Agora Digitale Transformation

Studie

IT-Beschaffung beim Bund: Standards, KPIs und Informationsmanagement

Autor:

Max Schulze

in Zusammenarbeit mit

LEITMOTIV

Agora Digitale Transformation gGmbH
Krausenstraße 8
10117 Berlin

T. +49(0)30 81 45 03 78 80
www.agoradigital.de
info@agoradigital.de

Ansprechperson:

Dr. Stefan Heumann
stefan.heumann@agoradigital.de

Gefördert von: STIFTUNG MERCATOR

IT-Beschaffung beim Bund: Standards, KPIs und Informationsmanagement
https://agoradigital.de/projekte/government-as-a-platform/

Design: Jakub Stejskal, Make Studio | Coverbild: Jakub Stejskal, Make Studio
Satz: www.parzelle34.de, Melissa Harms

Juli 2026 | DOI 10.5281/zenodo.20662422

Inhalt

Vorwort

Für große Organisationen und Unternehmen ist eine effektive IT-Steuerung und ein damit verbundenes IT-Controlling ein wichtiges Instrument, um organisationsübergreifend IT-Strategien und Standards durchzusetzen und Kosten zu sparen. Die Bundesregierung beschafft jährlich IT-Ausstattung und Software im Umfang mehrerer Milliarden Euro. Zahlreiche Handreichungen und Anforderungskataloge sollen das Einhalten von Qualitäts-, Wirtschaftlichkeits- und Sicherheitsstandards gewährleisten. In diesem Papier beschäftigen wir uns mit den bereits bestehenden Grundlagen, auf die eine effektive IT-Steuerung aufgesetzt werden könnte. Hierzu geben wir einen Überblick über bestehende Standards und Handreichungen und zeigen, wie diese mit KPIs verknüpft werden könnten. Die Übersicht zeigt, dass es eine Vielzahl an Dokumenten und Standards gibt. Diese Komplexität erschwert die Nutzung dieser Handreichungen bei der IT-Beschaffung und im IT-Controlling. Eine Verbesserung der IT-Beschaffung und der IT-Ausgabenkontrolle sollte daher auch die Konsolidierung der unterschiedlichen Dokumente, eine Priorisierung besonders wichtiger Vorgaben und eine Entwicklung mit ihr verbundener KPIs beinhalten.

Stefan Heumann
Geschäftsführer, Agora Digitale Transformation

Einleitung und Kontext

Eine professionelle IT-Beschaffung und damit verknüpfte Instrumente zur Qualitätskontrolle und Ausgabensteuerung sind ein wichtiger Baustein bei der Verwaltungsdigitalisierung auf Bundesebene. Denn in der Regel entwickelt die Bundesverwaltung IT-Dienste und -Lösungen nicht selbst, sondern kauft diese am Markt ein oder beauftragt ihre Entwicklung und Betrieb. Für die IT-Beschaffung und damit verknüpftes IT-Controlling existieren bereits zahlreiche Standards und Handreichungen. In diesem Papier wollen wir einen Überblick über die wichtigsten Dokumente geben.

Die ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT) schaffen bereits eine Basis für standardisierte Verträge in der IT-Beschaffung des Bundes. Dieses Papier baut auf dem bestehenden Vertragswerk der EVB-IT und den geltenden IT-Standards und Richtlinien der EU und des Bundesamts für Sicherheit in der Informationstechnik (BSI) auf und zeigt, wie welche relevanten IT-Kennzahlen und -Kriterien über kritische Dimensionen, von Sicherheit, zur Funktionalität, bis hin zur Betriebsführung und Kosten- und Nutzungseffizienz damit verknüpft werden könnten. Die Bewertung der KPIs ist in der Regel nur über eine Erhebung der hierfür relevanten Informationen bei den IT-Dienstleistern möglich und müsste im Vertragsmanagement bei der Beauftragung entsprechend berücksichtigt werden. Mit einem hier skizzierten Prozess zur Erhebung der notwendigen Informationen für das Beschaffungscontrolling und einer kontinuierlichen Prüfung (des Lieferanten-Monitoring) können Risiken, insbesondere im Bereich der Cyber-Sicherheit und der physischen Sicherheit, vermieden werden. Grundlage für einen solchen Prozess bieten Konzepte aus dem Beschaffungscontrolling und Vertragsmanagement, die in der Wirtschaft bereits umgesetzt werden.

