen Vorgaben gebündelt.
- Die Technologie, Technik, physische Umsetzung, Implementierung und Migration werden in den technischen Vorgaben gebündelt.

Für die Nutzenden wird die Anzahl der Vorgaben durch thematische Zusammenfassung übersichtlicher aufbereitet.

Korrigiert

Architekturrichtlinie ab Version v6.1	Architekturrichtlinie 2022 (v6.0)
AV - Allgemeine Vorgaben	ÜBAV - Übergreifende Architekturvorgaben
GV - Geschäftliche Vorgaben	GSAV - Geschäftliche Architekturvorgaben
FV - Funktionale Vorgaben	DAAV - Architekturvorgaben für Dienste IDAV - Architekturvorgaben für Information und Daten
TV - Technische Vorgaben	TIAV - Technische Architekturvorgaben, Technik und Infrastruktur TNAV - Technische Architekturvorgaben, Weitverkehrsnetze

Architekturrichtlinie ab Version v6.1	Architekturrichtlinie 2022 (v6.0)
	ISAV - Architekturvorgaben zur Informationssicherheit

Insbesondere Architekturvorgaben zur Informationssicherheit sind ob der thematisch übergreifenden Anwendung in mehreren Regelungsbereichen verortet. Übergreifende Themen stellen ihren strategischen Kern in den allgemeinen Vorgaben (AV) dar und detaillieren in den weiteren Regelungsbereichen.

Übertragen

v6.1	v6.0	Titel
AV-01	ÜBAV-01	Architekturvorgaben und
	ÜBAV-02	Recht
AV-02	ÜBAV-04	Standards, Methoden,
	ÜBAV-07	Referenzarchitekturen und
	ÜBAV-10	Interoperabilität
AV-03	ÜBAV-12	Nachhaltigkeit
AV-04	ÜBAV-18	Daten
AV-05	ÜBAV-08	Benutzerfreundlichkeit und Barrierefreiheit
AV-06	ÜBAV-16	Digitale Kollaboration
AV-07	ÜBAV-17	Open Source
AV-08	ÜBAV-05	Informationssicherheit, Datenschutz, Geheimschutz und
	ÜBAV-06	Systemgrundkonfiguration
AV-09	ÜBAV-03	Souveränität und
	ÜBAV-09	Unabhängigkeit
AV-10	ÜBAV-11	Kopplung,
	ÜBAV-13	Komplexität,
	ÜBAV-14	Modularität, Wiederverwendbarkeit und
	ÜBAV-15	Cloud Computing

v6.1	v6.0	Titel
GV-04	GSAV-01	Projektmanagement

v6.1	v6.0	Titel
GV-05	GSAV-02	Prozessmanagement
	GSAV-03	
	GSAV-04	
GV-08	IDAV-05	Daten-Governance

v6.1	v6.0	Titel
FV-01	DAAV-01	Allgemeine Nutzungs- und Leistungsverpflichtung
FV-02	DAAV-03	Dienst- und Schnittstellenbeschreibungen
FV-04	DAAV-04	Anwendungen für den Bundesclient
FV-05	IDAV-01	Information,
	IDAV-02	Zeichen und
	IDAV-03	Daten
	IDAV-04	
	IDAV-06	
	IDAV-07	
FV-08	DAAV-06	Identitätsinformation,
	DAAV-07	Zugriffssteuerung,
	ISAV-01	Sicherheitskonzeption,
	ISAV-02	Schutzbedarf, Quality of Service,
	ISAV-03	Security by Design,
	ISAV-05	Separierung und Mandantentrennung
FV-09	DAAV-02	Entkopplung
	DAAV-05	

v6.1	v6.0	Titel
TV-01	TIAV-05	Entwicklung,
	TIAV-06	Programmiersprachen und
	TIAV-07	Qualitätsmanagement
TV-02	DAAV-08	Schnittstellen
	ISAV-07	

v6.1	v6.0	Titel
TV-05	TIAV-03	Datenbanksysteme
TV-08	ISAV-04	Kryptografie,
	ISAV-06	sicherheitsrelevante Ereignisse und
	ISAV-09	Schadprogrammabwehr
TV-09	TNAV-01	Kommunikationsverbindungen und
	TNAV-02	Netzwerkprotokoll
TV-10	TIAV-01	Betrieb
	TIAV-02	
	TIAV-04	
	ISAV-08	

Aktualisiert

- Revisionssichere IDs wurden um eine Releasenummer erhöht
- Revisionssichere IDs beginnen statt mit AV mit V
- Fehlerhafte Referenzen

Glossar

Abkürzung	Langbezeichnung
ÜBAV	übergreifende Architekturvorgaben
GSAV	geschäftliche Architekturvorgaben
DAAV	Architekturvorgaben für Dienste
IDAV	Architekturvorgaben für Informationen und Daten
TIAV	technische Architekturvorgaben, Technik und Infrastruktur
TNAV	technische Architekturvorgaben, Weitverkehrsnetze
ISAV	Architekturvorgaben zur Informationssicherheit
AV	allgemeine Vorgaben
GV	geschäftliche Vorgaben
FV	funktionale Vorgaben
TV	technische Vorgaben

Abkürzung	Langbezeichnung
V	Vorgabe

Kurzbezeichnung	Langbezeichnung
Korrigiert	Inhalt wurde orthografisch und grammatikalisch angepasst
Übertragen	Inhalt wurde zwischen Vorgaben verschoben
Aktualisiert	Inhalt wurden überarbeitet
Gelöscht	Inhalt wurden entfernt
Hinzugefügt	Inhalt wurden aufgenommen

Inhaltsverzeichnis

Kurzdarstellung

Die Organisation des Beauftragten der Bundesregierung für Informationstechnik hat die vorliegende „Architekturrichtlinie für die IT des Bundes" erarbeitet. Das Dokument wird kontinuierlich unter Einbindung der Stakeholder, insbesondere den Ressorts und Behörden sowie den IT-Dienstleistern der öffentlichen Verwaltung des Bundes, fortgeschrieben und beschlossen.

Mit Hilfe der Vorgaben der Architekturrichtlinie können Architekturentscheidungen systematisch, nachvollziehbar und transparent getroffen werden. Neben der Unterstützung der IT-Konsolidierung des Bundes wird durch dieses Dokument auch die Umsetzung weiterer Strategien, Initiativen und Beschlüsse auf Bundes- und Landesebene sowie auf EU-Ebene unterstützt. Die „Architekturrichtlinie für die IT des Bundes" fördert die zielgerichtete Weiterentwicklung der Informationstechnik und trägt somit zur Erreichung der strategischen und politischen Ziele für die IT der Bundesverwaltung bei.

Die Ausgangsebene des Dokuments bilden u. a. die in der „IT-Strategie der Bundesverwaltung" benannten architekturrelevanten Ziele sowie die Vorgaben und Parameter aktueller Projekte und Initiativen des Bundes im Kontext der IT-Architektur. Diese schaffen mit dem Metamodell der „Rahmenarchitektur IT-Steuerung Bund"[1] den grundlegenden Rahmen für die Architekturvorgaben.

Im Anhang „Technische Spezifikationen zur Architekturrichtlinie" werden im Sinne einer operativen, technischen Umsetzung die Vorgaben konkretisiert. Mit einem definierten Weiterentwicklungsprozess und den aufgestellten Grundsätzen zur Nutzung der Architekturrichtlinie sind wesentliche Aspekte des Architekturmanagements berücksichtigt. Damit werden für die Zukunft eine hohe Qualität und Aktualität der Vorgaben sowie ein regelmäßiger Abgleich mit aktuellen Projekten und geltenden Beschlüssen gewährleistet.

[1] CIO Bund. Abschlussbericht Rahmenarchitektur IT-Steuerung Bund. Beschluss Nr. 81/2012. 15. März 2012 unter http://www.cio.bund.de/Web/DE/Politische-Aufgaben/IT-Rat/Beschluesse/Tabelleninhalte/beschluss_81_2012.html zuletzt abgerufen am 24. April 2019.

1 Einführung

In diesem Kapitel wird der Kontext, die Zielsetzung, der Geltungsbereich, die Zielgruppe, die Einordnung und Abgrenzung von Vorhaben, der Aufbau der Architekturrichtlinie für die IT des Bundes und der Ausblick für die kommenden Fortschreibungen vorgestellt.

1.1 Kontext

Das am 5. Dezember 2007 vom Bundeskabinett beschlossene Konzept „IT-Steuerung Bund" [2] hat dem Rat der IT-Beauftragten der Ressorts (IT-Rat) u. a. die Aufgabe übertragen, gemeinsame Standards und Architekturen für die IT der Bundesverwaltung festzulegen. Hierzu zählt auch der Aufbau eines aktiven Architekturmanagements für die IT der Bundesverwaltung.

Mit dem Aufbau eines solchen Architekturmanagements schafft die Bundesverwaltung die Voraussetzungen für einen nachhaltigen, effektiven, souveränen und wirtschaftlichen Einsatz ihrer IT.[3] Ein solches Architekturmanagement ist für Verwaltungen und Unternehmen ein wesentlicher Schlüssel zur Steigerung der Leistungsfähigkeit ihrer IT. Es gewährt den Blick aus einer übergreifenden Perspektive und ermöglicht eine zielgerichtete Unterstützung verschiedener Interessengruppen zu einem einheitlichen Vorgehen im Management ihrer IT.

Im Jahr 2009 wurde das Grundlagenpapier „Rahmenarchitektur IT-Steuerung Bund"[4] vom IT-Rat verabschiedet. Es legt die grundlegenden Prinzipien, Ansätze und Begrifflichkeiten fest, anhand derer das Architekturmanagement ausgestaltet werden soll.

Mit dem Projekt „IT-Konsolidierung Bund", welches durch das Bundeskabinett mit dem Grobkonzept zur IT-Konsolidierung Bund vom 20. Mai 2015[5] beschlossen wurde, soll die IT der unmittelbaren Bundesverwaltung zukunftsfähig gestaltet und eine moderne, sichere sowie flexible IT-Architektur gewährleistet werden. Der Maßgabebeschluss des Haushaltsausschusses des Deutschen Bundestages (ADrs. 18(8)2134 Abs. II Ziffer 4) vom 17. Juni 2015 fordert die Bundesregierung auf,

„(...) *sicherzustellen, dass bei der laufenden technischen Weiterentwicklung der IT-Infrastruktur in der Bundesverwaltung und der Neuvergabe von Aufträgen keine Entscheidungen getroffen werden, die einer geplanten späteren Konsolidierung im Wege stehen. Die Gesamtprojektleitung soll dazu, so bald wie möglich, entsprechende Architekturrichtlinien erarbeiten. Für alle Bereiche, die von der Konsolidierung be-*

[2] CIO Bund. IT-Steuerung Bund. 2007 unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/cio-bund/steuerung-it-bund/konzept-it-steuerung-bund.pdf?__blob=publicationFile&v=1 zuletzt abgerufen am 09. Januar 2024.

[3] CIO Bund. IT-Architektur Bund. In Anlehnung an https://www.cio.bund.de/Webs/CIO/DE/digitaler-wandel/Achitekturen_und_Standards/IT_Architektur_Bund/IT_Architektur_Bund-node.html zuletzt abgerufen am 09. Januar 2024.

[4] Rat der IT-Beauftragten. Rahmenarchitektur IT-Steuerung Bund. Beschlossen am 26. März 2009.

[5] CIO Bund. Grobkonzept zur IT-Konsolidierung Bund. 20. Mai 2015 unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/it-konsolidierung/grobkonzept-zur-it-konsolidierung-bund.pdf?__blob=publicationFile&v=1 zuletzt abgerufen am 09. Januar 2024.

troffen sein werden, sind diese Richtlinien verbindlich. Die Ressorts sind bei der Erarbeitung der Richtlinien zu konsultieren. Über Ausnahmen entscheidet der IT-Rat."

Seit dem 6. November 2019 teilen sich das BMI und das BMF die Zuständigkeit für die IT-Konsolidierung Bund. Während die Betriebskonsolidierung und Dienstleisterertüchtigung im Verantwortungsbereich des BMF liegt, verantwortet das BMI u.a. die Dienstekonsolidierung und die hier vorliegende Architekturrichtlinie. Mit dem Beschluss des Eckpunktepapiers „Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung" des IT-Rats vom 24.03.2020 und des IT-Planungsrats vom 04.05.2020[6] haben Bund, Länder und Kommunen sich zum Ziel gesetzt, die Digitale Souveränität der Öffentlichen Verwaltung gemeinsam und kontinuierlich zu stärken. Die Verwendung von offenen Standards und Schnittstellen ist zur Erreichung dieses Ziels von herausragender Bedeutung. Zu diesem übergeordneten Ziel für die IT des Bundes kann mit der konsequenten Umsetzung der Architekturrichtlinie für die IT des Bundes ein wesentlicher Beitrag geleistet werden.

1.2 Zielsetzung

Ziel des vorliegenden Dokumentes ist, alle von der IT-Konsolidierung Bund betroffenen Projekte, Programme und Organisationen inklusive der dafür notwendigen Infrastruktur durch strategische sowie technische Architekturvorgaben aktiv bei Entscheidungsprozessen zu unterstützen und somit die zielgerichtete Weiterentwicklung der IT des Bundes zu fördern. Perspektivisch sollen gemeinsame Architekturvorgaben zusätzlich die Zusammenarbeit im föderalen Bereich, auf Bundesebene sowie auf EU-Ebene stärken.

Die Föderale Architekturrichtlinie[7] orientiert sich an dem vorliegenden Dokument und ist für eine Vielzahl föderaler Szenarien einsetzbar.

Mit Hilfe der Vorgaben soll es ermöglicht werden Architekturentscheidungen systematisch, nachvollziehbar und transparent zu treffen sowie laufende und geplante IT-Projekte nach den strategischen Anforderungen und politischen Aufgaben der Bundesverwaltung auszurichten. Durch die Verbindlichkeit der Vorgaben wird die Zielerreichung des Projektes „IT-Konsolidierung Bund" (vgl. 1.5 Einordnung und Abgrenzung Vorhaben) weiter gefördert. Gemeinsam genutzte IT, insbesondere die durch IT-Vorhaben wie beispielsweise IT Konsolidierung Bund hervorgebrachten Dienste und dafür etablierter und verwendeter IT-Infrastruktur, werden als „Gemeinsame IT des Bundes" definiert.

Die Architekturrichtlinie soll von den betroffenen Beschaffungsstellen, Dienststellen und Dienstleistern eingehalten werden. Die Verantwortung zur Umsetzung und Prüfung der Einhaltung tragen diese

[6] IT-Planungsrat und IT-Rat. Stärkung der Digitalen Souveränität der öffentlichen Verwaltung. Eckpunkte. März 2020 unter https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-19_Entscheidungsniederschrift_Umlaufverfahren_Eckpunktepapier.pdf zuletzt abgerufen am 06. April 2022.

[7] IT-Planungsrat. Föderale Architekturrichtlinien unter https://www.fitko.de/fileadmin/fitko/foederale-koordination/gremienarbeit/Foederales_IT-Architekturboard/Foederale_IT-Architekturrichtlinien_V1.0.pdf zuletzt abgerufen am 28. März 2022.

Stellen eigenständig. Darüber hinaus dienen die Beschreibungen der Vorgaben als Grundlage für das zukünftige Architekturcontrolling.

Der Anhang „Technische Spezifikationen zur Architekturrichtlinie“ konkretisiert im Sinne einer operativen, technischen Umsetzung die im Hauptdokument aufgeführten Architekturvorgaben. Der Anhang wurde im Rahmen der Fortschreibung der Architekturrichtlinie 2019 erstmals erstellt und löst den ehemaligen Standard SAGA 5 vollständig ab. Dafür wurden die für die IT-Konsolidierung der Bundesverwaltung relevanten technischen Spezifikationen aus SAGA 5 vollständig in diesen Anhang integriert und, sofern sinnvoll, aktualisiert.

1.3 Geltungsbereich

Die Architekturrichtlinie für die IT des Bundes ist über den Maßgabebeschluss des Haushaltsausschusses des Deutschen Bundestages (ADrs. 18(8)2134 Abs. II Ziffer 4) vom 17. Juni 2015 hinaus für alle Projekte, Programme und Organisationen der unmittelbaren und mittelbaren IT des Bundes inklusive der Verwaltungsdigitalisierung vom Beauftragten der Bundesregierung für die Informationstechnik zur Anwendung vorgegeben. Das Voranschreiten der Digitalisierung im Bund erfordert diese Erweiterung des Geltungsbereichs.

Für bereits konsolidierte Dienste fungiert die noch zu etablierende Nachfragemanagementorganisation (NMO), im Geltungsbereich des BMI und entsprechend ihres Organisationskonzeptes, als Verstetigung der Dienstekonsolidierung. Sie sorgt unter Anwendung des vorliegenden Dokuments für die Harmonisierung der Facharchitekturen von BQI-Diensten sowie für die bedarfsgerechte Fortentwicklung der IT des Bundes.

Für die IT des Bundes, insbesondere für sich vor und in Konsolidierung befindliche IT-Infrastruktur betrifft die „Architekturrichtlinie für die IT des Bundes“ alle IT-Maßnahmen zur laufenden technischen Weiterentwicklung sowie zur Neuvergabe von Aufträgen zur IT-Infrastruktur. Die Vorgaben dieser Architekturrichtlinie, ebenso wie besondere fachliche Anforderungen und politische Rahmenbedingungen, sind gemäß Grobkonzept IT-Konsolidierung Bund vor der Umsetzung entsprechender Maßnahmen zu beachten.[8]

Gemäß dem Grobkonzept des Projektes „IT-Konsolidierung Bund“ ist grundsätzlich der gesamte IT-Betrieb der unmittelbaren Bundesverwaltung (Betriebs-, Test- und Entwicklungsumgebungen) von der Konsolidierung betroffen. Der Umsetzbarkeit zentraler Vorgaben können durch die Aufgabenerledigung in den Behörden, durch rechtliche und politische Rahmenbedingungen sowie durch vergaberechtliche Anforderungen Grenzen gesetzt sein. Das ist insbesondere dann der Fall, wenn durch die Zusammenarbeit mit Stellen außerhalb der Bundesverwaltung, z. B. Bund-Länder-Ebene sowie

[8] Der Geschäftsbereich des BMVg nutzt das “NATO Architecture Framework (NAF)” und entwickelt dazu das entsprechende Datenmodell (Architekturdatenmodell der Bundeswehr, ADMBw) weiter. Auf Basis dieses Rahmenwerks entsteht der IT-Bebauungsplan der Bundeswehr (IT-BPB).

auf EU- oder internationaler Ebene, andere Zielsysteme bedient werden müssen. Da die fachliche Aufgabenerfüllung in den Behörden von der Konsolidierung nicht beeinträchtigt werden darf und die derzeitige Qualität der IT-Unterstützung mindestens erhalten bleiben muss, sind Ausnahmen in definierten Fällen möglich (z. B. Einsatz-IT, spezielle IT im Bereich der Forschung).

Generell ausgenommen sind die Auslands-IT, die IT der Nachrichtendienste und die IT für den Umgang mit eingestuften Informationen der Geheimhaltungsgrade „VS-VERTRAULICH“ oder höher.

IT-Umgebungen und Verfahren, die sich nicht für eine Konsolidierung eignen, können anhand des „Kriterienkatalog für Ausnahmefälle“ des Dokuments „Planungsgrundlagen der Betriebskonsolidierung“ ermittelt werden. Hierbei ist zu beachten, dass einmal getroffene Ausnahmen in Zukunft konsolidierungspflichtig werden können (z. B. aufgrund geänderter technischer Rahmenbedingungen).[9] Die Einhaltung der Architekturrichtlinie wird daher auch bei diesen Entscheidungen empfohlen, um das Risiko zukünftiger Inkompatibilitäten zu minimieren.

Die Festlegung des Konsolidierungsumfangs erfolgt anhand des „Kriterienkatalog für Ausnahmefälle“ im Rahmen behördenspezifischer IST-Analysen. Aufgrund der laufenden Weiterentwicklung der IT in den Behörden erfolgt eine zyklische Wiederholung der IST-Analyse in den Behörden mit einer regelmäßigen Überprüfung der Gültigkeit von Ausnahmeregelungen.

1.4 Zielgruppe

Die Architekturvorgaben richten sich an Entscheidungstragende, Projektleitende, Mitarbeitende des IT-Controllings, Einkaufende und Architekturschaffende mit Verantwortung für IT-Projekte, Architektur, Anwendungen und Infrastruktur in der unmittelbaren Bundesverwaltung. Dies umfasst somit sowohl Ressorts und Behörden als auch die entsprechenden IT-Dienstleister im Leistungsverbund und die zukünftige NMO. Außerdem richtet sich diese Richtlinie an das IT-Service Management und Entscheidungstragende des IT-Betriebs.

Die Vorgaben gelten sowohl für die beauftragenden Stellen als auch für ihre Auftragnehmenden. Ein geeigneter Wissenstransfer an alle relevanten Mitarbeitende ist durch die jeweiligen Behörden sicherzustellen.

1.5 Eingrenzung und Abgrenzung Vorhaben

Die IT des Bundes ist von zentraler und stetig steigender Bedeutung für die Handlungsfähigkeit von Staat und Verwaltung. Die strategische Ausrichtung der IT des Bundes unterliegt verschiedenen bereits verabschiedeten Beschlüssen des Bundes, berücksichtigt Vorgaben auf europäischer Ebene und umfasst bereits initiierte strategische Projekte sowie Initiativen. Die Architekturvorgaben unterstützen

[9] In Anlehnung an Dokument „IT-Konsolidierung Bund - Planungsgrundlagen der Betriebskonsolidierung einschließlich Rechenzentrums-Konsolidierungsplan 2017-2019 und Kriterienkatalog für Ausnahmefälle“, S. 97, Kapitel 1.3.

dabei die Erreichung der architekturrelevanten Ziele der folgenden bereits initiierten Projekte und Initiativen:

- **„IT-Konsolidierung Bund“**: Ein zentrales Vorhaben zur strategischen Ausrichtung der IT des Bundes stellt das auf Grundlage des Beschlusses des Bundeskabinetts vom 20. Mai 2015[10] zum 1. Juli 2015 eingerichtete, ressortübergreifende Projekt „IT-Konsolidierung Bund“ dar. Zielsetzung des Projektes ist die zukunftsfähige Aufstellung der IT der unmittelbaren Bundesverwaltung. Hieraus ergibt sich u. a. die Notwendigkeit die Informationssicherheit vor dem Hintergrund steigender Komplexität zu gewährleisten, die Hoheit und Kontrollfähigkeit über die eigene IT dauerhaft zu erhalten, auf innovative technologische Trends flexibel reagieren zu können, einen leistungsfähigen, wirtschaftlichen, stabilen, umweltverträglichen und zukunftsfähigen Betrieb sicherzustellen, ein attraktiver Arbeitgeber für IT-Fachpersonal zu bleiben bzw. noch stärker zu werden und Daten der Bundesverwaltung umfassend zu schützen und gegen Missbrauch zu sichern.