Definitionen: IT-Ausgaben und EVB-IT

IT-Ausgaben lassen sich laut der EVB-IT[1] wie folgt kategorisieren:

Vertragsgegenstand	Anmerkung
Kauf von Hardware	nicht in diesem Papier betrachtet
Instandhaltung von Hardware	nicht in diesem Papier betrachtet
Kauf von Standardsoftware, bei Bedarf mit Pflegeleistung	vorgeschlagene Kriterien & Prozess sind anwendbar
Miete von Standardsoftware	vorgeschlagene Kriterien & Prozess sind anwendbar
Beschaffung von IT- Dienstleistungen, z.B. Beratungsleistungen, Benutzerunterstützung, Hotline	vorgeschlagene Kriterien & Prozess sind anwendbar, wenn die IT-Dienstleistungen sich auf die Schaffung neuer oder Erneuerung von IT-Systemen oder Software beziehen
Pflege von Standardsoftware	vorgeschlagene Kriterien & Prozess sind anwendbar, wenn der Lieferant der Standardsoftware auch die Pflege übernimmt, ansonsten nur Anwendung auf den Miet- oder Kaufvertrag
Cloudleistungen, insbesondere IaaS, PaaS und SaaS	vorgeschlagene Kriterien & Prozess sind anwendbar
Erstellung von IT-Systemen aus einer oder mehreren Systemkomponenten (Standardsoftware und/oder Hardware, ggf. Individualsoftware) einschließlich weiterer Leistungen zur Herbeiführung der Betriebsbereitschaft, wobei letztere und/oder die Erstellung der Individualsoftware den Schwerpunkt der Leistung darstellen, z.B. weil sie mehr als 15% - 20% des Auftragswertes ausmachen	vorgeschlagene Kriterien & Prozess sind anwendbar

[1] https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/evb-it-und-bvb/aktuelle_evb-it-node.html

Erstellung von Individualsoftware, Anpassung von Software auf Quellcodeebene oder durch Customizing auf Softwareleistungen reduzierter, gekürzter EVB-IT Systemvertrag	vorgeschlagene Kriterien & Prozess sind anwendbar
Kauf von IT-Systemen aus einer oder mehreren Systemkomponenten (Standardsoftware und/oder Hardware) einschließlich weiterer Leistungen zur Herbeiführung der Betriebsbereitschaft, ohne dass diese Leistungen den Schwerpunkt bilden	vorgeschlagene Kriterien & Prozess sind anwendbar
Serviceleistungen rund um ein IT-System oder für Individualsoftware, die über den Regelungsumfang zum Service in den EVB-IT Systemverträgen hinausgehen	vorgeschlagene Kriterien & Prozess sind anwendbar

Grundsätzlich lassen sich diese Vertragsformen in drei Kategorien zusammenfassen, welche die Grundlage für die Entwicklung der vorgeschlagenen Kriterien bilden.

Software

Sowohl die Erstellung von Individualsoftware, der Kauf oder die Miete von Standardsoftware als auch die Miete von Software-Diensten (Software-as-a-Service und Platform-as-a-Service) fallen alle unter die Kategorie „Software“, denn das eingekaufte Produkt ist in allen Fällen ein Software-Produkt.

IT-Infrastruktur

Bei der Beschaffung von Cloud Dienstleistungen kann auch IT-Infrastruktur im Rahmen eines Mietvertrags eingekauft werden (Infrastructure-as-a-Service, IaaS). Die Miete von IT-Infrastruktur unterscheidet sich zum Kauf von Hardware in dem Sinne, dass nicht physische Kapazität gemietet wird, sondern lediglich eine bestimmte Menge an Rechen-, Speicher- und Übertragungskapazität.

Wird eine Software gemietet, z.B. im Rahmen von Software-as-a-Service-Angeboten, so ist die IT-Infrastruktur in den meisten Fällen Teil des Produkts, weshalb die Kriterien und Frage-stellung für IT-Infrastruktur auch in der Software-Kategorie, je nach Vertragsgegenstand, optional hinzugefügt werden können.

Dienstleistungen

Dienstleistungen sind dann relevant, wenn es sich um Pflegeleistungen durch den Software-Hersteller (z.B. Anpassungen/„Customizing“ der Software) oder um Beratungsleistungen oder Rahmenverträge handelt, bei denen eine neue Software hergestellt wird oder die Betriebsführung einer bestehenden Software durch externe Dienstleistung übernommen wird („Managed Services“).

Prozess für das Beschaffungscontrolling

Bei der Beschaffung von IT-Systemen und Dienstleistungen ist eine kritische Prüfung der Funktionalität, Sicherheit und Betriebsführung erforderlich. Angriffe auf IT-Systeme nehmen kontinuierlich zu. Das BSI stuft die Risiken als hoch ein.[2] Die Kosten für die Bundes-IT steigen gleichermaßen.[3] Zudem sinkt, auch durch den zunehmenden Einsatz von KI-basierter Code-Generierung, die Qualität von Software.[4] Diese Trends zeigen deutlich, dass bei der IT-Beschaffung die Kennzahlen zu erheben und klare Kriterien dafür anzuwenden wichtiger wer-den. Denn die Erhebung der Kennzahlen schafft einen Anreiz für Lieferanten die IT-Systeme zu verbessern und gleichzeitig die notwendigen Informationen für ein effektives Vertragsmanagement.

Bei der Entwicklung der dafür notwendigen Prozesse kann auf die bestehende Praxis aus der Wirtschaft aufgebaut werden: das Beschaffungscontrolling. Die Zielsetzung eines effektiven Beschaffungscontrollings[5] umfasst in der Regel drei Elemente:

- Beschaffungskosten reduzieren
- Beschaffungsqualität erhöhen
- Beschaffungsrisiko verringern

Im Sinne des Beschaffungscontrollings, einer Aufgabe, die Teil der IT-Beschaffung ist, muss im ersten Schritt die **Informationsversorgung** sichergestellt werden[6].

Zweitens hat das Beschaffungscontrolling eine **Kontroll- und Steuerungsfunktion.** Dafür bietet sich die Etablierung von drei bekannten Mechanismen an: (1) ein Kennzahlensystem[7], (2) „*Total Cost of Ownership*"-Bewertung[8] und (3) eine Lieferantenbewertung[9].

So aufgesetzt, ergänzt das Beschaffungscontrolling die bestehende **Planungsfunktion** der einkaufenden Organisation des Bundes.

Auf Basis der Zielstellungen des Beschaffungscontrollings ergibt sich folgende Prozessarchitektur:

1. **Erfassung und Planung der Ausgaben** (ITRWEB 2.0 / IT-PLUTO, *Informationsversorgung*)
2. **Informationsbeschaffung:** Zustellung eines digitalen Fragebogens an den Zulieferer *(Informationsversorgung)*

[2] https://www.tagesschau.de/inland/innenpolitik/bsi-lagebericht-cybersicherheit-100.html

[3] https://www.tagesspiegel.de/gesellschaft/medien/digitalisierung-ausgaben-des-bundes-fur-software-deutlich-gestiegen-13891324.html

[4] https://www.computerwoche.de/article/3987861/mangelnde-softwarequalitat-verursacht-millionenschaden.html