- **„IT-Betriebskonsolidierung Bund“**: Das Bundesministerium der Finanzen hat von der Bundesregierung den Auftrag erhalten (Kabinettbeschluss vom 6. November 2019), die IT-Betriebskonsolidierung in einem Projekt IT-Betriebskonsolidierung Bund (BKB) umzusetzen. Mit gleichem Beschluss hat die Bundesregierung das Projektziel auf eine Umsetzung der IT-Betriebskonsolidierung Bund in einem Servicemodell Infrastructure as a Service (IaaS) mit dem IT-Dienstleister ITZBund fokussiert. Dabei sollen grundsätzlich alle IT-Verfahren einer Behörde auf den vom ITZBund bereitgestellten, betriebenen und gepflegten Standard-Betriebsumgebungen in einem der Master-Rechenzentren des ITZBund bereitgestellt werden. Der genannte Kabinettsbeschluss zur Neuausrichtung der IT-Konsolidierung in zwei getrennten strategischen Projekten mit einem operativen IT-Dienstleister bedingte eine Überarbeitung der bestehenden Konzepte (im Jahr 2020).

- **„Dienstekonsolidierung“**: Die IT-Konsolidierung führt das 2010 als „Gemeinsame IT des Bundes“ initiierte Programm fort und zielt darauf ab, ressortübergreifend einheitliche, sichere und standardisierte, an der IT-Nachfrage ausgerichtete Basis-, Querschnitts- und Infrastrukturdienste für die IT der Bundesverwaltung bereitzustellen. Die Ziele, Handlungsfelder und Kernaktivitäten für die Gemeinsame IT des Bundes sind im Kontext der Dienstekonsolidierung in der „Strategie Dienstekonsolidierung 2018-2025“[11] definiert. Die Strategie Dienstekonsolidierung beinhaltet darüber hinaus die fortgeschriebenen funktionalen Beschreibungen als Dienstesteckbriefe und den Status der Dienstekonsolidierung. Das „IT-Rahmenkonzept des Bundes“ beschreibt alle

[10] CIO Bund. Grobkonzept zur IT-Konsolidierung Bund. 20. Mai 2015 unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/it-konsolidierung/grobkonzept-zur-it-konsolidierung-bund.pdf?__blob=publicationFile&v=1 zuletzt abgerufen am 09. Januar 2024.

[11] CIO Bund. Strategie Dienstekonsolidierung 2018-2025 Version 2021. Oktober 2021 unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/it-konsolidierung/dienstekonsolidierung/strategie_dienstekonsolidierung.pdf?__blob=publicationFile&v=2 zuletzt abgerufen am 09. Januar 2024.

laufenden IT-Maßnahmen und bestehenden IT-Vorhaben/ IT-Verfahren der „Gemeinsamen IT des Bundes“. Die technische Realisierung der IT-Lösungen erfolgt durch die IT-Dienstleister des Leistungsverbundes. Das „IT-Rahmenkonzept des Bundes“ wird jährlich fortgeschrieben und beschlossen.

- **„Onlinezugangsgesetz/ Digitalisierungsprogramm“**: Im Onlinezugangsgesetz (OZG)[12] verpflichten sich Bund und Länder, sämtliche Leistungen der deutschen Verwaltung bis zum Ende des Jahres 2022 erstmals vollständig digital in einem Portalverbund 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.

- **„Netze des Bundes“**[13]: Zukunftssichere Aufstellung der Bundesverwaltung im Bereich der IT-Netze und netznaher Basisdienste. Bereitstellung einer Kommunikationsplattform mit erhöhtem Sicherheitsniveau, auf welche bereits die drei vom BMI verantworteten Netze IVBB, IVBV/BVN, DOI vollständig migriert wurden („Netze des Bundes (NdB) 1.0“). Gemäß „Verwaltungsvorschrift zum Schutz von Verschlusssachen (VSA)“[14] werden hierdurch die gestiegenen Anforderungen und Sicherheitsbedarfe bei der Vernetzung der Bundesbehörden für die Übermittlung von nicht eingestuften bis maximal „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (VS-NfD) eingestuften Daten erfüllt. Die notwendigen Parallelanschlüsse der Behörden an Fremdnetze sind dabei zu berücksichtigen. Nutzende, die die Anforderungen an NdB nicht einhalten können, sollen über das NdB- Extranet / Grundschutzzone Zugriff auf ggf. „separierte“ NdB-Dienste erhalten.[15] NdB soll mit Blick auf die vom IT-Rat am 25. Februar 2019 beschlossene „Netzstrategie der öffentlichen Verwaltung 2030“[16] (IVÖV) als die Integrationsplattform der gesamten öffentlichen Verwaltung fortentwickelt werden. Sondernetze“, wie z. B. die Netze der Polizeien (CNP), sind gesondert zu betrachten. In diesem Dokument werden unter „NdB“ sowohl das „NdB 1.0“ (s. o.) sowie das zukünftige NdB-Extranet/ Grundschutz-Zone verstanden.

- **„Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung“**: Mit dem Beschluss des Eckpunktepapiers zur „Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung“[17] des

[12] BMJ. OZG. Unter https://www.gesetze-im-internet.de/ozg/ zuletzt abgerufen am 13. April 2022.

[13] BDBOS. Die Netze des Bundes. 2019 unter https://www.bdbos.bund.de/DE/NdB/ndb_node.html zuletzt abgerufen am 06. April 2022.

[14] Verwaltungsvorschriften im Internet. Verschlusssachenanweisung – VSA. 10. August 2018 unter https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_13032023_SII554001405.htm zuletzt abgerufen am 11. Januar 2024.

[15] Der derzeitige Entwicklungsstand des Zonenkonzepts und der möglichen Übergänge zwischen den Zonen, erlaubt noch keine konkrete Beschreibung in der Architekturrichtlinie. Im Rahmen der Fortschreibung 2023 wird dies konkretisiert.

[16] CIO Bund. Netzstrategie 2030 für die öffentliche Verwaltung. November 2018 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 10. Januar 2024.

[17] IT-Planungsrat. Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung. Januar 2021 unter https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf zuletzt abgerufen am 06. April 2022.

IT-Rats vom 24. März 2020 und des IT-Planungsrats vom 4. Mai 2020 haben sich Bund, Länder und Kommunen zum Ziel gesetzt, die Digitale Souveränität[18] der Öffentlichen Verwaltung in ihren Rollen als nutzende, bereitstellende und auftraggebende Stelle von Digitalen Technologien gemeinsam und kontinuierlich zu stärken. Um bestehende und potenzielle Abhängigkeiten zu reduzieren, haben sich Bund, Länder und Kommunen auf zentrale Handlungsfelder verständigt. Diese umfassen insbesondere die kontinuierliche Analyse von Abhängigkeiten und deren potenzielle Auswirkungen auf die Digitale Souveränität der Öffentlichen Verwaltung sowie die Erarbeitung, Erprobung und Umsetzung von Konzepten und alternativen Lösungen. Dazu zählt u. a. eine konsequente IT-Architekturentwicklung im Sinne der Digitalen Souveränität, z. B. durch die Förderung der Interoperabilität durch offene Standards und Schnittstellen.

- **„KG Green-IT“**: Der IT-Planungsrat hat auf seiner 30. Sitzung im Oktober 2019 die Etablierung der Koordinierungsgruppe (KG) Green-IT[19] beschlossen, um denen im Rahmen der kontinuierlichen Digitalisierung der Verwaltung aufkommenden ökologischen und sozialen Risiken zu begegnen. Die KG Green-IT verantwortet die Entwicklung einer Strategie zum Thema Green-IT sowie die (Weiter-)Entwicklung und anschließende Implementierung von Maßnahmen für Klimaschutz, Energiewende und Ressourcenschonung im Kontext der Digitalisierung in Bund und Ländern. Mit dem Eckpunktepapier der Green-IT[20] wurden dem IT-Planungsrat bereits erste konkrete Zielsetzungen und Handlungsfelder, die zur Umsetzung der benannten Ziele notwendig sind, vorgestellt.
- **„Europäischer Interoperabilitätsrahmen“**: Die EU hat zur Stärkung der grenzübergreifenden Zusammenarbeit den Europäischen Interoperabilitätsrahmen (EIF) beschlossen. Der EIF gibt Empfehlungen gemäß denen europäische digitale Verwaltungsleistungen realisiert werden sollen. Ziel ist es, die Fragmentierung der Dienstleistungen und Daten der öffentlichen Verwaltung in der EU zu reduzieren und einen digitalen Binnenmarkt zu fördern. Um die Interoperabilität deutscher Verwaltungen mit europäischen Diensten zu gewährleisten, kann es sinnvoll sein, hinsichtlich bestimmter Aspekte die Kompatibilität der Architekturrichtlinie mit dem EIF herzustellen. Einige Interoperabilitätsprinzipien des EIFs sind daher in dieser Version der Architekturrichtlinie referenziert.

Vorhandene Projekte, Initiativen und Dokumente

Begleitend und ergänzend zu den bereits genannten Projekten existieren u. a. folgende Projekte, Initiativen und Dokumente auf Bundesebene, deren Umsetzung durch diese Architekturrichtlinie

[18] Gemäß der Studie zum Thema „Digitale Souveränität“ der Kompetenzstelle Öffentliche IT (ÖFIT) wird Digitale Souveränität definiert als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“.

[19] IT-Planungsrat. Entscheidung 2019/63 - Klima- und Ressourcenschutz durch Green-IT unter https://www.it-planungsrat.de/beschluss/beschluss-2019-63 zuletzt abgerufen 12. Dezember 2023

[20] Green-IT. Eckpunkte – Ziele, Themenfelder und Maßnahmen. 14. Dezember 2020 unter https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-11_Green_IT_AL1_Eckpunkte.pdf zuletzt abgerufen am 01. April 2022.

gefördert wird: - IT-Strategie der Bundesverwaltung 2017-2021 - Konzept IT-Steuerung Bund - Grobkonzept IT-Konsolidierung Bund - Neuorganisation IT-Konsolidierung Bund - Eckpunkte IT-Betriebskonsolidierung Bund - Strategie Dienstekonsolidierung - IT-Rahmenkonzept des Bundes - Nachfragemanagementorganisation (NMO) - Maßnahmenprogramm Nachhaltigkeit der Bundesregierung - Polizei 2020, das Strategieprojekt der deutschen Polizeien - Aktionsprogramm zum Klimaschutz 2020 - Umsetzungsplan Bund - Digitalisierungsprogramm des IT-Planungsrats - Programm zur nachhaltigen Nutzung und zum Schutz der natürlichen Ressourcen - Ziele und Rahmenbedingungen der Green-IT-Initiative des Bundes - Allgemeine Verwaltungsvorschrift zur Beschaffung energieeffizienter Produkte und Dienstleistungen (AVVEnEff) - Leitfaden zur konsequenten Einbeziehung der Belange von Menschen mit Behinderungen

Auf europäischer Ebene werden mit dem „digitalen Kompass 2030“[21] der Europäischen Kommission, Meilensteile für den digitalen Wandel der Europäischen Union (EU) bis 2030 festgelegt, Pfade zu deren Erreichung aufgezeigt und ein Governance-Rahmen errichtet. Neben dem Aufbau digitaler Kompetenz, dem digitalen Wandel in Unternehmen und der Errichtung einer sicheren und leistungsfähigen digitalen Infrastruktur ist die Digitalisierung öffentlicher Dienste ein Kernaspekt. Unter dem Motto „Government as a Service“ soll das Angebot digitaler öffentlicher Dienste ausgebaut und Interoperabilität über alle Regierungsebenen hinweg sichergestellt werden.

1.6 Aufbau des Dokumentes

Die Inhalte des vorliegenden Dokumentes sind wie folgt gegliedert:

- Kapitel 1 „Einführung” beschreibt Kontext und Anwendungsrahmen sowie Ausblick der Architekturrichtlinie für die IT des Bundes.
- In Kapitel 2 „Grundlagen“ werden prinzipielle Grundlagen für das Verständnis der Architekturvorgaben vermittelt, die übergeordneten, strategischen Ziele der IT des Bundes beschrieben und das Metamodell der „Rahmenarchitektur IT-Steuerung Bund“ sowie dessen Architekturgrundsätze erläutert.
- Kapitel 3 „Architekturvorgaben“ beinhaltet die ausgearbeiteten Architekturvorgaben, welche in die verschiedenen Teilgebiete des Metamodells der „Rahmenarchitektur IT-Steuerung Bund“ aufgeteilt wurden.
- In Kapitel 4 „Nutzung von Architekturvorgaben“ werden Mechanismen zur Nutzung der Architekturvorgaben, deren kontinuierliche Fortschreibung sowie wesentliche Zuständigkeiten festgelegt.
- In Kapitel 5 „Anhang“ werden das Glossar und die Verzeichnisse der Architekturrichtlinie für die IT des Bundes geführt.

[21] Europäische Kommission. Digitaler Kompass 2030. 09. März 2021 unter https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en zuletzt abgerufen am 05. April 2022.

1.7 Ausblick

Im Rahmen der Fortschreibung 2023 sollen die Themen Registermodernisierung, Ökosystem digitale Identitäten, Mobile Computing (Mobiles Arbeiten und Mobile Apps) sowie Künstliche Intelligenz (KI) in den Fokus gestellt werden. Dazu werden die Themen hinsichtlich ihrer Relevanz für die IT des Bundes analysiert und ggf. in bestehende Vorgaben integriert oder eine eigene Vorgabe erstellt. Darüber hinaus soll das Thema Nachhaltigkeit, durch die im Jahr 2022 zu entwickelnde Green-IT Strategie vom IT-Planungsrat geschärft werden. Ebenfalls soll die Darstellung von Cloud-Bereichen und Schutzzonen, die Transparenz zu Fertigungstiefen, Lieferketten und Social/ Corporate Governance sowie Deployment Environment und Supportmodelle beleuchtet werden.

Ferner sollen neben der Fortschreibung der Architekturrichtlinie 2023 ein Architektur- Controlling aufgesetzt, eine interaktive Bereitstellungsform entwickelt, die Sichtbarkeit der Architekturrichtlinie gestärkt und die Aufteilung der technischen Spezifikation in Abhängigkeit zum Hauptdokument erarbeitet werden. Die Abstimmungen zu Umfang der IT des Bundes, zum Geltungsbereich, zur Wirkung der Architekturvorgaben und zur Fortschreibungssystematik sollen unter Klärung der praxisnahen und wirtschaftlichen Beteiligungs- sowie Umsetzungsmöglichkeiten abgeschlossen werden.

2 Grundlagen

Das Architekturmanagement stellt ein wesentliches Instrument zur operativen Umsetzung strategischer Ziele dar. Im vorliegenden Kapitel werden daher zunächst die strategischen Aspekte mit Architekturbezug beschrieben und mit den Architekturvorgaben in Zusammenhang gebracht.

Zur Strukturierung und methodischen Integration der Architekturvorgaben in den Gesamtkontext wird nachfolgend das vom BMI entwickelte Metamodell der „Rahmenarchitektur IT-Steuerung Bund“ erläutert. Dieses bildet den inhaltlichen Rahmen für die in der Architekturrichtlinie beschriebenen Architekturvorgaben.

2.1 Strategische Aspekte mit Architekturbezug

Die strategische Ausrichtung der IT des Bundes stellt eine wesentliche Zielsetzung für die Erarbeitung der Architekturvorgaben dar, da die zukünftige Architektur diese Ausrichtung bestmöglich unterstützen soll.

Die strategischen Ziele der Bundesverwaltung werden in der „IT-Strategie der Bundesverwaltung“ fortgeschrieben. Sofern im Zuge der Fortschreibung der IT-Strategie der Bundesverwaltung Anpassungen hinsichtlich der Architekturvorgaben erforderlich sind, werden diese im Fortschreibungs- und Aktualisierungsprozess der Architekturrichtlinie berücksichtigt und eingearbeitet.

Dieses Kapitel führt die architekturrelevanten Ziele der IT-Strategie auf und leitet konkrete architekturrelevante Themenfelder für die Architekturrichtlinie ab.

Als oberstes Ziel ist die leistungsfähige und bedarfsgerechte Unterstützung der Fachaufgaben sowie der gesetzlichen, politischen und strategischen Vorhaben des Bundes, der Ressorts und derer Behörden zu sehen. Auch die Einhaltung der Vorgaben gemäß § 8 BSIG[22] sowie die Einhaltung von Daten- und Geheimschutzvorgaben fallen hierunter.

Mit Einhaltung der Architekturvorgaben werden durch die Projekte folgende strategische IT-Ziele[23] im Sinne des Architekturmanagements eingehalten:

1. **Effektivität und Qualität der IT des Bundes**
2. **Digitale Verwaltung**
3. **Zukunftsfähigkeit und Offenheit für Innovationen**
4. **Informationssicherheit und Datenschutz**
5. **Attraktivität als Arbeitgeber**

[22] BSI. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG). 14. August 2009 unter https://www.gesetze-im-internet.de/bsig_2009/__8.html zuletzt abgerufen am 23. Mai 2022.

[23] CIO Bund. IT-Strategie der Bundesverwaltung. Januar 2023 unter https://www.cio.bund.de/Webs/CIO/DE/digitaler-wandel/it-strategie/it-strategie-node.html zuletzt abgerufen am 10. Januar 2024.

6. **Wirtschaftlichkeit und Kosteneffizienz**
7. **Inklusion und Barrierefreiheit**
8. **Umweltverträglichkeit und Nachhaltigkeit**
9. **Kooperationen**
10. **Kontrollfähigkeit und Steuerbarkeit**

Effektivität und Qualität

Vor dem Hintergrund wachsender Komplexität und sich ändernder Rahmenbedingungen gilt es, die Effektivität und Qualität der IT als Unterstützungsprozess für die Erfüllung der Fachaufgaben der unmittelbaren Bundesbehörden weiter zu steigern. Hierfür sind die Wiederverwendbarkeit und Flexibilität der IT-Lösungen des Bundes zu erhöhen und ein leistungsfähiger sowie stabiler IT-Betrieb der IT-Landschaft sicherzustellen.

Aus dieser Zielsetzung leiten sich für die Architektur folgende Schwerpunkte ab: - Optimierte, bedarfsgerechte Unterstützung der Fachaufgaben und der politischen sowie strategischen Vorhaben des Bundes und der Ressorts - Erhöhen der Modularisierung und Flexibilisierung der IT-Landschaft - Anforderungsgerechte Standardisierung - Absicherung der Zuverlässigkeit und Vorsehen notwendiger Redundanzen

Digitale Verwaltung

Die voranschreitende Digitalisierung der verschiedenen Verwaltungsprozesse ist einer der Kernpunkte für die strategische Ausrichtung der Behörden. Digitalisierung beschleunigt Prozesse, unterstützt die Kommunikation und Kooperation der Behörden untereinander und verbessert den Zugang zu Verwaltungsdienstleistungen für Bürgerinnen und Bürger sowie für Unternehmen. Zudem unterstützt eine digitale Verwaltung die Kooperation des Bundes und der Länder sowie die Zusammenarbeit im internationalen Kontext.

Geleitet durch die Vorgaben des „E-Government-Gesetzes“[24] und dem damit verbundenen Ziel des Bürokratieabbaus, ergeben sich folgende Themenfelder für die Architektur: - Bereitstellung eines elektronischen Zugangs zur Verwaltung - Digitale Unterstützung von Verwaltungsprozessen, insbesondere unter Nutzung von Basisdiensten zur Dokumenten- und Vorgangsbearbeitung (Akte, Vorgänge, Kollaboration, Archivierung)

Zukunftsfähigkeit und Offenheit für Innovationen

Die Verwaltung der Zukunft wird u. a. durch Innovationen erreicht. Die IT ist dabei einer der zentralen Treiber von Innovationen. Sie ermöglicht die technische Umsetzung neuer Konzepte zur Einbindung der Bürgerinnen und Bürger und schafft Raum für neue Arbeitsweisen. Ein effektiver und bedarfsorientierter IT-Betrieb muss langfristig durch den Einsatz zeitgemäßer und umweltverträglicher

[24] BMI. E-Government-Gesetz. 1. August 2013 unter https://www.bmi.bund.de/DE/themen/moderne-verwaltung/e-government/e-government-gesetz/e-government-gesetz-node.html zuletzt abgerufen am 23. Mai 2022.

Technologien sichergestellt werden. Die Zukunftsfähigkeit der Bundesverwaltung soll durch folgende Maßnahmen gewährleistet werden: - Regelmäßige Evaluierung der IT-Systeme und Technologie-Upgrades - Strukturierte Prozesse zur Bewertung und schnellen Bereitstellung technischer Innovationen - Förderung von Innovationen durch die Zusammenarbeit mit externen Partnern

Die Förderung von Innovationen nimmt langfristig einen positiven Einfluss auf alle Ziele.