[5] „Die indirekten Ziele des Beschaffungscontrollings können weitestgehend mit den generellen Beschaffungszielen gleichgesetzt werden (Piontek, 2016, S. 39). Somit sollen die richtigen Güter und Dienstleistungen in der erforderlichen Art, Menge und Qualität zur gewünschten Zeit am gewünschten Ort zur Verfügung stehen und dies zu möglichst niedrigen Kosten (Grün & Brunner, 2013, S. 120). Konkret sehen die indirekten Ziele wie folgt aus (Piontek, 2016, S. 45):"

[6] https://wiki.hslu.ch/controlling/Beschaffungscontrolling Piontek, 2016, S. 40, 47

[7] Arnold, 1997, S. 237-238, 240

[8] Ellram, 1995, S. 4, 20; Piontek, 2016, S. 144

[9] Britzelmaier, 2017, S. 405

3. **Bewertung der vorgelegten Information** des Zulieferers und der zu beschaffenden IT-Sache mit (a) Kriterienkatalog (b) Kennzahlensystem und (c) TCO-Methode oder Lieferantenbewertung *(Kontrolle und Steuerung)*
4. **Erfassung der Informationen und Bewertungen,** z.B. über ITR4Web Platform
5. **Jährliche Erneuerung und Auswertung** der Informationen zu den Kennzahlen und zu den Kriterien; *Monitoring (Informationsversorgung und Kontrolle)*

Offen bleibt die Frage, ob das Beschaffungscontrolling die Verantwortung für die Bewertung der jährlichen Berichterstattung durch die Lieferanten übernehmen kann („*Contract Management*“) oder ob dafür zusätzliche Ressourcen oder Werkzeuge (z.B. eine KI-gestützte Bewertung der jährlichen Kennzahlen) geschaffen werden müssen. Die Bewertung der Kennzahlen erfordert Kompetenzen im Bereich der IT-Steuerung, welche in den einkaufenden Organisationen möglicherweise nicht vorhanden sind.

Etablierte Mechanismen zur IT-Steuerung

Mit einem **Kennzahlensystem**[10] kann durch den vorgeschlagenen Prozess nicht nur die Kontrollfunktion, sondern auch die Steuerungsfunktion wahrgenommen werden. Mit den gewonnenen Daten aus der Ermittlung der Beschaffungskennzahlen sollen Zielkonflikte gelöst, sowie Abweichungen, Chancen und Risiken erkannt werden. Weiter können damit Ergebnisse gemessen und Rationalisierungspotenziale erschlossen werden. Das System dient als Orientierungsrahmen und erleichtert zudem die Beurteilung der Zielerreichung.

Ein Kennzahlensystem für IT-Beschaffung des Bundes gibt es nach unseren Recherchen bisher nicht und findet sich daher als Vorschlag in diesem Papier. Das Kennzahlensystem muss so-wohl regulatorische Rahmenbedingungen erfassen (NIS2, DORA, EU Cybersecurity Act, EU Cyber Resilience Act, DSGVO), sicherheitsrelevanten Anforderungen folgen (BSI) und die Um-setzung von Rahmenbedingungen prüfen (Deutschland-Stack, OZG-Rahmenarchitektur, IT-Architekturrichtlinie des Bundes, Blauer Engel) und sollte dabei auf etablierten Standards auf-bauen (ISO/IEC 27000-Reihe, 25000-Reihe, 20000-Reihe, 38500-Reihe, ISO/IEC 12207). Zudem gibt es praxisorientierte Rahmenwerke aus der Wirtschaft, die bei der Schaffung von Kennzahlen hilfreich sein können (ITIL 4, TOGAF 10, COBIT 2019, sowie die Prinzipien der FinOps Stiftung). Auf Basis des Kennzahlen- und Kriterienkatalogs kann in der Folge eine **Lieferantenbewertung** durchgeführt werden.