Informationssicherheit und Datenschutz

Durch die voranschreitende Vernetzung, steigende Komplexität der IT und den Ausbau der digitalen Infrastruktur kommen der Informationssicherheit, dem Datenschutz und dem Geheimschutz immer höhere Stellenwerte zu. Für zukünftige Architekturentscheidungen sind folgende Zielsetzungen von essenzieller Bedeutung: - Gewährleistung der Sicherheit der Daten vor unberechtigter Informationsgewinnung und -beschaffung und ungewolltem Verlust (Vertraulichkeit), unberechtigter Veränderung (Integrität) sowie vor Systemausfällen mit Einschränkungen der zugesicherten Nutzbarkeit von Informationen, IT-Diensten und -Funktionen (Verfügbarkeit und Authentizität) - Gewährleistung der Einhaltung der geltenden Vorgaben in der Bundesverwaltung zur Informationssicherheit, insbesondere des Umsetzungsplan Bund (UP Bund, des § 8 BSIG und IT-Grundschutz-Standards) - Gewährleistung der Einhaltung der einschlägigen Datenschutzgesetze (insbesondere der seit Mai 2018 unmittelbar geltenden EU-Datenschutzgrundverordnung sowie ergänzender Regelungen im BDSG) sowie weiterer datenschutzrechtlicher Regelungen beim Umgang mit personenbezogenen Daten (u. a. des grundrechtlich verbürgten Rechts auf informationelle Selbstbestimmung) - Gewährleistung der Einhaltung des Sicherheitsüberprüfungsgesetzes (SÜG) und der allgemeinen Verwaltungsvorschriften zur Ausführung des SÜG, insbesondere der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA) bei der Handhabung von Verschlusssachen - Erleichterung der Bereitstellung von an verschiedenen Schutzbedarfen ausgerichteten IT-Leistungen - Anforderungsgerechte Reduzierung der Komplexität der Anwendungslandschaft auf ein notwendiges Maß - Berücksichtigung von Robustheit und Resilienz in frühen Entwicklungsstadien von Architektur und Design

Attraktivität als Arbeitgeber

Der stetig wachsende Anteil IT-unterstützter Prozesse in der Verwaltung lässt den Bedarf an qualifiziertem IT-Fachpersonal weiter steigen. Dabei steht die Bundesverwaltung im direkten Wettbewerb mit der Privatwirtschaft und muss sich noch stärker als bisher als zeitgemäßer und attraktiver Arbeitgeber positionieren. Zielsetzung ist die dauerhafte Bindung von vorhandenem IT-Personal und die Gewinnung von neuem Personal (insbesondere von Auszubildenden, Studierenden und IT-Fachpersonal).

Dies soll u. a. durch ein technologisch attraktives Arbeitsumfeld (z. B. durch Einsatz vergleichbar nutzerfreundlicher Kommunikationswerkzeuge wie „im öffentlichen Raum“) und Verbesserung der Karriere- und Arbeitsmodelle (z. B. flexiblere Arbeitszeiten) sowie durch zielgerichtete Weiterbildungen erreicht werden. Eine erhöhte Attraktivität als Arbeitgeber wirkt sich positiv auf die Erreichung weiterer Ziele aus.

Wirtschaftlichkeit und Kosteneffizienz

Die Entwicklung und der Betrieb der IT des Bundes unterliegen dem Wirtschaftlichkeitsgebot. Bei der Erreichung der Ziele und Umsetzung von Maßnahmen sollen Ressourcen wirtschaftlich und effizient eingesetzt werden. Daraus leiten sich unter Beachtung technischer, wirtschaftlicher sowie informationssicherheitsrelevanter Aspekte die folgenden wesentlichen Themenfelder für die IT-Architektur ab: - Realisierung von Einsparpotenzialen durch Beschaffungsbündelung und Konsolidierung - Steigerung des Virtualisierungsgrades, effizienter Ressourceneinsatz durch Standardisierung, Wiederverwendung, Erhöhung der Auslastung und Automatisierung - Vollständige Lebenszyklusbetrachtung (bzgl. Wirtschaftlichkeit und Ressourceneffizienz)

Inklusion und Barrierefreiheit

Die fortschreitende technische Entwicklung birgt Chancen und Risiken für Menschen mit Behinderungen und für Menschen mit geringen IT-Kenntnissen. Chancen, weil mit der voranschreitenden Digitalisierung neue Techniken, Arbeitsfelder und Unterstützungsmittel entstehen. Risiken, weil bei der Entwicklung einer neuen Technik die Zugangsmöglichkeit für Menschen mit Behinderung oft übersehen wird und nicht alle Teilnehmenden die gleichen Nutzungsvoraussetzungen mitbringen. Die „Chancengleichheit im Netz“ ist ein Thema von großer politischer und gesellschaftlicher Bedeutung, denn die breite Anwendung neuer Kommunikationstechniken ist eine der zentralen Voraussetzungen für die Wettbewerbsfähigkeit eines Landes und dessen Beschäftigungsentwicklung.

Das Ziel umfasst den folgenden architektonischen Aspekt: Die digitalen Angebote des Bundes müssen gemäß § 12a des Behindertengleichstellungsgesetzes[25] barrierefrei erreichbar sowie für Bürgerinnen und Bürger und Mitarbeitende mit Beeinträchtigungen im selben Funktionsumfang nutzbar sein.

Umweltverträglichkeit und Nachhaltigkeit

Die IT-Systeme des Bundes sollen nach umweltverträglichen und nachhaltigen Grundsätzen entwickelt und betrieben werden. Dies umfasst ökonomische, ökologische und soziale Aspekte. Als Maßgabe soll trotz steigender Leistung z. B. der Energieverbrauch der IT-Systeme mindestens konstant gehalten und nach Möglichkeit durch begleitende Maßnahmen zum Einsatz energieschonender Technologien kontinuierlich gesenkt werden. Bereits bei der Beschaffung soll das Nachhaltigkeitsgebot berücksichtigt werden. Mit Blick auf die Architekturrichtlinie folgt daraus: - Der IT-Betrieb soll umweltverträglich und nachhaltig gestaltet werden. Hierbei sind jegliche Inanspruchnahmen von Ressourcen über den gesamten Lebenszyklus zu betrachten. - Die IT-Beschaffung soll, soweit wirtschaftlich und technisch möglich, konsequent umweltverträgliche und nachhaltige Aspekte entsprechend der IT-Beschaffungsstrategie für die zentralen IT-Beschaffungsstellen berücksichtigen.

Kooperationen

Der wachsende Digitalisierungsgrad in der Verwaltung bietet die Chance und ist zugleich erforderlich,

[25] BMJ. Gesetz zur Gleichstellung von Menschen mit Behinderungen (Behindertengleichstellungsgesetz – BGG). 01. Mai 2022 unter https://www.gesetze-im-internet.de/bgg/__12a.html zuletzt abgerufen am 23. Mai 2022.

um dem gesteigerten Bedarf an nationaler und internationaler Kooperation gerecht zu werden. Voraussetzung für einen effizienten Abgleich und Austausch von Daten zwischen Organen verschiedener Verwaltungsebenen wie beispielsweise der NATO, UN, EU, im Bund und den Ländern sind gemeinsame, standardisierte Schnittstellen. Zudem werden die Aktivitäten des „Federated Mission Networking“[26] (FMN) durch die Interoperabilität grenzübergreifender Kooperationen maßgeblich verbessert. Diese Architekturvorgaben müssen die Entwicklung und den Ausbau kompatibler, standardisierter und zukunftsfähiger Schnittstellen ermöglichen. Damit wird der kooperative und organisationsübergreifende Informationsaustausch, insbesondere in der Digitalen Verwaltung, gefördert. Zusätzlich müssen weitere Kooperationen mit der Wirtschaft und mit Zweckverbänden gestärkt werden.

Aus dieser Zielsetzung ergibt sich für die Architektur ein Schwerpunkt hinsichtlich der Einbettung von zukunftsweisenden Schnittstellen in neue und vorhandene Systeme. Dabei ist der Datenaustausch mit anderen Verwaltungsebenen sowie externen Empfangenden (beispielsweise mit Wirtschaft und Forschung) zu berücksichtigen. Etablierung quelloffener Standards und Schnittstellen ist dabei als zentraler Baustein für die Kooperation mit anderen Verwaltungseinheiten, aber auch mit Akteurinnen und Akteuren außerhalb der Verwaltung zu betrachten.

Kontrollfähigkeit und Steuerbarkeit

Die bedarfsgerechte und damit erfolgreiche Zusammenarbeit zwischen den IT-Dienstleistern und den Ressorts erfordert effektive Planungs- und Steuerungsmechanismen mit zentraler Koordination und Kontrolle. Dieses Ziel ist durch eine klare und eindeutige Zuweisung von Aufgaben, Kompetenzen und Zuständigkeiten innerhalb der weiterentwickelten IT-Organisationen umzusetzen.

Folgende Prämissen sind im Rahmen der zukünftige IT-Architektur zu berücksichtigen: - Die systematische Zusammenarbeit zwischen Fach- und IT-Seite (i. S. von Nachfrage und Angebot) soll durch die Techniken und Methoden der „Rahmenarchitektur IT-Steuerung Bund“ gefördert werden. Dies umfasst zum einen die Etablierung eines Anforderungs-, Architektur- und IT-Projekt(portfolio)- Managements, zum anderen die Umsetzung eines strategischen und operativen IT-Controllings. - Die ressortübergreifende IT-Steuerung soll durch effektiven und effizienten IT-Einsatz das IT-Dienstleistungsangebot für die Verwaltung verbessern. - Die Schaffung geeigneter Planungsinstrumente soll einen effektiven und effizienten IT-Einsatz gewährleisten, Innovationen fördern, administrative Handlungsfähigkeit bewahren und die Effizienz der Verwaltung steigern.

Dieser strategische Aspekt wird insbesondere in Kapitel 5 Nutzung von Architekturvorgaben aufgegriffen, wo auch dessen Umsetzung spezifiziert wird.

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

[26] NATO. Federated Mission Networking. Unter https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx zuletzt abgerufen am 06. April 2022.

ausgeschlossen.

Im Rahmen der kontinuierlichen Fortschreibung relevanter Konzepte und Beschlüsse im Kontext der vorliegenden Architekturrichtlinie sind diese Zielkonflikte gemeinsam durch Ressorts, IT-Dienstleister, Fachexperten und die Projektleitung des BMI zu bewerten und zur Synchronisation an der jeweils geeigneten Stelle zu adressieren. Des Weiteren sind diese Zielkonflikte in die Abhängigkeiten und/oder Implikationen der betroffenen Vorgaben aufzunehmen.

2.2 Metamodell der "Rahmenarchitektur IT-Steuerung Bund" Architekturgrundsätze

Die Struktur der in Kapitel 3 dargestellten Architekturvorgaben orientiert sich an dem Metamodell der „Rahmenarchitektur IT-Steuerung Bund"[27].

Dieses Metamodell stellt einen übergreifenden Begriffs- und Strukturrahmen für die Erstellung von Modellen zum Zweck der Planung und Steuerung der IT der Bundesverwaltung dar und soll damit die gemeinsame Basis einer effizienten ressortübergreifenden Zusammenarbeit schaffen. Es schließt auch Definitionen der auf dieser Ebene erforderlichen Objekte und Relationen ein. Die folgende Abbildung stellt eine vereinfachte Form des Metamodells dar, aus der die einzelnen Teilmodelle der Rahmenarchitektur ersichtlich werden. Diese vereinfachte Form wurde gewählt, um die architekturrelevanten Komponenten des Modells aufzuzeigen.

Die Abbildung verdeutlicht, dass aus den bereits in Kapitel 3.1 Strategische Aspekte mit Architekturbezug erläuterten strategischen Zielen übergreifende Architekturvorgaben abgeleitet wurden.

Betrachtet man nun unter Berücksichtigung der strategischen Ziele die einzelnen Teilbereiche des Metamodells, so lassen sich hieraus diverse spezifische Vorgaben für jeden Bereich ermitteln. Konkret wurden Architekturvorgaben für folgende Bereiche des Metamodells aufgestellt: - Allgemeine Vorgaben - Geschäftliche Vorgaben - Funktionale Vorgaben - Technische Vorgaben

Die folgende Auflistung zeigt, auf welche thematischen Ebenen und Themenfelder sich die Vorgaben innerhalb der einzelnen Modelle beziehen.

Allgemeine Ebene:

Architekturvorgaben zu

- Ressorts- oder behördenspezifischen Aufgaben mit denen die Bundesregierung ihren originären Zweck erfüllt und
- Querschnittsaufgaben, welche in ähnlicher oder gleicher Weise in multiplen Ressorts anfallen.

[27] CIO Bund. Abschlussbericht Rahmenarchitektur IT-Steuerung Bund. Beschluss Nr. 81/2012. 15. März 2012 unter http://www.cio.bund.de/Web/DE/Politische-Aufgaben/IT-Rat/Beschluesse/Tabelleninhalte/beschluss_81_2012.html zuletzt abgerufen am 24. April 2019.

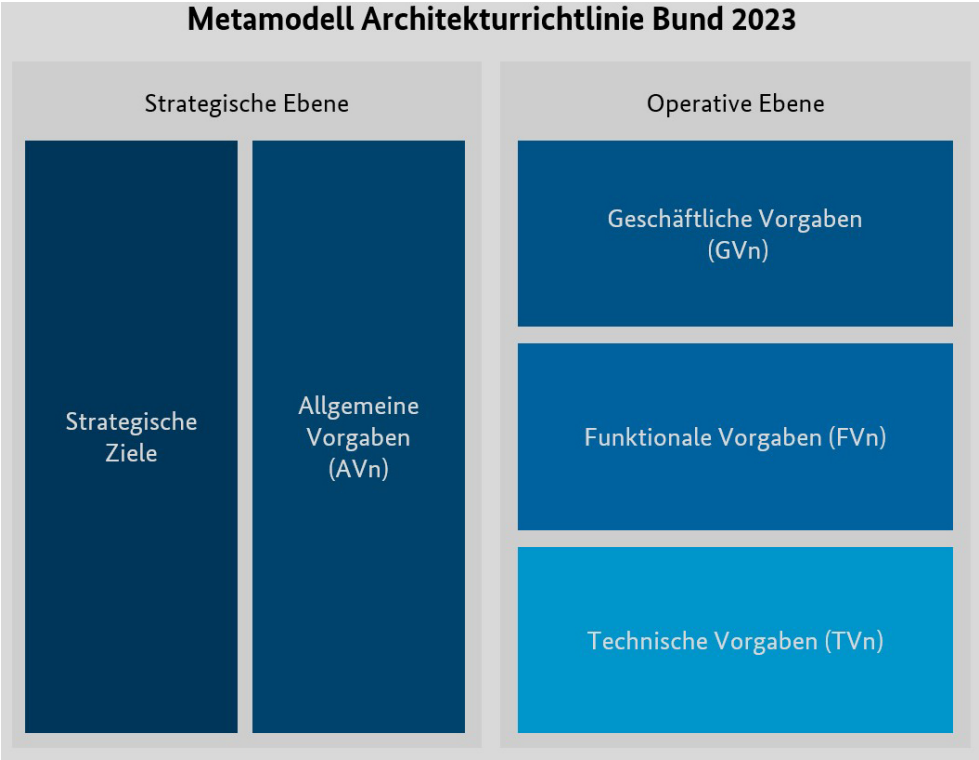

Abbildung 3: Metamodell der Architekturrichtlinie für die IT des Bundes

Geschäftliche Ebene:

Architekturvorgaben zu

- Ressorts- oder behördenspezifischen Aufgaben mit denen die Bundesregierung ihren originären Zweck erfüllt und
- Querschnittsaufgaben, welche in ähnlicher oder gleicher Weise in multiplen Ressorts anfallen.

Funktionale Ebene:

Architekturvorgaben zu

- Fachdiensten,
- Basisdiensten,
- Querschnittsdiensten und
- Infrastrukturdiensten.

Technische Ebene:

Architekturvorgaben zu

- IT-Lösungen,
- IT-Komponenten,
- Basis-Infrastruktur der Bundesverwaltung und
- Anzuwendenden Standards.

3 Architekturvorgaben

In diesem Kapitel wird die generelle Struktur und Semantik zur Beschreibung der Architekturvorgaben erläutert sowie konkrete Architekturvorgaben entlang des Metamodells beschrieben.

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® Framework[28] adaptierte, Formatvorlage genutzt.

*— **Beginn der Formatvorlage** —*

ID: Revisionssichere Identifikationsnummer
Titel der Architekturvorgabe
Kernvorgabe inklusive des Verbindlichkeitsgrades

Beschreibung - Konkretisiert und vervollständigt die Kernvorgabe durch einzelne eindeutige und widerspruchsfreie Architekturartefakte, Prüfelemente und Referenzen.

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

Abhängigkeiten - Beschreibt 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).

*— **Ende der Formatvorlage** —*

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

Der **Titel** inklusive dem Verbindlichkeitsgrad erleichtert das Identifizieren der relevanten Architekturvorgaben.

Die **ID** als revisionssichere Identifikationsnummer identifiziert Änderungen an einzelnen Architekturvorgaben. Die Nummerierung erfolgt fortlaufend, wobei das Präfix AV 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

[28] The 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.

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.

Die **Kernvorgabe** wird zur schnellen Erfassbarkeit und Verständlichkeit als einzelner grammatikalisch gleich aufgebauter Satz formuliert. Der Titel der Architekturvorgabe ergibt sich aus einer gekürzten Version der Kernvorgabe.

Die **Beschreibung** wird zur Bewertung der Anwendbarkeit der Architekturrichtlinie einheitlich strukturiert. Aus der Beschreibung entlang der Strukturierung können Prüfkriterien und Referenzen abgeleitet 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.[29] Die Kennzahlen orientieren sich an den in der Beschreibung definierten Architekturartefakten, Prüfelementen und Referenzen. Die konkrete Ausgestaltung des Kennzahlensystems sowie deren Weiterentwicklung werden in den Konzepten des „IT-Controlling Bund“ erarbeitet und weiterentwickelt.

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 der Architekturrichtlinie entsprechend Abschnitt 1.4 Zielgruppe, insbesondere bei den Behörden und Dienstleistern, in der Anwendung der Architekturvorgabe. Die Anwendung und Bewertung unterliegen dabei den jeweiligen Umsetzenden. Die Bewertung der Implikationen sollte sich auch auf die Beschreibung und Begründung beziehen. 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 2119[30] und sieht zur

[29] IT-Rat. Feinkonzept IT-Controlling Bund (TP4). Beschluss Nr. 2017/11. 06. Juli 2017 unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/it-rat/beschluesse/beschluss_2017_11.pdf?__blob=publicationFile&v=1 zuletzt abgerufen am 10. Januar 2024.

[30] Best Current Practice. 1997 unter https://tools.ietf.org/html/rfc2119 zuletzt abgerufen am 24. April 2019.

Beschreibung des Verbindlichkeitsgrads einer Architekturvorgabe vier Abstufungen vor, die in der nachfolgenden Auflistung verdeutlicht werden.

Muss: - Begriffsdefinition: „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: - Begriffsdefinition: „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: - Begriffsdefinition: „KANN“ kennzeichnet eine Aussage mit dem Charakter einer gestatteten Option. - Anmerkungen: Beschreibung einer zulässigen rechtlichen/ technischen Option.

Darf nicht: - Begriffsdefinition: „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:

- 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 Allgemeine Vorgaben

Neben Architekturvorgaben für die spezifischen Architekturebenen des Metamodells der Rahmenarchitektur IT-Steuerung Bund existieren grundlegende Rahmenbedingungen, die für alle Architekturebenen gelten.

Diese werden im folgenden Kapitel als Allgemeine Vorgaben vorgegeben. Sie sind als grundlegende Basisprinzipien zu verstehen und müssen bei allen IT-Vorhaben (gemäß Kapitel 1.5 Einordnung und

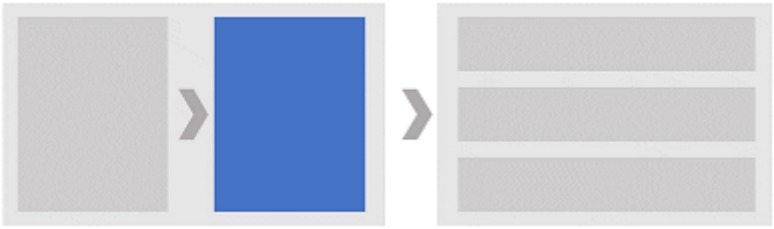

Abbildung 4: Folgende auf die Abbildung des Metamodells aus Kapitel 2.2 wird in dieser kleinen Abbildung die allgemeine Ebene hervorgehoben.

Abgrenzung Vorhaben) berücksichtigt werden, weshalb von einer Darstellung von Abhängigkeiten untereinander abgesehen wird. Die Erarbeitung der Architekturvorgaben basiert auf - der Herleitung von Vorgaben aus den architekturrelevanten strategischen Zielen der IT des Bundes, - der Herleitung von Vorgaben aus dem Grobkonzept zur IT-Konsolidierung Bund und - der Ableitung übergreifender Aspekte aus den spezifischen Vorgaben der Bereiche im Metamodell IT-Steuerung Bund (Geschäftliche Ebene, Diensteebene, Technische Ebene, Informationsebene, Informationssicherheit, Datenschutz und Geheimschutz) (Kapitel 3.3 Allgemeine Vorgaben bis Kapitel 3.6 Technische Vorgaben).

Der Zusammenhang zwischen den Allgemeinen Vorgaben und den spezifischen Architekturvorgaben des Metamodells ist bereits in Kapitel 2.2 Metamodell der „Rahmenarchitektur IT-Steuerung Bund“ aufgezeigt worden.

Die Allgemeinen Vorgaben sollen einen grundlegenden (architektonischen) Bereich abgrenzen, innerhalb dessen die einzelnen Projekte Architekturentscheidungen treffen können. Dieser Bereich wird durch die geschäftlichen Vorgaben, die funktionalen Vorgaben und die technischen Vorgaben weiter konkretisiert.

Die Gesamtheit dieser Vorgaben bildet für die einzelnen IT-Maßnahmen das Rahmenwerk, auf dessen Grundlage Architekturentscheidungen getroffen werden sollen. Ziel ist es, aus den Vorgaben klare Handlungsempfehlungen entnehmen zu können, um die spätere Konsolidierung der IT zu unterstützen. Mit Einhaltung der Architekturvorgaben werden durch die Projekte die strategische IT-Ziele im Sinne des Architekturmanagements eingehalten.

Es folgt eine Übersicht aller Allgemeinen Vorgaben (AVn) und den eng mit diesen Vorgaben verknüpften strategischen Aspekten mit Architekturbezug der IT des Bundes (vgl. 2.1 Strategische Aspekte mit Architekturbezug). Zu diesem Zweck wurde jedes strategische Ziel mit einer Nummer versehen, die anschließend den Vorgaben zugeordnet wird.

Bezeichner	Allgemeine Vorgabe	Verknüpfte strategische Ziele
AV-01	Architekturvorgaben und Recht	Alle
AV-02	Standards, Methoden und Referenzarchitekturen	1, 2, 3, 4, 7, 8 und 9
AV-03	Nachhaltigkeit	10

Bezeichner	Allgemeine Vorgabe	Verknüpfte strategische Ziele
AV-04	Daten	Alle
AV-05	Benutzerfreundlichkeit und Barrierefreiheit	6 und 9
AV-06	Digitale Kollaboration	2, 3, 4, 6, 7, 8 und 9
AV-07	Open Source	2, 3, 4, 8 und 9
AV-08	Informationssicherheit, Datenschutz und Systemkonfiguration	2, 5 und 7
AV-09	Souveränität und Unabhängigkeit	1, 2, 4, 5 und 7
AV-10	Kopplung, Komplexität, Modularität, Wiederverwendbarkeit und Cloud Computing	1, 2, 3, 4, 5, 6, 7, 8 und 10

ID: V-9001-R03

AV-01 Architekturvorgaben und Recht

Die Architekturvorgaben **müssen** eingehalten werden.

Die rechtlichen Rahmenbedingungen **müssen** eingehalten werden.

Beschreibung

- Die Architekturvorgaben müssen in allen Bereichen des Geltungsbereichs[31] der Architekturrichtlinie angewendet werden.
- Die Architekturvorgaben müssen gemäß ihres Verbindlichkeitsgrades[32] eingehalten werden.
- Die Architekturvorgaben müssen entsprechend den Grundsätzen zur Nutzung der Architekturrichtlinie angewendet werden.[33]
- Die geltenden nationalen und internationalen rechtlichen Rahmenbedingungen müssen, bezogen auf den Anwendungsfall, zu jeder Zeit und in allen Bereichen eingehalten werden.
- Die geltenden weiterführenden Rechtsnormen und Beschlüsse müssen, bezogen auf den jeweiligen Anwendungsfall, zu jeder Zeit und in allen Bereichen eingehalten 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

- Bei Umsetzungsvorhaben wird frühzeitig die Konformität mit und die Wirksamkeit von Architekturvorgaben beachtet.
- Zur Umsetzung der Architekturvorgaben sind adäquate Aus- und Weiterbildungsmöglichkeiten im Rahmen eines Architekturmanagements sicherzustellen.
- Das Zusammenspiel zwischen der IT-Governance und den Vorgaben der Architekturrichtlinie ist zu beachten.

[31] Vgl. Kapitel 1.3.

[32] Vgl. Kapitel 3.2.

[33] Vgl. Kapitel 5.

- 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.
- 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-R03

AV-02 Standards, Methoden, Referenzarchitekturen und Interoperabilität

Standards und einheitliche Methoden **sollen** angewendet werden.

Die Weiterentwicklung der IT-Landschaft **muss** sich an Referenzarchitekturen orientieren.

Die Interoperabilität **soll** gewährleistet werden.

Beschreibung

- Offene technische Standards sollen bei der Neu- und Weiterentwicklung von IT-Komponenten und IT-Lösungen verwendet werden.
- Etablierte organisatorische Methoden und Vorgehensmodelle wie insbesondere NAF™[34], V-Modell® XT[35], V-Modell XT Bund[36], Scrum[37], SAFe®[38], TOGAF®[39], ITIL©[40] und COBIT®[41] sollen an die behördenspezifischen Bedarfe angepasst werden.
- Die Weiterentwicklung der IT-Landschaft muss auf Basis von, u. a. auf der Internetseite des CIO des Bundes veröffentlichten, Referenzarchitekturen[42] erfolgen, soweit diese für den entsprechenden Anwendungsfall vorhanden sind.
- Die Interoperabilität von IT-Lösungen soll auf technischer, semantischer, rechtlicher als auch auf organisatorischer Ebene durch die Berücksichtigung des European Interoperability Framework (EIF)[43] sichergestellt werden.
- Die Interoperabilität von IT-Lösungen soll durch die Einhaltung erweiterter Regelungen zur Harmonisierung und Kompatibilität des Managements, der Prozesse, der Schnittstellen und der Netzwerkinfrastruktur gewährleistet werden.

---

[34] Software AG. Installing NAF under IMS TM. Unter https://documentation.softwareag.com/natural/nat426mf2/naf_mf/naf_mf_iins.htm zuletzt abgerufen am 23. Mai 2022.

[35] CIO Bund. V-Modell XT. 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.

[36] CIO Bund. V-Modell XT Bund. 2019 unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitaler-wandel/architekturen-standard/v_modell_xt_bund_pdf.pdf?__blob=publicationFile&v=2 zuletzt abgerufen am 11. Januar 2024.

[37] Scrum.org. Welcome to the home of Scrum. 2022 unter https://www.scrum.org/ zuletzt abgerufen am 23. Mai 2022.

[38] SAFe. Scaled Agile Framework for Lean Enterprises. Unter https://www.scaledagileframework.com/ zuletzt abgerufen am 23. Mai 2022.

[39] The 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 23. Mai 2022.

[40] IT-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 23. Mai 2022.

[41] ISACA. COBIT Framework. 2019 unter https://www.isaca.org/credentialing/cobit zuletzt abgerufen am 23. Mai 2022.

[42] Liste der auf der Website des CIO des Bundes veröffentlichten Referenzarchitekturen: - Gesamtarchitektur für die Dienstekonsolidierung - Rahmendokument für die Domänenarchitekturen - Domänenarchitektur E-Government - Domänenarchitektur Enterprise Resource Planning - Domänenarchitektur Elektronische Verwaltungsarbeit - Domänenarchitektur Infrastruktur - Referenzarchitektur Portale und Integration - Referenzarchitektur Akten- und Lebenszyklusmanagement (ersetzt Teile der Referenzarchitektur elektronische Verwaltungsarbeit) - Referenzarchitektur elektronische Verwaltungsarbeit - Referenzarchitektur Logistik - Referenzarchitektur Personal - Referenzarchitektur Haushalt, Steuerung und Information - Referenzarchitektur Fördermanagement - Referenzarchitektur Normsetzung - Plattformen der Dienstekonsolidierung - Plattform der IT-Betriebskonsolidierung Bund - Organisationskonzept elektronische Verwaltungsarbeit

[43] Europäische Kommission. European Interoperability Framework (EIF). 2017 unter https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0018.02/DOC_3&format=PDF zuletzt abgerufen am 15. März 2022.

- Die Interoperabilität von IT-Lösungen hinsichtlich des Daten- und Informationsaustausches soll durch die Nutzung von geltenden standardisierten Austauschformaten[44] sichergestellt werden.
- Die Interoperabilität von IT-Lösungen soll hinsichtlich der Kompatibilität von Betriebsumgebungen sichergestellt werden.
- Die Interoperabilität von IT-Lösungen, die im Bereich der NATO eingesetzt werden, soll durch die Berücksichtigung der Allied Data Publication 34 (ADatP-34) („NATO Interoperability Standards and Profiles (NISP)"), STANAG 552420, sichergestellt werden.

Begründung

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

Abhängigkeiten

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

Implikationen

[44] Technische Spezifikation der Architekturrichtlinie für die IT des Bundes. Abschnitt 2.3.3 bis 2.3.7.

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

ID: V-9012-R03

AV-03 Nachhaltigkeit

Die Nachhaltigkeit von Informationstechnik **soll** über den gesamten Lebenszyklus sichergestellt werden.

Beschreibung

- Die ökologischen und sozialen Nachhaltigkeitsziele sollen gemäß der IT-Beschaffungsstrategie[45] umgesetzt werden.
- Die Kriterien aus Umweltzeichen gemäß „Blauer Engel“[46], dem Europäischen Umweltzeichen[47] und dem Energy Label[48] sollen umgesetzt werden.
- Der Betrieb von IT und Rechenzentren soll gemäß des Eckpunktepapiers der KG Green IT[49] auf eine Optimierung des Energieverbrauches ausgerichtet werden.
- Der Ressourcenverbrauch von IT-Lösungen soll über den Lebenszyklus bei möglichst optimaler Auslastung minimiert werden.
- Die Verwertung von Informationstechnik nach Nutzungsende soll bei weiter bestehender Funktionsfähigkeit auf dem Reuse-Markt und anhand der Vorgaben des Elektrogesetzes[50] erfolgen.

Begründung

- Mit der Beschaffung von umweltverträglicher IT und ressourceneffizienter Software werden die Regelungen der „Allgemeinen Verwaltungsvorschrift zur Beschaffung energieeffizienter Leistungen (AVV-EnEff)“[51] eingehalten.
- Die Einhaltung der Verpflichtungen aus dem Maßnahmenprogramm Nachhaltigkeit – Weiterentwicklung 2021[52] der Bundesregierung, aus dem Klimaschutzprogramm 2030 und dem

[45] KoITB. IT-Beschaffungsstrategie für die zentralen IT-Beschaffungsstellen. 11. Dezember 2018 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.

[46] Blauer Engel. Energieeffizienter Rechenzentrumsbetrieb (DE-ZU 161). Unter https://www.blauer-engel.de/de/produktwelt/rechenzentren zuletzt abgerufen am 10. März 2022.

[47] RAL gemeinnützige GmbH. Über das EU Ecolabel. Unter https://eu-ecolabel.de/eu-ecolabel-das-umweltzeichen-ihres-vertrauens/ueber-das-eu-ecolabel zuletzt abgerufen am 10. März 2022.

[48] Europäische Kommission. Energielabel und Ökodesign. 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 10. März 2022.

[49] IT-Planungsrat. Beschluss 2021/11. 17. März 2021 unter https://www.it-planungsrat.de/beschluss/beschluss-2021-11 zuletzt abgerufen am 15. März 2022.

[50] BMJ. Gesetz über das Inverkehrbringen, die Rücknahme und die umweltverträgliche Entsorgung von Elektro- und Elektronikgeräten. 2015 unter https://www.gesetze-im-internet.de/elektrog_2015/index.html zuletzt abgerufen am 10. März 2022.

[51] BMWi. Allgemeine Verwaltungsvorschrift zur Beschaffung energieeffizienter Leistungen (AVV-EnEff). 18. Mai 2020 unter https://www.bmwi.de/Redaktion/DE/Downloads/A/avv-eneff.pdf?__blob=publicationFile&v=8 zuletzt abgerufen am 28. Februar 2022.

[52] Staatssekretärsausschuss für nachhaltige Entwicklung. Maßnahmenprogramm Nachhaltigkeit. 25. August 2021 unter https://www.bundesregierung.de/resource/blob/998008/1953740/1fa562505e19485b107b61ddb19ea0a7/2021-08-25-massnahmenprogramm-nachhaltigkeit-2021-data.pdf?download=1 zuletzt abgerufen am 07. März 2022.

Deutschen Ressourceneffizienzprogramm III werden gefördert.

- 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.

Abhängigkeiten

- Keine

Implikationen

- Die Anschaffungskosten für Hardware können im Zusammenhang mit dieser Richtlinie steigen, da umweltfreundliche Geräte häufig preisintensiver sind.
- Die ergänzenden Hilfestellungen des Umweltbundesamts sowie der Kompetenzstelle nachhaltige Beschaffung (KNB) sollten berücksichtigt werden.
- Es sollte die Möglichkeit des (dynamischen) Up-/ Down-Sizing, um bedarfsgerechte Hardwarenutzung zu fördern, beachtet werden.
- 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.6[53] berücksichtigt werden.

---

[53] Bundesamt für Sicherheit in der Informationstechnik. IT-Grundschutz-Kompendium. Februar 2022 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2022.pdf?__blob=publicationFile&v=3#download=1 zuletzt abgerufen am 15. März 2022.

ID: V-9080-R02

AV-04 Daten

Daten **müssen** die Grundlage für das Verwaltungshandeln sein.

Beschreibung

- Daten müssen interdisziplinär für die Generierung von Information und Wissen bereitgestellt und genutzt werden.
- Daten müssen zur Steigerung der Transparenz und Nachvollziehbarkeit von Entscheidungen eingesetzt werden.
- 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

- FV-05 Information, Zeichen und Daten
- GV-08 Daten-Governance
- TV-05 Datenbanksysteme

Implikationen

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

ID: V-9007-R03

AV-05 Benutzerfreundlichkeit und Barrierefreiheit

Die Benutzerfreundlichkeit und Barrierefreiheit **müssen** sichergestellt werden.

Beschreibung

- Die Benutzerfreundlichkeit von IT-Lösungen muss durch die Anwendung der DIN EN ISO 9241 110[54], des EN 301 549[55] und des Styleguides der Bundesregierung[56] sichergestellt werden.
- Die Barrierefreiheit von IT-Lösungen muss gemäß dem § 12a Behindertengleichstellungsgesetz[57], dem Barrierefreiheitsstärkungsgesetz[58], dem Industriestandard DIN EN ISO 9241 171[59] und der Barrierefreie Informationstechnik Verordnung – BITV 2.0[60] sichergestellt werden, ferner ist die europäische Norm DIN-EN 301549[61] zu berücksichtigen.

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
- FV-04 Anwendungen für den Bundesclient

---

[54] DIN. DIN EN ISO 9241-110 - Ergonomie der Mensch-System-Interaktion – Teil 11. Unter https://www.din.de/de/mitwirken/normenausschuesse/naerg/veroeffentlichungen/wdc-beuth:din21:279590417 zuletzt abgerufen am 10. März 2022.

[55] ETSI. EN 301 549. August 2018 unter https://www.etsi.org/deliver/etsi_en/301500_301599/301549/02.01.02_60/en_301549v020102p.pdf zuletzt abgerufen am 06. April 2022.

[56] Presse- und Informationsamt der Bundesregierung. Das Corporate Design der Bundesregierung. Unter https://styleguide.bundesregierung.de/sg-de zuletzt abgerufen am 10. Februar 2022.

[57] BMJ. Gesetz zur Gleichstellung von Menschen mit Behinderungen (Behindertengleichstellungsgesetz - BGG). 1. Juli 2021 unter https://www.gesetze-im-internet.de/bgg/__12a.html zuletzt abgerufen am 06.04.2022.

[58] BMAS. Barrierefreiheitsstärkungsgesetz. 22. Juli 2021 unter https://www.bmas.de/DE/Service/Gesetze-und-Gesetzesvorhaben/barrierefreiheitsstaerkungsgesetz.html zuletzt aufgerufen am 01. März 2022.

[59] DIN. DIN EN ISO. Ergonomie der Mensch-System-Interaktion – Teil 171: Leitlinien für die Zugänglichkeit von Software. 2008 unter https://www.din.de/de/mitwirken/normenausschuesse/naerg/veroeffentlichungen/wdc-beuth:din21:107114575 zuletzt abgerufen am 28. Februar 2022.

[60] BMJ. Barrierefreie-Informationstechnik-Verordnung – BITV 2.0. 12. September 2011 unter https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html zuletzt abgerufen am 28. Februar 2022.

[61] DIN. DIN EN 301549 Barrierefreiheitsanforderungen für IKT-Produkte und -Dienstleistungen. Englische Fassung EN 301549 V3.2.1. 2021 unter https://www.din.de/de/mitwirken/normenausschuesse/naerg/entwuerfe/wdc-beuth:din21:342462419 zuletzt abgerufen am 14. April 2022.

- TV-01 Entwicklung, Programmiersprachen und Qualitätsmanagement

Implikationen

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

ID: V-9074-R02

AV-06 Digitale Kollaboration

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

Beschreibung

- Zentral bereitgestellte kollaborative Dienste sollen bevorzugt für die digitale Zusammenarbeit verwendet werden.
- Kollaborative Funktionalitäten sollen zur Nutzung innerhalb einer IT-Anwendung oder durch Einbindung einer Drittanwendung in die genutzte IT-Anwendung bereitgestellt werden.
- Kollaborative Funktionalitäten sollen eine digitale behördenübergreifende Zusammenarbeit in Echtzeit ermöglichen.

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[62]. Darüber hinaus wird die Familienfreundlichkeit durch die Möglichkeit des mobilen Arbeitens[63] gestärkt.

Abhängigkeiten

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

Implikationen

- Bei der Einbindung kollaborativer Dienste ist die Vermeidung von Medienbrüchen je Anwendungsgebiet (z. B. unterschiedliche Chatprogramme) zu beachten.
- 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.
- Beim Einsatz digitaler kollaborativer Dienste sind die behördeninternen Nutzungsregeln zu beachten und bedarfsweise weiterzuentwickeln.
- Bei der Nutzung von kollaborativen Funktionalitäten ist die Einstufung der Inhalte zu beachten.

---

[62] BMI. Verwaltung-Innovativ. Personal. Unter https://www.verwaltung-innovativ.de/DE/Regierungsprogramm/lp_17/Regierungsprogramm_Monitoring/Artikel/personal.html zuletzt abgerufen am 25. Februar 2022.

[63] BMI. Arbeitsgruppe „Der öffentliche Dienst als attraktiver und moderner Arbeitgeber". 2017 unter https://www.demografie-portal.de/DE/Politik/Bund/Dialogprozess/Arbeitsgruppen/Oeffentlicher-Dienst/ergebnisbericht-2017.pdf zuletzt abgerufen am 25. Februar 2022.

ID: V-9075-R02

AV-07 Open Source

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

Beschreibung

- Open Source soll kontinuierlich in ihrem Einsatz ausgebaut werden.
- Open Source und deren Weiterentwicklung soll durch eine aktive Beteiligung an der Open Source Community gefördert werden.
- Open Source Software, die durch oder für die öffentliche Verwaltung entwickelt wird, soll auf der Open CoDE Plattform der öffentlichen Verwaltung[64] oder entsprechenden Plattformen 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 der Beschlüsse des Koalitionsvertrages[65] hinsichtlich Open Source gefördert. Ferner wird der Beschluss 2020/39[66] 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, Zeichen und Daten

Implikationen

- Die Vorteile, die sich aus der Nutzung von Open Source Software ergeben, sollten beim Beschaffungsprozess besonders beachtet werden.

---

[64] Die Open CoDE Plattform ist unter folgendem Link zu erreichen: https://opencode.de/.

[65] SPD / GRÜNE / FDP. Mehr Fortschritt wagen. 2021 unter https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800 zuletzt abgerufen am 13. April 2022.

[66] IT-Planungsrat. OZG-Umsetzung. 18. September 2020 unter https://www.it-planungsrat.de/beschluss/beschluss-2020-39 zuletzt abgerufen am 03. März 2022.

- Bei beschaffter Open Source Software ist das potenziell notwendige Angebot von Servicedienstleistungen zu beachten.
- Die zu erwartenden Aufwände für eine aktive Beteiligung an der Open Source Community sollten bei der Planung von Entwicklungsprojekten berücksichtigt werden.
- Bei der Veröffentlichung von Quellcodes sollte eine angemessene Lizenzierung beachtet werden.

ID: V-9004-R04

AV-08 Informationssicherheit, Datenschutz, Geheimschutz und Systemgrundkonfiguration

Die Informationssicherheit, der Datenschutz und der Geheimschutz **müssen** gewährleistet werden.

Eine sichere Systemgrundkonfiguration **muss** gewährleistet werden.

Beschreibung

- Die Informationssicherheit muss durch den Aufbau eines Informationssicherheitsmanagementsystems (ISMS) gemäß BSI-Standards 200-1[67], 200-2[68] und 200-3[69] gewährleistet werden.
- Die Informationssicherheit muss gemäß den geltenden Vorgaben des § 8 BSIG[70] umgesetzt werden.
- Die Informationssicherheit muss die Vorgaben des UP Bund (2017)[71] berücksichtigen.
- Der personelle Geheimschutz muss gemäß dem Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz - SÜG)[72] sowie der allgemeinen Verwaltungsvorschrift zum personellen Geheimschutz und zum vorbeugenden personellen Sabotageschutz (SÜG Ausführungsvorschrift - SÜG-AVV)[73] sichergestellt werden.
- Der materielle Geheimschutz muss gemäß der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA)[74] unter Berücksichtigung von gegebenenfalls vorhandenen ressortspezifischen Anpassungen sichergestellt werden.
- Der Datenschutz muss gemäß den gesetzlichen Regelungen, insbesondere der Datenschutz-

[67] BSI. BSI-Standard 200-1. Januar 2021 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf?__blob=publicationFile&v=2 zuletzt abgerufen am 18. März 2022.

[68] BSI. BSI-Standard 200-2. 15. November 2017 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2;%20zuletzt%20abgerufen%20am%2018.%20M%C3%A4rz%202022 zuletzt abgerufen am 24. März 2022.

[69] BSI. BSI-Standard 200-3. 15. November 2017 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2;%20zuletzt%20abgerufen%20am%2018.%20M%C3%A4rz%202022 zuletzt abgerufen am 24. März 2022.

[70] BSI. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) § 8 Vorgaben des Bundesamtes. 2009 unter https://www.gesetze-im-internet.de/bsig_2009/__8.html zuletzt abgerufen am 18. März 2022.

[71] BMI. Umsetzungsplan Bund 2017. 01. September 2017 unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.pdf?__blob=publicationFile&v=3 zuletzt abgerufen am 23. Mai 2022.

[72] BMJ. Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen. 05. Juli 2022 unter https://www.gesetze-im-internet.de/s_g/BJNR086700994.html#BJNR086700994BJNG000100307 zuletzt abgerufen am 02. März 2022.

[73] BMJ. Allgemeine Verwaltungsvorschrift zum personellen Geheimschutz und zum vorbeugenden personellen Sabotageschutz - SÜG-Ausführungsvorschrift (SÜG-AVV). 08. Juni 2022 unter https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_08062022_SII554001415.htm zuletzt abgerufen am 10. Januar 2024.

[74] BMJ. Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA). 13. März 2023 unter https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_13032023_SII554001405.htm zuletzt abgerufen am 10. Januar 2024.

grundverordnung (DSGVO)[75] und dem Bundesdatenschutzgesetz (BDSG)[76] sowie dem Beschluss IT-Planungsrat Nr. 2020/06 vom 25. März 2020 zum Standard-Datenschutzmodell (SDM)[77], sichergestellt werden.
- Eine sichere Systemgrundkonfiguration muss durch die Aktivierung aller relevanten Sicherheitseinstellungen in der Grundkonfiguration einer IT-Lösung sichergestellt werden.
- Eine sichere Systemgrundkonfiguration muss durch regelmäßige, in adäquaten Abständen durchgeführte Sicherheitsaudits geprüft werden.

Begründung

- 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.
- 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

- FV-08 Identitätsinformation, Zugriffssteuerung, Sicherheitskonzeption, Schutzbedarf, Quality of Service, Security by Design, Separierung und Mandantentrennung
- TV-02 Schnittstellen
- TV-08 Kryptographie, Sicherheitsrelevante Ereignisse, Schadprogrammabwehr
- TV-10 Betrieb

Implikationen

- Die Klassifikation des Schutzbedarfes von Daten, Informationen und Algorithmen ist zu beachten.

---

[75] EU. Datenschutzgrundverordnung (DSGVO). 27. April 2016 unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679 zuletzt abgerufen am 11. Januar 2024.

[76] BMJ. Bundesdatenschutzgesetz (BDSG). 25. Mai 2018 unter https://www.gesetze-im-internet.de/bdsg_2018/ zuletzt abgerufen am 02. März 2022.

[77] IT-Planungsrat. Beschluss vom 25. März 2020. Standard-Datenschutzmodell unter https://www.it-planungsrat.de/beschluss/beschluss-2020-06 zuletzt abgerufen am 02. März 2022.

- Die Referenzmaßnahmen des Standard-Datenschutzmodells sind nach Möglichkeit umzusetzen.
- Vor Inbetriebnahme neuer IT-Systeme sollten notwendige Schutzmaßnahmen (wie z. B. die Konfigurationsempfehlungen des BSI[78]) evaluiert und durch entsprechende Sicherheitseinstellungen beachtet werden.
- Es ist zu beachten, dass die Sicherheitseinstellungen, die die höchste Sicherheit gewährleisten, der Nutzerfreundlichkeit entgegenstehen können.
- Bei der Aktivierung der Sicherheitseinstellungen sollte der zur Bewältigung der Aufgabenstellung benötigte Funktionsumfang beachtet werden.

---

[78] Bundesamt für Sicherheit in der Informationstechnik. SiSyPHuS Win10: Empfehlung zur Härtung von Windows 10 mit Bordmitteln. Februar 2022 unter https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/AP11/SiSyPHuS_AP11_node.html zuletzt abgerufen am 15. März 2022.

ID: V-9070-R03

AV-09 Souveränität und Unabhängigkeit

Die Digitale Souveränität **muss** sichergestellt werden.

Die Hersteller- und Anbieterunabhängigkeit **soll** sichergestellt werden.

Beschreibung

- Die IT-Lösungen müssen (der Betriebshoheit) unterliegen und damit vollumfänglich kontrollier- und steuerbar sein.
- Die IT-Architektur muss flexibel um neue Elemente und für bestehende Elemente um neue Funktionen erweiterbar sein.
- Die in der IT-Architektur eingesetzten IT-Komponenten und IT-Lösungen müssen durch Alternativlösungen austauschbar sein.
- Die Kompetenzen für die Entwicklung, Wartung, Pflege und den Betrieb von IT-Lösungen müssen in ausreichendem Umfang beim internen Personal vorhanden sein.
- Die Hersteller- und Anbieterunabhängigkeit soll durch die Verfolgung eines Multi-Vendor-Ansatzes, bevorzugt in einer IT-Sourcing-Strategie, für die eingesetzten IT-Lösungen sichergestellt werden.
- Die Herstellerunabhängigkeit soll durch die Vermeidung von Abhängigkeiten zu herstellerspezifischen Funktionen, Schnittstellen und Hardware-Technologien/ Plattformen sichergestellt werden.
- Die Anbieterunabhängigkeit soll durch die Vermeidung von Abhängigkeiten anbieterspezifischer IT-Serviceleistungen 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 2021/09[79] 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.

[79] IT-Planungsrat. Strategie zur Stärkung der digitalen Souveränität für die IT der Öffentlichen Verwaltung. Januar 2021 unter https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf zuletzt abgerufen am 09. März 2022.

Abhängigkeiten

- Keine

Implikationen

- Beim Einsatz neuer IT-Komponenten oder IT-Lösungen sind bereits bestehende Abhängigkeiten zu beachten.
- Bei der Nutzung innovativer Technologien sind durch den unwesentlichen Grad der Verbreitung sowie die geringe Anzahl an Anbietenden mögliche entstehende Abhängigkeiten besonders zu beachten.
- Die notwendigen Ressourcen für die Sicherstellung der Digitalen Souveränität sind bei der Planung zu berücksichtigen.
- 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.
- Die Vorgaben des Vergaberechts, insbesondere der Grundsatz der produktneutralen Beschaffung[80], sollten beachtet und die ergänzenden Vertragsbedingungen der EVB-IT bei der Beschaffung in ihrer jeweils gültigen Fassung angewendet werden.
- Bei der Einführung von Multi-Vendor-Strategien sollte die Einrichtung notwendiger Rollen und Prozesse beachtet werden.
- 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.

---

[80] BMJ. Verordnung über die Vergabe öffentlicher Aufträge (Vergabeverordnung – VgV) §31 Leistungsbeschreibung. 2016 unter https://www.gesetze-im-internet.de/vgv_2016/__31.html zuletzt abgerufen am 10. März 2022.

ID: V-9011-R03

AV-10 Kopplung, Komplexität, Modularität, Wiederverwendbarkeit und Cloud Computing

Lose Kopplung **muss** sichergestellt werden.

Die Komplexität **soll** auf ein notwendiges Maß reduziert werden.

Die Modularität und Wiederverwendbarkeit **sollen** sichergestellt werden.

Das Cloud Computing **soll** bevorzugt genutzt werden.

Beschreibung

- Die lose Kopplung muss durch den Einsatz von IT-Komponenten mit keinen oder geringen Abhängigkeiten zueinander sichergestellt werden.
- Die lose Kopplung muss eine unabhängige Nutzung, Aktualisierung und Weiterentwicklung der eingesetzten IT-Komponenten ermöglichen.
- Die lose Kopplung muss einen autonomen Betrieb der eingesetzten IT-Komponenten ermöglichen.
- Die lose Kopplung muss bei der Neu- und Weiterentwicklung von IT-Komponenten und IT-Lösungen umgesetzt werden.
- Die Komplexität von IT-Lösungen und IT-Architekturen soll durch die Reduzierung der Anzahl sowie der Heterogenität der eingesetzten IT-Komponenten auf ein notwendiges Maß beschränkt werden.
- Die Komplexität von IT-Lösungen und IT-Architekturen soll durch die Reduzierung der Anzahl der Abhängigkeiten von IT-Komponenten auf ein notwendiges Maß beschränkt werden.
- Die Komplexität von IT-Lösungen und IT-Architekturen soll durch die Vermeidung von funktionellen Redundanzen auf ein notwendiges Maß reduziert werden.
- Die Komplexität von IT-Lösungen und IT-Architekturen soll durch eine fachliche Strukturierung reduziert werden.
- Die Modularität soll bei der Entwicklung von IT-Lösungen durch die Verwendung von IT-Komponenten, die das „Separation of Concerns“-Prinzip einhalten, sichergestellt werden.
- Die Modularität soll sich an einheitlichen Kriterien hinsichtlich Wirtschaftlichkeit orientieren.
- Die Wiederverwendbarkeit von IT-Komponenten und IT-Lösungen soll bei der Neu- und Weiterentwicklung berücksichtigt werden.
- Cloud Computing soll als prioritäre Infrastruktur- und Plattformkomponente für die Bereitstellung und Nutzung von IT-Lösungen verwendet werden.
- Für das Cloud Computing kompatible Anwendungen sollen bei der Beschaffung und in der Anwendungsentwicklung bevorzugt werden.
- Beim Einsatz von Cloud Computing sollen die Standards der Deutschen Verwaltungscloud-

Strategie (DVS)[81], Gaia-X[82], Sovereign Cloud Stack (SCS)[83] oder Bundescloud eingehalten werden.
- Für den Einsatz von Cloud Computing müssen bei Vertragsabschlüssen die ergänzenden Vertragsbedingungen Cloud (EVB-IT Cloud)[84] in der jeweils gültigen Fassung angewendet werden.

Begründung

- 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.
- Wesentlicher Erfolgsfaktor für den Aufbau der 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.
- 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.
- Modularität bietet die Möglichkeit, dass die einzelnen IT-Komponenten separat geplant, entwickelt und getestet werden können.
- Durch die Umsetzung der Vorgabe wird die im Rahmen der OZG-Umsetzung geforderte Wiederverwendung und Nachnutzung als Servicestandard gefördert.[85]
- 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 2020/54[86] und

[81] IT-Planungsrat. Deutsche Verwaltungscloud-Strategie: Rahmenwerk der Zielarchitektur. August 2021 unter https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-46_Deutsche_Verwaltungscloud-Strategie_AL1.pdf zuletzt abgerufen am 15. Februar 2022.

[82] BMWi. Gaia-X. Unter https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html zuletzt abgerufen am 16. Februar 2022.

[83] BMWi. Sovereign Cloud Stack. Unter https://scs.community/ zuletzt abgerufen am 16. Februar 2022.

[84] CIO Bund. Aktuelle EVB-IT. Unter https://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Aktuelle_EVB-IT/aktuelle_evb_it_node.html#doc4623280bodyText3 zuletzt abgerufen am 18. März 2022. Durch die Anwendung der ergänzenden Vertragsbedingungen Cloud (EVB-IT Cloud) wird die Vorgabe des § 55 Abs. 2 BHO umgesetzt.

[85] BMI. Onlinezugangsgesetz. Prinzip 14: Wiederverwendung und Nachnutzung unter https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/servicestandard/prinzip-14/prinzip-14-node.html zuletzt abgerufen am 09. Januar 2024.

[86] IT-Planungsrat. Deutsche Verwaltungscloud-Strategie: Föderaler Ansatz. November 2020 unter https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-54_Deutsche_Verwaltungscloud_Strategie.pdf zuletzt abgerufen am 15. Februar 2022.

2021/46[87] zur DVS getroffen.

Abhängigkeiten

- FV-09 Entkopplung
- TV-01 Entwicklung, Programmiersprachen und Qualitätsmanagement
- TV-10 Betrieb

Implikationen

- Bei der Umsetzung der losen Kopplung sollten gängige Architektur und Entwurfsmuster berücksichtigt werden.[88]
- Die bei der Umsetzung der losen Kopplung entstehende Komplexität sollte beachtet werden.
- Der erhöhte Planungs- und Umsetzungsaufwand, der durch die Entkopplung von Diensten entsteht, sollte beachtet werden.
- Mechanismen zur Reduktion der Komplexität sind in strategischen, prozessualen und technischen Strukturen zu verankern.
- 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.
- Es sollten spezifische Maßgaben hinsichtlich des Designs von logischen Teilblöcken zur Optimierung der Wiederverwendbarkeit berücksichtigt werden.
- Die Wiederverwendung und Wiederverwendbarkeit von IT-Komponenten sollte bei Neu- und Weiterentwicklungen im Rahmen übergreifender Architekturgremien beachtet werden.
- Durch die Umsetzung der Modularität kann es zu Performanceverlusten kommen, dies sollte berücksichtigt werden.
- Der erhöhte Planungs- und Umsetzungsaufwand für IT-Lösungen, der durch die Entkopplung von IT-Komponenten entsteht, sollte beachtet werden.
- Modularisierung sollte bereits bei der Architekturkonzeption und in Ausschreibungsunterlagen berücksichtigt werden.
- Standards für die Infrastruktur- und Plattformbereitstellungen für Cloud Computing sind zu berücksichtigen.
- 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.

---

[87] IT-Planungsrat. Deutsche Verwaltungscloud-Strategie: Rahmenwerk der Zielarchitektur. August 2021 unter https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-46_Deutsche_Verwaltungscloud-Strategie_AL1.pdf zuletzt abgerufen am 15. Februar 2022.

[88] IEEE. Design patterns in object oriented analysis and design. 12. August 2011 unter https://ieeexplore.ieee.org/abstract/document/5982229 zuletzt abgerufen am 06. April 2022.

3.4 Geschäftliche Vorgaben

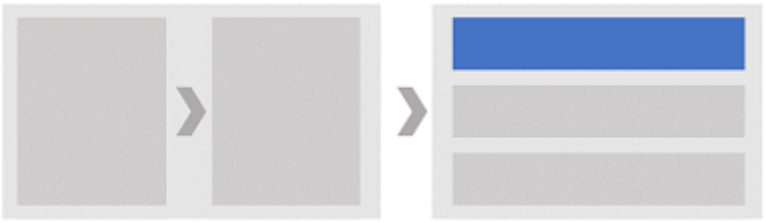

Abbildung 5: Folgende auf die Abbildung des Metamodells aus Kapitel 2.2 wird in dieser kleinen Abbildung die geschäftliche Ebene hervorgehoben.

Dieses Kapitel beinhaltet Vorgaben mit einem Bezug zu Projekt- und Prozessmanagement von Behörden. Ziel dieser Vorgabe ist, die Behörden auf organisatorischer Ebene bei der Umsetzung der IT-Konsolidierung zu unterstützen.

ID: V-9015-R03

GV-04 Projektmanagement

Das Projektmanagement **soll** methodengestützt durchgeführt werden.

Beschreibung

- Zur Einführung von IT-Lösungen und zur Durchführung von IT-Maßnahmen soll der Praxisleitfaden „Projektmanagement für die öffentliche Verwaltung“ beachtet werden.[89]
- Bei der Durchführung von Organisationsprojekten soll zudem das Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung (kurz: Organisationshandbuch) berücksichtigt werden.
- Andere Projektmanagementmethoden (z. B. V-Modell XT®[90], V-Modell XT Bund[91] und S-O-S-Methode[92]) und neue Methoden zum agilen Projektmanagement (z. B. Scrum) können als Alternative oder Ergänzung zu den hier vorgeschlagenen klassischen Methoden eingesetzt 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 Standards, Methoden, Referenzarchitekturen und Interoperabilität

Implikationen

- Keine

---

[89] BMI. Praxisleitfaden Projektmanagement für die Öffentliche Verwaltung. 20. November 2013 unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/moderne-verwaltung/praxisleitfaden-projektmanagement.html zuletzt abgerufen am 23. Mai 2022.

[90] CIO Bund. Das V-Modell XT. 2022 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 10. Januar 2024.

[91] CIO Bund. V-Modell XT Bund. 2019 unter https://www.cio.bund.de/Webs/CIO/DE/digitaler-wandel/Achitekturen_und_Standards/V_modell_xt/V_modell_xt_bund/v_modell_xt_bund-node.html; zuletzt abgerufen am 10. Januar 2024.

[92] BVA. S-O-S-Methode für Großprojekte. 2022 unter https://www.bva.bund.de/DE/Services/Behoerden/Beratung/Beratungszentrum/GrossPM/_documents/stda_sos_methode.html zuletzt abgerufen am 31. März 2022.

ID: V-9016-R03

GV-05 Prozessmanagement

Ein Prozessmanagement **muss** standardisiert etabliert werden.

Prozessmodelle **müssen** auf standardisierten Notationen aufbauen.

Für den Austausch von Prozessmodellen **müssen** spezifische Austauschformate verwendet werden.

Beschreibung

- Zur begleitenden Einführung der elektronischen Unterstützung von Verwaltungsabläufen muss ein Prozessmanagement in den Behörden, unter Berücksichtigung der DIN SPEC 90158 „Handlungsleitfaden für ein strategisches und operatives Prozessmanagement in der öffentlichen Verwaltung“, etabliert werden.
- Sofern für die Etablierung eines Prozessmanagements Beratungsbedarf besteht, können die Beratungsleistungen der Kompetenzzentren Prozessmanagement genutzt werden. Darüber hinaus ist das Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung des BMI[93] zu berücksichtigen.
- Zusätzlich müssen die Muster- und Referenzprozesse aus den Bereichen Haushalt und Beschaffung sowie das Referenzmodell des Projektes E-Beschaffung und bei Nutzung der E-Akte Bund das Vorgehensmodell des Projektes E-Akte als Grundlage für die Architekturen in diesen Bereichen beachtet werden.
- Das Föderale Informationsmanagement (FIM) liefert nach dem Baukastenprinzip standardisierte Informationen zu den Arbeitsabläufen von Verwaltungsleistungen (Antrags-, Genehmigungs- und Anzeigeverfahren).
- FIM dient als ein methodischer Standard für die Digitalisierung von Verwaltungsdienstleistungen für das Online-Zugangsgesetz (OZG) und weitere Anwendungsbereiche.
- Die Vorgaben und Standards für FIM sind unter fimportal.de veröffentlicht.

Folgende grafische Modellierungssprachen und Notationen müssen für die jeweiligen Aufgabenfelder verwendet werden:

- Modellierung von Prozessen
  - Für die Modellierung von Geschäfts- und technischen Prozessen muss die Business Process Model and Notation (BPMN) 2.0 verwendet werden. BPMN ist eine grafische Notation zur Modellierung und Ausführung von Geschäftsprozessen. Dabei dürfen ausschließlich Modellierungselemente verwendet werden, die der BPMN-Standard der Version 2.0 vorsieht. Die Verwendung softwarespezifischer BPMN-Erweiterungen ist nicht erlaubt, um

[93] BMI und BVA. Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung. Unter: https://www.orghandbuch.de/OHB/DE/node.html zuletzt abgerufen am 01. April 2022.

Lock-In-Effekte und Probleme bei der Datenübertragung zu vermeiden. Notationselemente und BPMN 2.0-spezifische Konventionen sind ausschließlich so zu verwenden, wie es von der Object Management Group[94] (OMG) vorgesehen ist.
  - Für Fallmanagement z. B. im juristischen Umfeld muss die Case Management Model and Notation (CMMN) 1.1 verwendet werden.
  - CMMN-Diagramme können im Rahmen von Prozessmanagement in eine BPMN Diagrammstruktur integriert werden.
  - Für Entscheidungsmodelle im Geschäftsprozessmanagement zum Beschreiben und Modellieren von wiederholbaren und auf festen Parametern basierenden Entscheidungen in Organisationen muss die Decision Model and Notation (DMN) 1.2 verwendet werden.
  - DMN-Diagramme können in eine BPMN Diagrammstruktur integriert werden.
  - Für die Darstellung der Ablauforganisation bzw. funktionalen Aufbaustrukturen müssen Wertschöpfungskettendiagramme (WKD) verwendet werden. Diese können mit BPMN-Diagrammen verknüpft werden.
  - Die Ereignisgesteuerte Prozesskette (EPK auch in der Ausprägung eEPK) darf nicht verwendet werden, wenn eine Behörde mit Geschäftsprozessmodellierung neu beginnt. Vorhandene EPK-Diagramme müssen mittelfristig im Rahmen der Pflege nach BPMN 2.0 migriert werden. Neue Prozesse sollen nicht in EPK modelliert werden.

- Modellierung von Organisationsarchitekturen

  - Für die Modellierung von Aufbauorganisationen beziehungsweise dem hierarchischen Aufbau der Organisation sowie Unternehmens- beziehungsweise Behördenarchitekturen soll ArchiMate 3.1 verwendet werden.

- Softwarearchitekturen

  - Für die Abbildung von Software-Architekturen und vergleichbaren Aufgaben soll je nach Anwendungszweck entweder die Unified Modelling Language (UML) in Version 2 oder ArchiMate 3.1 verwendet werden.

Für den Austausch von Prozessmodellen müssen folgende Austauschformate genutzt werden:

- XProzess 2.0 oder höher.

Darin eingebettet sind die folgenden Standards zu verwenden:

- Business Process Modeling Language (BPML) 2.0

[94] Die Object Management Group ist ein Konsortium, das sich mit der Entwicklung von Standards für die herstellerunabhängige systemübergreifende objektorientierte Programmierung beschäftigt.

- XML Process Definition Language (XPDL) 2.1 Anmerkung: Keines der genannten Austauschformate kann derzeit eine fehlerfreie Übertragung der Daten zwischen IT-Anwendungen unterschiedlicher Hersteller gewährleisten.

Begründung

- Nach § 9 Absatz 1 EGovG[95] sollen Behörden des Bundes Verwaltungsabläufe, die erstmals zu wesentlichen Teilen elektronisch unterstützt werden, vor Einführung der informationstechnischen Systeme unter Nutzung gängiger Methoden dokumentieren, analysieren und optimieren.
- Die Prozesse sollen erhoben, dargestellt, bewertet und verbessert werden.
- Nach § 3 Absatz 2a EGovG[96] sollen Behörden mit Unterstützung der zentralen FIM-Bundesredaktion allgemeine Leistungsinformationen in standardisierter Form bereitstellen.
- Dies beinhaltet auch die Prozessdokumentation.
- Zudem gelten der Beschluss 2016/29[97] des IT-Planungsrats zur Etablierung von FIM als Anwendung bzw. Produkt des IT-Planungsrats und der Beschluss 2019/01[98] des IT-Planungsrats zur Nutzung von FIM im Rahmen von OZG.
- Die korrekte Abbildung von Prozessen über Verwaltungsabläufe, die erstmals zu wesentlichen Teilen elektronisch unterstützt werden sollen, ist eine elementare Voraussetzung für die zukünftige IT-Ausrichtung und deren organisatorische Rahmenbedingungen der Bundesverwaltung.
- 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.

[95] Gesetze im Netz. Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz - EGovG) § 9 Optimierung von Verwaltungsabläufen und Information zum Verfahrensstand. 25. Juli 2013 unter https://www.gesetze-im-internet.de/egovg/__9.html zuletzt abgerufen am 06. April 2022.

[96] Gesetze im Netz. Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz - EGovG) § 3 Information zu Behörden und über ihre Verfahren in öffentlich zugänglichen Netzen. 25. Juli 2013 unter https://www.gesetze-im-internet.de/egovg/__3.html zuletzt abgerufen am 06. April 2022.

[97] IT-Planungsrat. Steuerungsprojekt Förderales Informationsmanagement (FIM). 13. September 2016 unter https://www.it-planungsrat.de/beschluss/beschluss-2016-29 zuletzt abgerufen am 22. April 2022.

[98] IT-Planungsrat. OZG-Umsetzung (Digitalisierung von Verwaltungsleistungen). 12. März 2019 unter https://www.it-planungsrat.de/beschluss/beschluss-2019-01 zuletzt abgerufen am 06. April 2022.

- 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 2019/14[99] ist dafür der Standard XProzess zu verwenden.

Abhängigkeiten

- AV-02 Standards, Methoden, Referenzarchitekturen und Interoperabilität

Implikationen

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

---

[99] IT-Planungsrat. XÖV-Standard für FIM: XProzess. 12. März 2019 unter https://www.it-planungsrat.de/beschluss/beschluss-2019-14 zuletzt abgerufen am 06. April 2022.

ID: V-9075-R02

GV-08 Daten-Governance

Die Daten-Governance **soll** ausgebaut werden.

Beschreibung

- 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.
- Die Daten-Governance soll Richtlinien, Regeln und einheitliche Standards festlegen, welche eine strukturierte Erhebung, Nutzung und Nachnutzung von Daten ermöglichen.
- Die Daten-Governance soll spezifische Rollen und Verantwortlichkeiten definieren, die sowohl ihre Einhaltung und Weiterentwicklung als auch die Steigerung der Datenkompetenz gewährleisten.
- Die Daten-Governance soll Verhaltensregeln, Prozesse und Best-Practice-Ansätze zum Umgang mit Daten aufstellen.

Begründung

- Der Ausbau der Daten-Governance ist ein wesentlicher Bestandteil zur Erreichung der in der Datenstrategie der Bundesregierung[100] beschriebenen Ziele 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 Act[101] 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 Daten
- FV-05 Information, Zeichen und Daten

Implikationen

[100] Die Bundesregierung. Datenstrategie der Bundesregierung. 27. Februar 2021 unter https://www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1; zuletzt abgerufen am 15. Februar 2022.

[101] Europäische Kommission. Vorschlag für den Data Governance Act. 25. November 2020 unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767; zuletzt abgerufen am 15. Februar 2022.

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

3.5 Funktionale Vorgaben

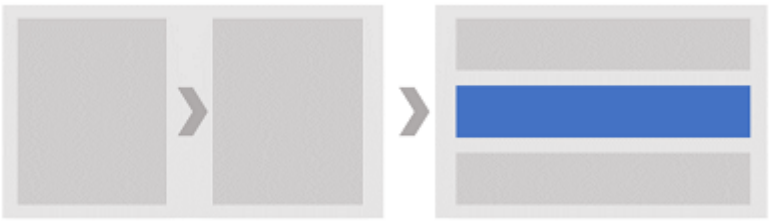

Abbildung 6: Folgende auf die Abbildung des Metamodells aus Kapitel 2.2 wird in dieser kleinen Abbildung die Funktionale Ebene hervorgehoben.

Dieses Kapitel beinhaltet Architekturvorgaben zur Nutzungs- und Leistungsverpflichtung von Diensten sowie allgemeine Vorgaben für Dienste. Ein Dienst ist hierbei eine logische Einheit, die einen definierten Umfang an Anforderungen erfüllt.

Die Nutzungsverpflichtung bezieht sich dabei insbesondere auf den funktionalen Umfang und die Leistungsverpflichtung auf das bereitgestellte Produkt. Allgemeine Architekturvorgaben definieren grundlegende Rahmenbedingungen und Prinzipien für Dienste und besitzen dabei eine Gültigkeit über die Grenzen eines Dienstes hinweg.

Architekturvorgaben zu Abhängigkeiten, Voraussetzungen und Qualität von Diensten ergeben sich aus den Domänenarchitekturen der Dienstekonsolidierung, welche über die allgemeine Vorgabe AV-02 zur Orientierung an Architekturen referenziert werden.

Architekturvorgaben zu Schnittstellen, Sicherheit und Standards von Diensten ergeben sich aus den Referenzarchitekturen der Dienstekonsolidierung, welche über die allgemeine Architekturvorgabe AV-02 zur Orientierung an Architekturen referenziert werden.

Die Architekturvorgaben für die Dienste wurden in einem ersten Schritt entlang der Funktionalitäten der Maßnahmenbeschreibungen des IT-Rahmenkonzeptes erstellt. In der Weiterentwicklung wurden die Architekturvorgaben für Dienste stärker auf das Dienstemodell angepasst. In der Architekturrichtlinie für die IT des Bundes 2020 wurde die redundanzfreie Verortung der Inhalte aus dem Anhang und der Nutzungs- und Leistungsverpflichtung aktualisiert sowie die Architekturvorgabe für Standardschnittstellen (DAAV-08) integriert. Mit der Architekturrichtlinie für die IT des Bundes 2021 ist eine weitere inhaltliche Überarbeitung der Architekturvorgaben für Dienste und ein kontinuierlicher Abgleich mit den weiteren Abschnitten des Dokumentes und der Anhänge vorgesehen.

Neben der Verfügbarkeit im NdB befindet sich die Bereitstellung bestimmter Dienste im Extranet/ in der Grundschutzzone derzeit in Planung.

ID: V-9019-R03

FV-01 Allgemeine Nutzungs- und Leistungsverpflichtung

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

Beschreibung

- Die Dienste der Dienstekonsolidierung (DK) sollen genutzt werden.
- Zur Nutzung der Dienste ist im IT-Rahmenkonzept des Bundes bereits folgende Regelung enthalten:
- „Das IT-Rahmenkonzept des Bundes ist das für alle Ressorts verbindliche Planungsinstrument für ressortübergreifende Vorhaben.
- In der Ressortplanung können keine Haushaltsmittel für die parallele Entwicklung etatisiert werden, die bereits durch ressortübergreifende IT-Maßnahmen im IT-Rahmenkonzept des Bundes abgedeckt sind.
- Für die Fortführung alternativer IT-Anwendungen dürfen Mittel nur veranschlagt werden, soweit dies wirtschaftlich ist.
- In der IT-Rahmenarchitektur des Bundes wird also die ressortübergreifend zu nutzende Basis- und Querschnitts-IT sowie zentrale IT-Infrastrukturen festgelegt.“[102]

Diese Regelung wird wie folgt weiter konkretisiert: - Die Dienste der DK sind durch IT-Maßnahmen des IT-Rahmenkonzeptes repräsentiert. - Die Wirtschaftlichkeit des Einsatzes eines Dienstes der DK für die Bundesverwaltung wird zentral durch die DK unter Beteiligung der Dienstleister nachgewiesen. - Die Nutzungsverpflichtung der Dienste der DK umfasst die gesamte unmittelbare Bundesverwaltung. - Der Nutzungsrahmen der Dienste der DK betrifft den jeweiligen Funktionsumfang im definierten Anwendungsbereich des Dienstes der DK gemäß den Dienstesteckbriefen im Anhang der Strategie Dienstekonsolidierung. - Die Verpflichtung zur Nutzung des Dienstes der DK tritt mit dem Zeitpunkt der Verfügbarkeit (Produktivsetzung) des Dienstes, ersichtlich aus dem Produktkatalog des Verbundes der IT-Dienstleister des Bundes, ein. - Mit der Eintragung eines Dienstes im Produktkatalog als produktiven Dienst besteht seitens der IT-Dienstleister eine Leistungsverpflichtung für die den Dienst realisierende IT-Lösung.

- Sowohl für produktive als auch für geplante Dienste der DK im definierten Funktionsumfang gemäß den Dienstesteckbriefen dürfen also abweichende Lösungen nicht mehr neu beschafft oder neu entwickelt werden.

[102] Rat der IT-Beauftragten. Rahmenarchitektur IT-Steuerung Bund. Beschlossen am 26. März 2009.

- Bestehende abweichende Lösungen derselben Funktionalität sind mit dem nächsten grundlegenden Versionswechsel durch die entsprechenden Dienste der DK zu prüfen und ggf. abzulösen.
- Sofern seitens der Maßnahme der DK keine zentrale Migrationsstrategie abgestimmt wird, sind entsprechende Migrationsstrategien, insbesondere bestehend aus der Machbarkeitsprüfung, der Zielsetzung und der groben zeitlichen, finanziellen sowie organisatorischen Abschätzung der Migration, frühzeitig, spätestens zum Ende des zwölften Monats nach der Produktivsetzung der Dienste der DK zu prüfen und ggf. zu erstellen.
- Für bereits produktive Dienste der DK sind die Migrationsstrategien bis spätestens zum Ende des zwölften Monats nach Verabschiedung des erneuerten Produktkataloges 2018 zu erstellen.

Begründung

- Die Nutzung gemeinsamer Basis-, Querschnitts- und Infrastrukturdienste dient der Harmonisierung und Konsolidierung der IT des Bundes. Weiterhin dürfen bei Basis-, Querschnitts- und Infrastrukturdiensten maximal zwei parallele IT-Lösungen entstehen.

Abhängigkeiten

- Keine

Implikationen

- Für alle Funktionen und Anwendungsbereiche, für die Basis-, Querschnitts- und Infrastrukturdienste der DK bereitgestellt werden, werden die evtl. vorhandenen eigenen Lösungen zukünftig abgelöst.
- Anwendungen und Dienste, die die entsprechenden Funktionen nutzen, werden entsprechend umgestellt.
- Der Rollout und die Umstellungen werden zwischen Behörde, DK und IT-Dienstleistern abgestimmt.
- 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.
- Die Behörden entscheiden anhand der fachlich-rechtlichen Vorgaben über die IT-technische Unterstützung (mit oder ohne IT).
- Insofern eine IT-technische Unterstützung erfolgen soll, sind die Vorgaben dieser Nutzungsverpflichtung für die Dienste der DK anzuwenden.
- Nutzende Behörden und IT-Dienstleister stimmen sich im Rahmen von Projekten und Aufträgen über die gegenseitige Nutzungs- und Leistungsverpflichtung ab.

- Für Behörden mit Bedarf zur Nutzung von geplanten oder angekündigten Diensten vor der Produktivsetzung werden durch die Maßnahmen der DK entsprechende Transitionspapiere (Zwischen-/ Übergangslösung; vgl. Strategie Dienstekonsolidierung) bereitgestellt.

ID: V-9025-R03

FV-02 Dienst- und Schnittstellenbeschreibungen

Dienste und Schnittstellen **müssen** standardisiert dokumentiert werden.

Beschreibung

- Die Dokumentation von Diensten muss spezifisch hinsichtlich Utility (Leistungsumfang), Warranty (Leistungsqualität) und den Service Design Aspekten (z. B. Organisation, technischer Aufbau) gestaltet sein, wobei auf vorhandenen Regelungen zur Dokumentation der DK aufzubauen ist (z. B. Dienstesteckbriefe, Domänen- und Referenzarchitekturen).
- Weiterhin müssen die durch einen Dienst angebotenen Schnittstellen hinsichtlich ihrer Ein- und Ausgabeparameter und ihres Verhaltens detailliert beschrieben sein.
- Es dürfen keine versteckten und undokumentierten administrativen Funktionen und erweiterten Schnittstellen vorgehalten werden.

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

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

ID: V-9026-R03

FV-04 Anwendungen für den Bundesclient

Neue Anwendungen **sollen** für die Nutzung über den Bundesclient entwickelt werden.

Beschreibung

- Neue Anwendungen sollen für die Nutzung über den Bundesclient konzipiert und realisiert werden.
- Die Beschaffung und Entwicklung von neuen Anwendungen orientiert sich an den durch die Maßnahme Bundesclient mit den Ressorts und Dienstleistern abgestimmten Empfehlungen zu Standards, Verfahren und Methoden für den Bundesclient.
- Für bestehende Lösungen und laufende Vorhaben, die den Bundesclient noch nicht berücksichtigen, ist die Möglichkeit einer Migrations- oder Ablösestrategie zu prüfen.

Begründung

- Der Nutzen eines zentralen Clients ist davon abhängig, ob die an einem Arbeitsplatz erforderlichen Dienste über diesen Client genutzt werden können.

Abhängigkeiten

- FV-01 Allgemeine Nutzungs- und Leistungsverpflichtung

Implikationen

- Neue Anwendungen sollen unter Berücksichtigung der Nutzbarkeit über den Bundesclient konzipiert werden.

ID: V-9040-R03

FV-05 Information, Zeichen und Daten

Der Datenaustausch **soll** mittels einheitlicher und quelloffener Formate erfolgen.

Zeichensätze und -kodierungen **sollen** standardisiert genutzt werden.

Metadaten **sollen** anhand einheitlicher Standards beschrieben werden.

Geodaten und Geodienste **sollen** standardisiert bearbeitet werden.

Das Datenmanagement **soll** den operativen Umgang mit Daten steuern.

Die öffentliche Bereitstellung von Daten **muss** gewährleistet werden.

Beschreibung

- Einheitliche und quelloffene Formate sollen für den Austausch von Daten und Informationen[103] verwendet werden.
- Für einheitliche und quelloffene Formate soll die uneingeschränkte und kostenfreie Nutzung als Mindestanforderung sichergestellt werden.
- Vor der Verwendung von Austauschformaten soll ihr kostenloser Erwerb oder ihr Erwerb gegen ein angemessenes Entgelt als Mindestanforderung sichergestellt werden.
- Es sollen standardisierte Zeichensätze und -kodierungen[104] verwendet werden.
- Zur Beschreibung von Metadaten sollen einheitliche Standards[105] verwendet werden.
- Bei der Bearbeitung von Daten, die einen räumlichen Bezug aufweisen (Geodaten), sollen einheitliche Standards im Geoinformationswesen[106] verwendet werden.
- Das Datenmanagement soll die operative Umsetzung einheitlicher Maßnahmen und Prozesse zur Erhebung, Analyse, Verarbeitung, Speicherung und Archivierung sowie Löschung von Daten gewährleisten.
- Das Datenmanagement soll die Nutzung von Daten in IT-Lösungen und Geschäftsprozessen sicherstellen.
- Das Datenmanagement soll durch die Einhaltung der FAIR-Prinzipien[107] nachhaltig gestaltet werden.
- Das Datenmanagement soll die Verknüpfung von Daten fördern (Linked Data).
- Die öffentliche Bereitstellung von Daten muss anhand § 12a – Gesetz zur Förderung der elektronischen Verwaltung erfolgen.
- Die öffentliche Bereitstellung von Daten muss sich an den zehn Kriterien zu Open Data der

[103] Technische Spezifikation der Architekturrichtlinie für die IT des Bundes. Abschnitt 2.2.5.

[104] Technische Spezifikationen der Architekturrichtlinie für die IT des Bundes. Abschnitt 2.3.1.

[105] Technische Spezifikationen der Architekturrichtlinie für die IT des Bundes. Abschnitt 2.3.2.

[106] Technische Spezifikationen der Architekturrichtlinie für die IT des Bundes. Abschnitt 2.2.5 und 2.3.6.

[107] Die FAIR-Prinzipien dienen einer nachhaltigen Nutzung von Daten. Nach den FAIR-Prinzipien sollen Daten auffindbar (Findable), zugänglich (Accessible), interoperabel (Interoperable) und wiederverwendbar (Reuseable) sein.

Sunlight-Foundation[108] orientieren.

Begründung

- Der Einsatz von einheitlichen Austauschformaten erleichtert die Kooperation der Bundesverwaltung.
- Damit geht eine höhere Effektivität in der Aufgabenerfüllung der Behörden einher.
- Der Einsatz von standardisierten Zeichensätzen und -kodierungen erleichtert die Kooperation der Bundesverwaltung, 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).
- Das Architekturkonzept der GDI-DE stellt insbesondere unter Beachtung der gesetzlichen Pflichten[109] 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 nach der Datenstrategie der Bundesregierung die Verwendbarkeit der Daten und fördert unter anderem die Möglichkeit des Einsatzes im Rahmen von Anwendungen der Künstlichen Intelligenz.

[108] Englisches Original: Sunlight-Foundation. „TEN PRINCIPLES FOR OPENING UP GOVERNMENT INFORMATION". 2007 unter https://sunlightfoundation.com/policy/documents/ten-open-data-principles/; zuletzt abgerufen am 24. Februar 2022; Deutsche Übersetzung nach BMI: BMI. „Die zehn Open-Data-Kriterien der Sunlight-Foundation". 2014 unter https://www.govdata.de/documents/10156/18448/GovData_Open-Data-Kriterien_der_Sunlight_Foundation.pdf/dca8fea0-8e04-4de0-8531-2bc3e8d4abc0; zuletzt abgerufen am 24. Februar 2022.

[109] Technische Spezifikationen der Architekturrichtlinie für die IT des Bundes. Abschnitt 2.2.5.

- Open Data fördert ein offenes Regierungs- und Verwaltungshandeln und stärkt die Ziele aus der Open-Data-Strategie der Bundesregierung[110], der europäischen Datenstrategie[111] und der Datenstrategie der Bundesregierung[112] wie z. B. der Aufbau eines gemeinsamen Daten-Ökosystems, die verstärkte Datennachnutzung, die Innovationsförderung und die Stärkung des Wirtschaftsstandorts Deutschland.
- Das E-Government-Gesetz[113], einschließlich des zweiten Open-Data-Gesetzes[114] und Datennutzungsgesetz[115], bildet 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 Datenstrategie[116], indem die Daten in das Europäische Metadatenportal (EDP) überführt werden.

Abhängigkeiten

- AV-04 Daten
- AV-09 Souveränität, Unabhängigkeit
- TV-05 Datenbanksysteme
- GV-08 Daten-Governance

Implikationen

- Für die Umsetzung der Vorgabe ist die regelmäßige Prüfung der Mindestanforderungen von genutzten Austauschformaten zu berücksichtigen.
- Für eine Nutzung von Geodaten und Geodatendiensten sind u. U. Änderungen bei den Einstellungen in Grundanwendungen wie z. B. im Browser notwendig.

---

[110] Die Bundesregierung. Open-Data-Strategie der Bundesregierung. 07.07.2021 unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/moderne-verwaltung/open-data-strategie-der-bundesregierung.pdf;jsessionid=3DFE0546973DE6006176A934F2A56C76.2_cid364?__blob=publicationFile&v=4; zuletzt abgerufen am 21. Februar 2022.

[111] Europäische Kommission. „Eine europäische Datenstrategie". Unter https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de; zuletzt abgerufen am 25. Februar 2022.

[112] Die Bundesregierung. Datenstrategie der Bundesregierung. 27. Februar 2021 unter https://www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1; zuletzt abgerufen am 21. Februar 2022.

[113] BJM. E-Government-Gesetz. Unter http://www.gesetze-im-internet.de/egovg/EGovG.pdf; zuletzt abgerufen am 21. Februar 2022.

[114] Zweites-Open-Data-Gesetz. 10. Februar 2021 unter https://www.bmi.bund.de/SharedDocs/downloads/DE/gesetzestexte/gesetzesentwuerfe/zweites-open-data-gesetz.pdf?__blob=publicationFile&v=2; zuletzt abgerufen am 21. Februar 2022.

[115] BMJ. Datennutzungsgesetz. 23. Juli 2021 unter https://www.gesetze-im-internet.de/dng/DNG.pdf; zuletzt abgerufen am 21. Februar 2022.

[116] Europäische Kommission. Eine europäische Datenstrategie. 19. Februar 2020 unter https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066; zuletzt abgerufen 21. Februar 2022.

- Eine Nichtumsetzung der verbindlichen Vorgaben aus den europäischen INSPIRE-Regelungen kann zu einem Vertragsverletzungsverfahren seitens der Europäischen Kommission gegenüber der Bundesrepublik Deutschland führen.
- Die bei der Umsetzung gemachten Erfahrungen sind bei der Weiterentwicklung der Regelungen zu beachten.
- Es ist zu beachten, dass schutzbedürftige Daten entsprechend ihres Schutzbedarfs veröffentlicht werden.
- Es ist zu beachten, dass keine personenbezogenen Daten für einen unberechtigten Empfängerkreis veröffentlicht werden.
- Die Einführung und Befolgung von funktionalen und organisatorischen Strukturen und Prozessen zur öffentlichen Bereitstellung von Daten sind wichtige Bausteine zur Einhaltung der Vorgabe.
- Die öffentliche Bereitstellung der Daten sollte bereits bei der Datenerhebung mit dem „Open by default“-Prinzip beachtet werden.

ID: V-9028-R04

FV-08 Identitätsinformation, Zugriffssteuerung, Sicherheitskonzeption, Schutzbedarf, Quality of Service, Security by Design, Separierung und Mandantentrennung

Identitätsinformationen **müssen** mittels standardisierter Schnittstellen verwaltet werden.

Die Zugriffssteuerung **muss** sichergestellt werden.

Sicherheitskonzepte **müssen** für alle IT-Verfahren erstellt und umgesetzt werden.

Der Schutzbedarf und Quality of Service **müssen** gewährleistet werden.

Die Sicherheit von IT-Verfahren und Produkten **soll** schon während der Entwicklungsphase berücksichtigt werden.

Die Separierung und Mandantentrennung sollen beim Betrieb von IT-Verfahren berücksichtigt werden.

Beschreibung

- Eine Schnittstelle von anderen Diensten mit eigenen identitätsbeschreibenden Attributen oder Berechtigungsrichtlinien an den Dienst „Ressortübergreifendes Identitätsmanagement für die Bundesverwaltung“ muss in der gesamten unmittelbaren Bundesverwaltung gemäß Architekturvorgabe FV-01 berücksichtigt werden.
- Sofern neu entwickelte und ressortübergreifend genutzte Dienste der Bundesverwaltung eigene identitätsbeschreibende Attribute (Rollenzuordnungen, etc.) oder Berechtigungsrichtlinien (Access Control Policies) vorhalten, müssen diese über dedizierte Schnittstellen auch durch externe Dienste abgefragt werden können.
- Jeder Zugriff auf eine Ressource muss durch das Access Management geschützt sein.
- Es darf auch für die Administrierenden keine Möglichkeit geben, am Access Management vorbei auf eine Ressource zuzugreifen.
- Für alle betriebenen IT-Verfahren muss vor der Inbetriebnahme ein gültiges Informationssicherheitskonzept gemäß BSI-Standards für IT-Grundschutz in der jeweils gültigen Fassung vorliegen, umgesetzt und dokumentiert sein.
- Das Informationssicherheitskonzept muss regelmäßig durch Revisionen bzw. Audits auf Wirksamkeit, Angemessenheit und Aktualität der eingesetzten Maßnahmen hin überprüft werden.
- Der Übergang von den BSI-Standards 100-1[117] bis 100-3[118] auf die neuen BSI-Standards muss gewährleistet werden.
- Bei Anwendung des modernisierten Grundschutzes muss die Standardabsicherung als Mindestanforderung angewendet werden.
- Schutzbedarf und Quality of Service von IT-Verfahren müssen festgelegt, regelmäßig überprüft

[117] BSI. BSI-Standard 100-1: Information Security Management Systems. 2008 unter https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf;jsessionid=054D90B160516FB6301217C7D2233C30.internet481?__blob=publicationFile&v=1; zuletzt abgerufen am 06. April 2022.

[118] BSI. BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz. 2008 unter https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf;jsessionid=306BBAED50DD5DA08035915DB2D74E22.internet481?__blob=publicationFile&v=1; zuletzt abgerufen am 06. April 2022.

und gewährleistet werden.
- Alle IT-Verfahren der Bundesverwaltung sollen sicher und robust gestaltet werden.
- Beim Betrieb von IT-Verfahren für unterschiedliche Nutzerbehörden in einer zusammenhängenden – insbesondere virtualisierten – IT-Umgebung sollen die Grundsätze der Separierung/ Mandantentrennung beachtet werden.
- Gemäß BSI-Standard 200-2[119] muss bei einem hohen Schutzbedarf durch eine Risikoanalyse festgelegt werden, ob eine logische Separierung/ Mandantentrennung ausreichend und wie diese gegebenenfalls umzusetzen ist.
- An der Entscheidungsfindung soll das BSI beteiligt werden.
- Es gelten die einschlägigen Cyber-Sicherheits-Empfehlungen des BSI als Empfehlung[120].
- Zudem ist der IT-Grundschutz-Baustein NET.1. für „Netzarchitektur und -design", insbesondere hinsichtlich der Anforderungen zu physikalischer und logischer Separierung zu beachten.
- Zusätzliche Hinweise finden sich in den Veröffentlichungen der ISi-Reihe des BSI zum Thema „Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)".

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.

Abhängigkeiten

- AV-08 Informationssicherheit, Datenschutz, Geheimschutz und Systemgrundkonfigutration

Implikationen

[119] BSI. BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise. 08. Mai 2008 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.html; zuletzt abgerufen am 06. April 2022.

[120] BSI. Informationen und Empfehlungen. Unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/informationen-und-empfehlungen_node.html; zuletzt abgerufen am 06. April 2022.

- Die Etablierung zentraler Sicherheitsdienste, welche durch Querschnittsdienste genutzt werden, stellt besondere Anforderungen an deren Sicherheit, Performance und Verfügbarkeit.
- 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.
- Entsprechende Prozesse und Maßnahmen sind bezogen auf die Einführung zu definieren (z. B. Penetration Testing der Anwendung oder Code Reviews).
- Hier muss sehr genau geprüft werden, welche Anforderungen bei der Konzeption, Umsetzung 1631 und dem Betrieb der Lösung berücksichtigt werden müssen.
- Ein Informationssicherheitskonzept unterstützt das Compliance-Management von IT-Verfahren.
- Die Festlegung von Schutzbedarf und Quality of Service ist maßgeblich für die zu ergreifenden IT-Sicherheitsvorkehrungen bei der Entwicklung und Implementierung von IT-Verfahren[121].
- Aspekte der Informationssicherheit sind bereits beim Entwurf von IT-Verfahren zu berücksichtigen. U. a. sind die Implikationen aus dem Anhang „Technische Spezifikationen zur Architekturrichtlinie“[122] zu beachten.
- Bei übergreifend konzipierten IT-Verfahren ist bereits zum Zeitpunkt der Konzeption eine Separierung/ Mandantentrennung nach Anforderungen der Nutzerbehörde zu berücksichtigen.

---

[121] BSI. BSI-Standard 200-1. Januar 2021 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf?__blob=publicationFile&v=2; zuletzt abgerufen am 18. März 2022. BSI. BSI-Standard 200-2. 15. November 2017 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2;%20zuletzt%20abgerufen%20am%2018.%20M%C3%A4rz%202022; zuletzt abgerufen am 24. März 2022. BSI. BSI-Standard 200-3. 15. November 2017 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2;%20zuletzt%20abgerufen%20am%2018.%20M%C3%A4rz%202022; zuletzt abgerufen am 24. März 2022.

[122] Technische Spezifikationen der Architekturrichtlinie für die IT des Bundes. Abschnitt 2.1.

ID: V-9024-R03

FV-09 Entkopplung

Die lose Kopplung von Diensten **soll** durch die Nutzung von Standards und Datenmodellen optimiert werden.
Die Fach-, Querschnitts-, und Basisdienste **sollen** vom Bundesclient entkoppelt werden.

Beschreibung

- Zur Optimierung der losen Koppelung von Diensten sollen offene Standards und übergreifend abgestimmte Datenmodelle eingesetzt werden.
- Weiterhin sollen die Abhängigkeiten zwischen Diensten minimiert werden.
- Fach-, Querschnitts- und Basisdienste sollen vom Bundesclient entkoppelt sein. Entkoppelt bedeutet in diesem Zusammenhang, dass Fach-, Querschnitts- und Basisdienste keine zwingenden Abhängigkeiten zu
  - spezifischen Laufzeitumgebungen oder
  - Software-Komponenten des Bundesclients haben sollen.
- Die Bereitstellung von Diensten soll serverbasiert erfolgen. Der Zugriff und die Nutzung von Fach-, Querschnitts- und Basisdiensten sollte über den Webbrowser erfolgen.
- Eine clientseitige Bereitstellung von Integrationspunkten an standardisierte Schnittstellen kann im Einzelfall erfolgen. Bei der Bereitstellung von Integrationspunkten ist die clientseitige Programmlogik möglichst klein zu halten und der Weiterentwicklungsbedarf bei Änderungen des Bundesclients zu planen und zu budgetieren.
- Diese Anforderung gilt für alle Dienste unabhängig von der tatsächlichen oder geplanten Nutzung des Bundesclients, die weiterentwickelt oder neu erstellt werden.

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.
- Der Bundesclient kann nur dann eine weitgehend einheitliche Basis für die unmittelbare Bundesverwaltung darstellen, wenn die Abhängigkeiten zu Diensten für den Bundesclient reduziert und perspektivisch möglichst ganz abgebaut werden.
- Damit werden Effizienz- und Standardisierungsvorteile realisiert.

Abhängigkeiten

- AV-10 Kopplung, Komplexität, Modularität, Wiederverwendbarkeit und Cloud Computing

Implikationen

- Die Vorgabe soll beim Entwurf, der Entwicklung und der Bereitstellung von Diensten berücksichtigt werden, wobei ein übergreifendes Schnittstellenmanagement unterstützend zu etablieren ist.
- Entwicklungs- und Beschaffungsvorhaben müssen sich an den Schnittstellen des Bundesclients und den verfügbaren Diensten orientieren.
- Insbesondere müssen die Richtlinien des Bundesclients und der Dienste bei der Entwicklung berücksichtigt werden.

3.6 Technische Vorgaben

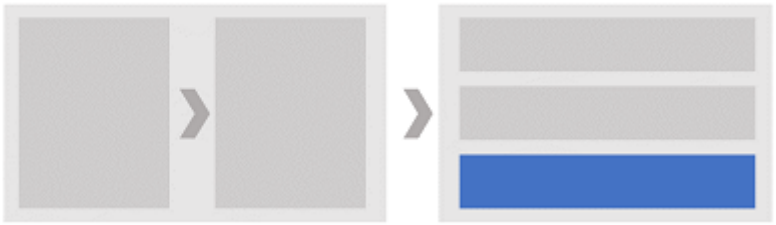

Abbildung 7: Folgende auf die Abbildung des Metamodells aus Kapitel 2.2 wird in dieser kleinen Abbildung die technische Ebene hervorgehoben.

Die technischen Vorgaben beziehen sich auf die technologische Umsetzung der IT-Architektur. Sie beinhalten prinzipielle Vorgaben für die Anwendungsentwicklung, wie beispielsweise die Nutzung von Programmiersprachen. Weiterhin werden durch die Vorgaben Infrastrukturaspekte geregelt. Die in diesem Kapitel aufgeführten Vorgaben sind für die Entwicklung von Fachverfahren relevant.

ID: V-9034-R03

TV-01 Entwicklung, Programmiersprachen und Qualitätsmanagement

Die cloudbasierte Entwicklung **soll** in einer standardisierten Umgebung erfolgen.
Bei der serverseitigen Anwendungsentwicklung **sollen** standardisierte Programmiersprachen und Entwicklungsumgebungen verwendet werden.
Das Qualitätsmanagement **muss** bei der Anwendungsentwicklung standardisiert erfolgen.

Beschreibung

- Die cloudbasierte Entwicklung von IT-Lösungen soll in einer standardisierten Umgebung[123] erfolgen.
- Die Cloud-Entwicklungsumgebung soll quelloffene Entwicklungswerkzeuge mit adäquatem Support (Programme, Frameworks, Bibliotheken) verwenden.
- Die Bereitstellung von cloudbasierten IT-Lösungen soll über einen standardisierten Prozess erfolgen (Continuous Delivery, Continuous Deployment).
- Alle (serverseitigen) Anwendungsentwicklungen sollen unter Verwendung standardisierter Programmiersprachen sowie Entwicklungs- und Laufzeitumgebungen[124] durchgeführt werden.
- Für die Anwendungsentwicklung sollen quelloffene Entwicklungswerkzeuge mit adäquatem Support (Programme, Frameworks, Bibliotheken) verwendet werden.
- Alle Anwendungen und Anwendungsentwicklungen müssen einem standardisierten Prozess des Qualitätsmanagements unterliegen.
- Insbesondere die Versionierung und Dokumentation von Quellcode und Artefakten, kontinuierliche Integration, statische Codeanalyse, (automatisierte) Softwaretests, Lasttests, Vulnerabilty Scans von eingesetzten Komponenten und kollaboratives Wissensmanagement sind durchzuführen.

Begründung

- 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.

[123] Technische Spezifikationen der Architekturrichtlinie für die IT des Bundes. Abschnitt 2.1.3.

[124] Technische Spezifikationen der Architekturrichtlinie für die IT des Bundes. Abschnitt 2.1.4.

- 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-10 Kopplung, Komplexität, Modularität, Wiederverwendbarkeit und Cloud Computing
- TV-10 Betrieb

Implikationen

- Die Standardkataloge mit den Empfehlungen der IT-Dienstleister zu offenen Elementen, Entwicklungswerkzeugen, Bibliotheken und Standards sind über den Leistungsverbund zu beziehen.
- Die IT-Dienstleister des Bundes stellen in deren Standardkatalogen Empfehlungen von offenen Elementen, Entwicklungswerkzeugen, Bibliotheken und Standards vor. Die Kataloge sind bei den IT-Dienstleistern über den Leistungsverbund zu beziehen.

ID: V-9071-R03

TV-02 Schnittstellen

Standardschnittstellen und -APIs **sollen** genutzt werden.

Schnittstellen und Protokollformate **müssen** standardisiert zugänglich gemacht und genutzt werden.

Beschreibung

- Für die Verbindung mehrerer Dienste oder IT-Lösungen sollen wenige Schnittstellen und APIs auf Basis offener Standards (fachlich und technisch) genutzt werden.

- Die verwendeten Schnittstellen und -APIs inklusive etwaiger Abweichungen (alternative individuelle Schnittstellen) sowie die dafür verwendeten offenen Standards müssen in den Architekturen dokumentiert werden.
- Es müssen Schnittstellen vorgesehen werden, über die dem BSI Schnittstellen- und Protokolldaten (§ 5 BSIG)[125] der IT-Verfahren in standardisierter Form zugänglich gemacht werden können.

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.
- Zur sicheren Gestaltung von E-Government-Dienstleistungen hat das BSI entsprechende Schnittstellen- und Protokolldaten nach § 5 BSIG zu analysieren.

Abhängigkeiten

- AV-02 Standards, Methoden, Referenzarchitekturen und Interoperabilität
- AV-08 Informationssicherheit, Datenschutz, Geheimschutz und Systemgrundkonfiguration
- AV-09 Souveränität, Unabhängigkeit
- AV-10 Kopplung, Komplexität, Modularität, Wiederverwendbarkeit und Cloud Computing

[125] BSI. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) § 8 Vorgaben des Bundesamtes. 20. August 2009 unter https://www.gesetze-im-internet.de/bsig_2009/__5.html; zuletzt abgerufen am 23. Mai 2022.

Implikationen

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

ID: V-9032-R03

TV-05 Datenbanksysteme

Datenbanken **sollen** standardisiert betrieben werden.

Beschreibung

- Relationale und nichtrelationale Datenbanksysteme (DBS) sollen auf Basis definierter Technologien[126] betrieben werden.

Begründung

- Die Standardisierung ermöglicht eine Vereinfachung der Programmierung durch einheitliche Sprache und Reduzierung des Schulungsaufwandes sowie bessere Portierbarkeit bei einem Wechsel des DBS.

Abhängigkeiten

- AV-04 Daten
- TV-02 Schnittstellen

Implikationen

- Keine

---

[126] Technische Spezifikationen der Architekturrichtlinie für die IT des Bundes. Abschnitt 2.1.4.

ID: V-9047-R03

TV-08 Kryptografie, sicherheitsrelevante Ereignisse und Schadprogrammabwehr

Kryptografische Verfahren **müssen** für alle IT-Verfahren eingesetzt werden.

Sicherheitsrelevante Ereignisse **müssen** für alle IT-Verfahren protokolliert, überwacht und detektiert werden.

Die Schadprogrammabwehr **muss** sichergestellt werden.

Beschreibung

- Es müssen für alle IT-Verfahren auf Grundlage des festgestellten Schutzbedarfs die aktuell zugelassenen kryptografischen Verfahren nach dem Stand der Technik eingesetzt werden.
- Zu berücksichtigen sind hierzu die Technischen Richtlinien TR-02102 (Kryptografische Verfahren: Empfehlungen und Schlüssellängen, Teile 1-4) und TR-03116 (Kryptografische Vorgaben für Projekte der Bundesregierung, Teile 1-6) des BSI.
- Beim Einsatz von Transport Layer Security (TLS) ist der Mindeststandard des BSI zur Verwendung von Transport Layer Security zu beachten.
- Für den Bereich des BMVg sind – abhängig vom Anwendungsfall – ggf. NATO- oder EU-Vorschriften zu beachten.
- Für IT-Verfahren ist eine Verschlüsselung auch nach der DSGVO und der VSA vorgeschrieben.
- Für alle IT-Verfahren muss von der verantwortlichen Behörde eine auf das Verfahren zugeschnittene Richtlinie für die Protokollierung von Ereignissen, insbesondere zur Detektion von Cyber-Angriffen, gemäß Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen[127] erstellt und umgesetzt werden.
- In diesem Zusammenhang gelten auch die jeweils aktuelle Version der Protokollierungsrichtlinie des Bundes und der Grundschutzbausteine OPS.1.1.5 „Protokollierung“ und DER.1 „Detektion von sicherheitsrelevanten Ereignissen“.
- Für alle IT-Verfahren müssen Virenschutz- und Schadprogrammabwehrleistungen nach dem aktuellen Stand der Technik genutzt werden.
- Zu berücksichtigen sind die Vorgaben gemäß § 8 BSIG[128], die Anforderungen aus dem IT-Grundschutz-Baustein OPS.1.1.4 „Schutz vor Schadprogrammen“[129] und weitere Empfehlungen des BSI sowie der angebotenen Dienste von NdB.

Begründung

[127] BSI. Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen. Unter https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/PDCA/PDCA_node.html; zuletzt abgerufen am 06. April 2022.

[128] Gesetze im Internet. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG). 14. August 2009 unter https://www.gesetze-im-internet.de/bsig_2009/__8.html; zuletzt abgerufen am 06. April 2022.

[129] BSI. OPS.1.1.4: Schutz vor Schadprogrammen (Edition 2021). 01. Februar 2021 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_1_4_Schutz_vor_Schadprogrammen_Edition_2021.html; zuletzt abgerufen am 06. April 2022.

- 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

- AV-08 Informationssicherheit, Datenschutz, Geheimschutz und Systemgrundkonfiguration

Implikationen

- Die für IT-Verfahren umgesetzten kryptographischen Verfahren sind stets unter Beachtung der Technischen Richtlinien des BSI auf dem aktuellen Stand der Technik zu halten.
- Die Konzeption muss turnusmäßig überprüft werden.
- Bereits bei der Konzeption von IT-Verfahren ist ein Protokollierungskonzept zu erstellen und im Weiteren zu berücksichtigen.
- Die Meldepflichten gemäß § 4 Abs. 6 BSIG i. V. m. der AVV zum BSIG sind zu beachten.
- Um dem nachzukommen, ist ein Prozess für ein Sicherheitsvorfallmanagement zu etablieren.
- 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-R04

TV-09 Kommunikationsverbindungen und Netzwerkprotokoll

Die zentral bereitgestellten Kommunikationsverbindungen **sollen** genutzt werden.
IPv6 **muss** als Netzwerkprotokoll verwendet werden.

Beschreibung

- Nutzende sollen die von NdB zentral bereitgestellten und gesicherten Kommunikationsverbindungen und Netzübergänge zu Fremdnetzen verwenden, sodass keine anderen (lokalen) Netzanschlüsse erforderlich werden. Folgende Kommunikationsverbindungen werden durch NdB über die Anschlussarten NdB A1 bis A5 angeboten und sollen bei der Planung durch die jeweilige Behörde berücksichtigt werden:
  - Zugriff auf zentrale Fachverfahren im Intranet des Bundes, die durch das ITZBund als zentralem IT-Dienstleister des Bundes bereitgestellt werden
  - Zugriff auf Dienste und Fachverfahren in anderen IT-Verwaltungsnetzen (NdB-VN, TestaNG usw.)
  - Bereitstellung von verschlüsselten LAN-Kopplungen zu weiteren Liegenschaften von Nutzenden (unter Berücksichtigung der Dienstesegmentierung)
  - Bereitstellung eines zentral abgesicherten Internetanschlusses für den Zugriff auf das Internet
  - Bereitstellung von leistungsfähigen Internetzugängen für eigene Internetdienste
  - Zugriff auf zentrale Dienste (z. B. E-Mail, De-Mail, PKI, X500) und Fachverfahren im Intranet des Bundes
  - Einwahl über BSI zugelassene mobile Zugänge
  - Einwahl von verwaltungsexternem Personal für Fernwartungstätigkeiten (sofern eine zentrale Fernwartungsplattform verfügbar ist)
- Alternativ Zugriff auf das NdB-Extranet/ Grundschutzzone mit Schutzbedarf „Normal“ und ohne Zugriff auf Inhalte bzw. Verfahren, die VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft sind.
- Wenn eine erforderliche Zugriffsmöglichkeit nicht über zentrale Netzübergänge bereitgestellt werden kann, wird diese unter Beachtung der Vorgaben des BSI dezentral durch den Betreiber des Nutzer-LAN bereitgestellt.
- IT-Systeme, Verfahren und Infrastrukturen müssen mit IPv6, und damit ohne IPv4 Adressen, vollständig funktionsfähig sein.
- Dies gilt für Neubeschaffungen, insbesondere im Rahmen einer Konsolidierung. Bestehende Systeme müssen im Rahmen der Systempflege/ Wartung IPv6-fähig gemacht werden. Die durch

die KoITB und den IT-Rat vorgegebenen Zeitlinien müssen eingehalten werden[130]. Folgende Richtlinien sind einzuhalten:

  - „IPv6 Referenzhandbuch der öffentlichen Verwaltung“ (Organisationshandbuch; V 1.0 v. März 2011, Beschluss IT-Planungsrat)
  - „IPv6 Routingkonzept der öffentlichen Verwaltung“ (V 1.0 v. August 2016, Beschluss IT-Planungsrat)
  - „DNS Konzept für die öffentliche Verwaltung“ (in Erarbeitung, BMI CI5) Zu beachten (als Empfehlungen) sind weiterhin:
  - „IPv6 Profile für die öffentliche Verwaltung“ (Beschaffungsgrundlage; V 1.1 v. Dezember 2013, BVA)
  - „IPv6 Migrationsleitfaden für die öffentliche Verwaltung“ (V 1.1 v. Dezember 2013, BVA)

- Für den Einsatz und die Einführung von IPv6 in der öffentlichen Verwaltung stehen (BSI-) abgestimmte Leitfäden, Beschaffungsrichtlinien sowie Einsatzkonzepte zur freien Verfügung.[131]

Begründung

- Die Bereitstellung/ Nutzung der NdB-Kommunikationsverbindungen ist erforderlich, um ein einheitliches, hohes Sicherheitsniveau für die NdB-Anschlüsse (NdB A1 bis A5) sicherzustellen.
- Dadurch wird die Verfügbarkeit/ Vertraulichkeit/ Integrität jeder einzelnen Nutzerin und jedes einzelnen Nutzers geschützt und ein sicherer NdB-interner Austausch von Informationen bis zum Geheimhaltungsgrad „VS-NUR FÜR DEN DIENSTGEBRAUCH“ ermöglicht.
- 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

[130] KoITB. Beschluss der Konferenz der IT-Beauftragten der Ressorts vom 11. November 2020. 2020 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 09. Januar 2024.

[131] BDBOS. Local Internet Registy. 2019 unter https://www.bdbos.bund.de/DE/Aufgaben/LIRdeGovernment/lirdegovernment_node.html zuletzt abgerufen am 10. Januar 2024.

- Unter Berücksichtigung des Schutzbedarfes der verarbeiteten Informationen und der Netzwerkinfrastruktur soll eine entsprechende Segmentierung der lokalen Netze der Nutzenden realisiert werden.

- Für NdB-Anschlüsse (NdB VS-NfD) und/ oder NdB-Extranet/ Grundschutzzone sind die jeweiligen vom BSI veröffentlichten Nutzerpflichten sowie die VSA zu beachten.

- Unter Berücksichtigung der von NdB angebotenen Kommunikationsverbindungen soll eine für die jeweilige Behörde geeignete LAN-Architektur entwickelt werden, in der das NdB-Nutzernetz implementiert wird.

- Die entsprechenden Kommunikationsverbindungen und Netzanschlüsse werden an den Anforderungen der IT-Konsolidierung des Bundes ausgerichtet, sodass für die IT-Konsolidierung benötigte Bandbreiten und eine ausreichende Netzqualität (Quality of Service), d. h. eine Priorisierung von Verkehrsklassen, zur Verfügung stehen.

- 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.[132] 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

[132] BDBOS. Local Internet Registy. 2019 unter https://www.bdbos.bund.de/DE/Aufgaben/LIRdeGovernment/lirdegovernment_node.html zuletzt abgerufen am 10. Januar 2024.

- IT-Softwarekomponenten (insbesondere Einzelentwicklungen – Fachverfahren für Behörden)

ID: V-9078-R02

TV-10 Betrieb

Die Betriebsumgebungen des Cloud Computing **müssen** kompatibel sein.

Der Betrieb von Hostrechnern **soll** standardisiert erfolgen.

Der Betrieb von Servern und Laufzeitumgebungen **soll** standardisiert erfolgen.

Die Sicherheit des Cloud Computing **muss** gewährleistet werden.

Beschreibung

- Die Betriebsumgebungen des Cloud Computing müssen die Kriterien des IT-Rats Beschlusses Nr. 2015/5[133] für die Nutzung von Cloud-Diensten der IT-Wirtschaft durch die Bundesverwaltung einhalten (u.a. Inhouse First [2], Vermeidung Lock-In [3c], Kauf First [3g]).
- Die Betriebsumgebungen für konsolidierungsrelevante IT-Lösungen und Verfahren in der unmittelbaren Bundesverwaltung müssen die Vorgaben für die Bundescloud berücksichtigen.
- Die Betriebsumgebungen des Cloud Computing sollen die unter 5.2 angeführten Standards der Deutschen Verwaltungscloud-Strategie (DVS)[134] einhalten.
- Die Betriebsumgebungen des Cloud Computing sollen die Kompatibilität mit dem Gaia-X Framework gewährleisten und die dort aufgeführten Standards zu Cloud Service Provider und Data Sharing within data spaces[135] einhalten.
- Für Hostrechner im Backend-Bereich sollen standardisierte Prozessorarchitekturen und Serverbetriebssysteme[136] genutzt werden.
- Um den Betrieb der Fachverfahren so einfach, wartbar, migrierbar und zukunftssicher wie möglich zu machen, sollen Server und Laufzeitumgebungen mit einheitlichen Technologien[137] verwendet werden.
- Für den sicheren Einsatz von Cloud Computing müssen die Kriterien 3.a., 3.b., 3.f., 3.h., 3.i. und 3.j. des IT-Rats Beschluss Nr. 2015/5[138] für die Nutzung von Cloud-Diensten der IT-Wirtschaft durch die Bundesverwaltung eingehalten werden.
- Für den sicheren Einsatz von Cloud Computing müssen die Basis- und Standardanforderungen des Prozess-Bausteins OPS.2.2: Cloud-Nutzung des BSI IT-Grundschutz-Kompendiums[139] in

[133] CIO Bund. Kriterien für die Nutzung von Cloud-Diensten der IT-Wirtschaft. 29. Juli 2015 unter https://www.cio.bund.de/Web/DE/Politische-Aufgaben/IT-Rat/Beschluesse/Tabelleninhalte/beschluss_2015_05.html zuletzt abgerufen am 22. Februar 2022.

[134] IT-Planungsrat. Deutsche Verwaltungscloud-Strategie: Rahmenwerk der Zielarchitektur. August 2021 unter https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-46_Deutsche_Verwaltungscloud-Strategie_AL1.pdf zuletzt abgerufen am 15. Februar 2022.

[135] Gaia-X. Policy Rules Document. 21. November 2021 unter https://gaia-x.eu/sites/default/files/2022-01/Policy_Rules_Document_21.11.pdf zuletzt abgerufen am 28. Februar 2022.

[136] Technische Spezifikation der Architekturrichtlinie für die IT des Bundes. Abschnitt 2.1.12 (Perspektivisch soll eine Referenzarchitektur zur Infrastruktur definiert werden).

[137] Technische Spezifikation der Architekturrichtlinie für die IT des Bundes. Abschnitt 2.1.2.

[138] CIO Bund. Kriterien für die Nutzung von Cloud-Diensten der IT-Wirtschaft. 29. Juli 2015 unter https://www.cio.bund.de/Web/DE/Politische-Aufgaben/IT-Rat/Beschluesse/Tabelleninhalte/beschluss_2015_05.html; zuletzt abgerufen am 22. Februar 2022.

[139] BSI. IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit. 2022 unter www.bsi.bund.de/.../IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html; zuletzt abgerufen am 22. Februar 2022.

der jeweils gültigen Fassung eingehalten werden.
- Für den sicheren Einsatz von Cloud Computing müssen Mindeststandards, hier insbesondere der Mindeststandard des BSI zur Nutzung externer Cloud[140]-Dienste sowie die Indikatoren des HV-Benchmark kompakt 4.0[141], eingehalten werden.

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.
- 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.

Abhängigkeiten

- AV-10 Kopplung, Komplexität, Modularität, Wiederverwendbarkeit und Cloud Computing
- AV-08 Informationssicherheit, Datenschutz, Geheimschutz und Systemgrundkonfiguration
- TV-01 Entwicklung, Programmiersprachen und Qualitätsmanagement

Implikationen

[140] BSI. Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG zur Nutzung externer Cloud-Dienste in der Bundesverwaltung. 15. Dezember 2022 unter https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html; zuletzt abgerufen am 10. Januar 2024.

[141] BSI. Mindeststandard des BSI für die Anwendung des HV-Benchmark kompakt. Juli 2018 unter https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/HV-Benchmark-kompakt/HV-Benchmark-kompakt_node.html; zuletzt abgerufen am 12.04.2022.

- Bereits vor der Inbetriebnahme sind die benannten Kriterien, Anforderungen und Standards zu überprüfen.
- Vor einer Beauftragung ist festzulegen, auf welcher Betriebsumgebung und mit welchen damit verbundenen Standards und Referenzen die IT-Lösungen und Verfahren betrieben werden.
- Bei der Bereitstellung konsolidierungsrelevanter IT-Lösungen und Verfahren ist der Betrieb auf der Bundescloud inklusive der IT-Betriebsplattform Bund zu prüfen.
- Beschaffte IT-Lösungen müssen mit der Prozessorarchitektur sowie dem Serverbetriebssystem kompatibel sein.
- Ergänzend zu den Verpflichtungen des Cloud-Anbieters ist auch der Cloud-Nutzer für den sicheren Einsatz der Cloud mitverantwortlich (shared responsibility).
- 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.
- Das Cloud Computing ist im Informationssicherheitsmanagement (ISM) des Cloud-Nutzers zu berücksichtigen.

4 Nutzung von Architekturvorgaben

In diesem Kapitel werden grundlegende Prämissen zur Nutzung und Mechanismen zur Sicherstellung der Einhaltung der Architekturvorgaben definiert.

4.1 Weiterentwicklung und Einhaltung von Architekturvorgaben

Zur Erstellung, fortlaufenden Überprüfung und bedarfsbezogenen Weiterentwicklung der in diesem Dokument dargelegten Architekturvorgaben wird der im Governance Framework COBIT 5[142] 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 8: 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 für die IT des Bundes zu berücksichtigen sind:

1. Die Beachtung der in diesem Dokument aufgeführten Architekturvorgaben ist bei der IT Leistungserbringung sowie der IT-Beschaffung (gemäß Zielbild zur Beschaffungsbündelung - Teilprojekt 5) der unmittelbaren Bundesverwaltung gemäß Geltungsbereich (vgl. Kapitel 1.3 Geltungsbereich) verbindlich.

[142] ISACA. COBIT Framework. 2019 unter http://www.isaca.org/COBIT/Pages/default.aspx; zuletzt abgerufen am 24. April 2019.

2. Die Sicherstellung und Überprüfung der Einhaltung der Architekturrichtlinie ist durch das jeweilige Ressort/ die Behörde und der dort verorteten Projekte und Programme selbst vorzunehmen (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 „IT Controlling Bund“ mithilfe von Eigenbewertungen und Kennzahlen ermittelt. Die Erkenntnisse aus der Bewertung der Architekturvorgaben im IT-Controlling Bund werden bedarfsweise den Gremien der IT-Steuerung 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 gesetzt[143] und können auf dieser Basis Anpassungsbedarfe ableiten.

4. Derzeit bestehen folgende Zuständigkeiten, die im Rahmen der nächsten Fortschreibung validiert werden:

    a) Für die allgmeinen Vorgaben ist die „Projektleitung Architekturrichtlinie“ verantwortlich.

    b) Für die Architekturvorgaben der geschäftlichen Ebene ist das BMI verantwortlich.

    c) Für die Architekturvorgaben des Dienstemodells ist das BMI, und für die Weiterführung als Daueraufgabe die noch zu etablierende NMO[144], verantwortlich.

    d) Für die Architekturvorgaben des technischen Modells und des Informationsmodells ist der Anbieterbeirat verantwortlich. Entscheidungen werden in gemeinsamer Abstimmung zwischen den IT-Dienstleistern getroffen.

    e) Für die Architekturvorgaben zur Netzinfrastruktur ist die BDBOS im Geschäftsbereich des BMI zuständig.

    f) Für die Architekturvorgaben zur Informationssicherheit sind das BSI und der BfDI in Abstimmung mit dem BMI verantwortlich. Für die Anforderungen des Geheimschutzes, die ebenfalls zu beachten sind, ist das BSI in Abstimmung mit dem BMI verantwortlich. Die Aktualisierung der mit der Informationssicherheit eng verbundenen Architekturvorgaben zum Datenschutz und Geheimschutz wird vom BMI übergeordnet koordiniert.

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

[144] Die Nachfragemanagementorganisation (NMO) ist ein Bestandteil des Vorschlags zur Weiterentwicklung der IT-Steuerung des Bundes.

5. 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. Sofern ein Grundsatz veraltet ist oder einer Überarbeitung bedarf, werden die in Punkt 4 dieser Aufzählung genannten Verantwortlichen diesen Umstand an den für die Architekturrichtlinie Verantwortlichen melden. Ferner werden die Verantwortlichen der jeweiligen Bereiche dazu aufgefordert, die Architekturvorgaben in ihrem Verantwortungsbereich einer kontinuierlichen Aktualisierung zu unterziehen. Die Fortschreibung und Aktualisierung dieser Architekturrichtlinie ist eine strategische und damit ministerielle Aufgabe. Bis zur Übergabe der Aufgaben im Rahmen des übergreifenden Architekturmanagements an die operative Regelorganisation liegt die Verantwortung für die Fortschreibung der „Architekturrichtlinie für die IT des Bundes“ im BMI. Eine Beteiligung der zentralen IT-Beschaffungsstellen wird dabei sichergestellt, um im Rahmen neuer oder angepasster Architekturvorgaben Konformität mit vergaberechtlichen Voraussetzungen sowie laufenden Verfahren zu gewährleisten.

4.2 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 Vorgaben basiert auf einer Nutzwertanalyse[145], welche mit dem Entscheidungsprozess der Satisfizierung[146] 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.:

[145] Die 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.

[146] Die 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.

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.

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.

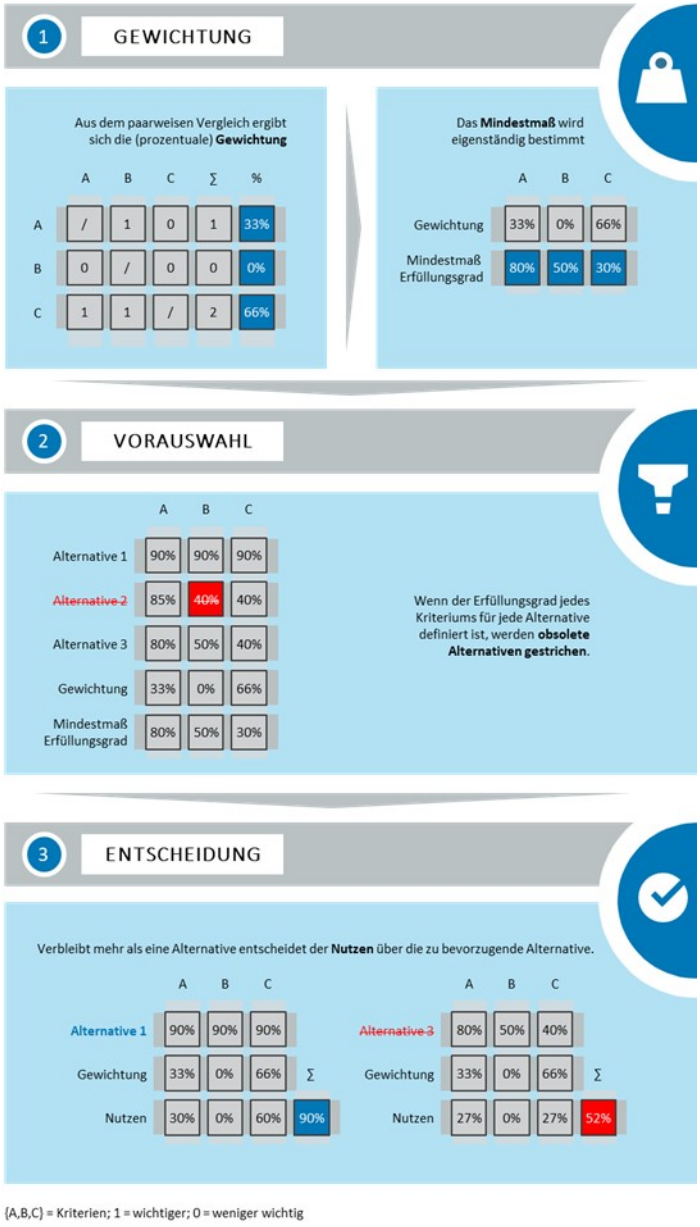

Abbildung 9: Beispielhafte Darstellung der Nutzwertanalyse mit Satisfizierung

5 Anhang

Der Anhang enthält das Glossar und die Verzeichnisse.

5.1 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 Amts 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.[147], [148] Cloud Computing bildet die Alternative zur traditionellen On-Premises Nutzung 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.[149]

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.

Digitale Kollaboration

---

[147] Bundesamt 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.

[148] IT-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.

[149] Die 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.

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.[150]

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.[151]

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.[152]

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.

Forschungs-IT

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

Informationstechnik des Bundes (IT des Bundes)

---

[150] ITWissen. Kollaboration. September 2019 unter https://www.itwissen.info/Kollaboration-collaboration.html; zuletzt abgerufen am 21. März 2021.

[151] Kompetenzzentrum 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.

[152] IT-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.

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.[153] Die Informationstechnik des Bunds 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.[154]

Interoperabilität

Interoperabilität bezeichnet die Fähigkeit von unterschiedlichen IT-Lösungen nahtlos zu interagieren.[155]

IT-Anwendung

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-Dienst

Ein IT-Dienst ist eine logische und rein konzeptionelle Einheit, die einen definierten Umfang an funktionalen Anforderungen erfüllt. Das Konzept des IT-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.

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.[156]

---

[153] Bundesministerium 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.

[154] CIO 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.

[155] Der 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.

[156] IT-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-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.

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.

Lose Kopplung

Die Lose Kopplung bezeichnet die Unabhängigkeit von Komponenten untereinander, wodurch Änderungen an einzelnen Komponenten einfacher durchgeführt werden können.[157]

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 Anwendungen[158], sofern diese als Baustein eigenständig und unabhängig nutzbar sind.[159]

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.[160]

Quality of Service

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

Querschnittsdienst

---

[157] Diese Definition orientiert sich an der AV-03

[158] Der 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.

[159] IT-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.

[160] Der 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.

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 für die IT des Bundes baut auf der Architekturrichtlinie auf und definiert Leitlinien und Vorgaben für eine standardisierte Umsetzung eines spezifischen Anwendungsfeldes.[161]

„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.[162]

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) 2119[163] 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.

---

[161] CIO 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.

[162] BSI. 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.

[163] Network Working Group. Datentracker. 1997 unter https://datatracker.ietf.org/doc/html/rfc2119; zuletzt abgerufen am 11. März 2022.

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.

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.[164]

[164] BSI. 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.

5.2 Verzeichnis aller Architekturvorgaben

Bezeichner	ID: 2022	ID: v6.1	Titel der Vorgabe 2022	Seite
AV-01	AV-9001-R02, AV-9002-R02	V-9001-R03	Architekturvorgaben und Recht	24
AV-02	AV-9003-R02, AV-9006-R02, AV-9079-R01	V-9003-R03	Standards, Methoden, Referenzarchitekturen und Interoperabilität	26
AV-03	AV-9012-R02	V-9012-R03	Nachhaltigkeit	29
AV-04	AV-9080-R01	V-9080-R02	Daten	31
AV-05	AV-9007-R02	V-9007-R03	Benutzerfreundlichkeit und Barrierefreiheit	32
AV-06	AV-9074-R01	V-9074-R02	Digitale Kollaboration	34
AV-07	AV-9075-R01	V-9075-R02	Open Source	35
AV-08	AV-9004-R03, AV-9005-R02	V-9004-R04	Informationssicherheit, Datenschutz, Geheimschutz und Systemgrundkonfiguration	37
AV-09	AV-9070-R02, AV-9008-R02	V-9070-R03	Souveränität und Unabhängigkeit	40
AV-10	AV-9011-R02, AV-9013-R02, AV-9014-R02, AV-9073-R01	V-9011-R03	Kopplung, Komplexität. Modularität, Wiederverwendbarkeit und Cloud Computing	42
GV-04	AV-9015-R02	V-9015-R03	Projektmanagement	46
GV-05	AV-9016-R02, AV-9017-R02, AV-9018-R02	V-9016-R03	Prozessmanagement	47

Bezeichner	ID: 2022	ID: v6.1	Titel der Vorgabe 2022	Seite
GV-08	AV-9075-R01	V-9075-R02	Daten-Governance	51
FV-01	AV-9019-R02	V-9019-R03	Allgemeine Nutzungs- und Leistungsverpflichtung	54
FV-02	AV-9025-R02	V-9025-R03	Dienst- und Schnittstellenbeschreibung	57
FV-04	AV-9026-R02	V-9026-R03	Anwendungen für den Bundesclient	58
FV-05	AV-9040-R02, AV-9041-R02, AV-9042-R02, AV-9043-R02, AV-9076-R01, AV-9077-R01	V-9040-R03	Informationen, Zeichen und Daten	59
FV-08	AV-9028-R03, AV-9029-R02, AV-9044-R02, AV-9045-R02, AV-9046-R02, AV-9048-R02	V-9028-R04	Identitätsinformationen, Zugriffssteuerung, Sicherheitskonzeption, Schutzbedarf, quality of Service, Security by Design, Separierung und Mandantentrennung	63
FV-09	AV-9024-R02, AV-9027-R02	V-9024-R03	Entkopplung	66

Bezeichner	ID: 2022	ID: v6.1	Titel der Vorgabe 2022	Seite
TV-01	AV-9034-R02, AV-9035-R02, AV-9072-R02	V-9034-R03	Entwicklung, Programmiersprachen und Qualitätsmanagement	69
TV-02	AV-9071-R02, AV-9050-R02	V-9071-R03	Schnittstellen	71
TV-05	AV-9032-R02	V-9032-R03	Datenbanksysteme	73
TV-08	AV-9047-R02, AV-9049-R02, AV-9052-R02	V-9047-R03	Kryptografie, sicherheitsrelevante Ereignisse und Schadprogrammabwehr	74
TV-09	AV-9036-R03, AV-9037-R02	V-9036-R04	Kommunikationsverbindungen und Netzwerkprotokoll	76
TV-10	AV-9078-R01, AV-9031-R02, AV-9033-R02, AV-9051-R03	V-9078-R02	Betrieb	80

5.3 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
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
DNS	Domain Name System

Abkürzung	Bedeutung
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
IVBB	Informationsverbund Berlin-Bonn

Abkürzung	Bedeutung
IVBV	Informationsverbund der Bundesverwaltung
IVÖV	Informationsverbund der öffentlichen Verwaltung
ITZBund	Informationstechnikzentrum Bund
KG	Koordningierungsgruppe
KI	Künstliche Intelligenz
KNB	Kompetenzstelle nachhaltige Beschaffung
KoITB	Konferenz der IT-Beauftragten der Ressorts
LAN	Local Area Network
MPLS WAN	Multiprotocol Label Switching Wide Are 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
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
TESTA-ng	Trans-European Services for Telematics between Administrations - New Generation

Abkürzung	Bedeutung
TLS	Transport Layer Security
TV	Technische Vorgabe
TOGAF	The Open Group Architecture Framework
UML	Unified Modelling Language
UN	United Nations
UP	Umsetzungsplan
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

5.4 Abbildungsverzeichnis

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
Januar 2024

Bildnachweis
Titelbild: vs148 / shutterstock.com

www.bmi.bund.de
www.cio.bund.de