Total Cost of Ownership (TCO) dient der kompletten Erfassung der entstehenden Kosten durch die Beschaffung eines IT-Systems. Durch TCO soll die einseitige Konzentration auf die Anschaffungskosten verhindert und die Kosten für den eigentlichen Beschaffungsprozess, die Wartung, Instandhaltung und Entsorgung ebenfalls in die Betrachtung miteinbezogen werden. Ziel dieses Konzepts ist es, die Lieferantenwahl und -beurteilung zu optimieren.[11] Das Äquivalent zu dieser Methode aus der Wirtschaft ist im Kontext der Bundesverwaltung die **WiBe Methode (5.0) für die**

[10] Arnold, 1997, S. 237-238, 240

[11] Ellram, 1995, S. 4, 20; Piontek, 2016, S. 144)

Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT.[12]

Wird die Beschaffung durch eine Vertragsmanagement-Funktion erweitert, ist es sinnvoll, dass in diesem Rahmen jährliche Monitoringberichte von den Lieferanten zu den Kennzahlen eingefordert und von der einkaufenden Stelle überprüft werden.

Aus Erfahrungen von Einkaufsorganisationen in ganz Europa ist das Vertragsmanagement die zentrale Aufgabe für langlaufende IT-Verträge. Die notwendige Kompetenz für die Bewertung der Kennzahlen und erbrachten Leistungen fehlt in vielen Einkaufsorganisationen und kann durch zusätzliche Ressourcen oder digitale Werkzeuge geschaffen werden.

Vorschlag zum Kriterienkatalog & Kennzahlsystem

Dimension	Relevanz	Kernfrage
Softwaresicherheit	Cybersicherheit der IT-Systeme des Bundes	Ist das IT-System nach EU & BSI Anforderungen gesichert und werden Sicherheitsaspekte im Betrieb kontinuierlich überwacht?
Physische Sicherheit	Sicherung der IT-Systeme in Krisensituationen	Ist der physische Standort des IT-Systems bekannt, sind entsprechende physische Sicherheitsmaßnahmen nach BSI umgesetzt und kann der Standort in Krisensituationen geschützt werden?
Funktionalität	Konsolidierung von IT-Systemen, Nutzung geteilter Infrastruktur, Standards und Dienste (z.B. Deutschland-Stack)	Kann die geforderte Funktion durch bestehende IT-Systeme abgedeckt werden? Werden für die Erfüllung die Standards und Dienste des Deutschland-Stacks genutzt?
Betrieb	Governance und Prozessfähigkeit für den Betrieb	Wird der Betrieb sichergestellt und werden standardisierte und regelkonforme Prozesse genutzt?
Finanzen	Betriebskosten, Schaffungskosten, Wirtschaftlichkeit, Kosten-Nutzen	Entsprechen die IT-Systemkosten dem Nutzen? („*Total Cost of Ownership*“)
Nachhaltigkeit	Umweltmanagement, Effizienz und Klimaziele	Werden bei der Schaffung und dem Betrieb der IT-Systeme die notwendigen Maßnahmen ergriffen, um Klimaziele einzuhalten?

[12] https://www.digitale-verwaltung.de/SharedDocs/downloads/Webs/DV/DE/digitale-loesungen/it-einkauf/wirtschaftlichkeits-betrachtung/wibe5-0/wibe-fachkonzept-5-0.pdf?__blob=publicationFile&v=5

1 Dimension: Softwaresicherheit

Die Dimension Softwaresicherheit umfasst das Patch-Management, die Durchführung von Sicherheitstests, die Erfassung und Bewertung von Software-Abhängigkeiten (Open Source und proprietär), das Schwachstellenmanagement, sowie die Einhaltung sicherer Entwicklungsprozesse. Für die Beschaffung von IT-Systemen ist diese Dimension, insbesondere im Kontext der NIS2-Richtlinie, des BSI IT-Grundschutzes und der bevorstehenden Anforderungen der EU Cyber Resilience Act (CRA) von zentraler Bedeutung.

1.1 Patch- und Änderungsmanagement

Element	Beschreibung
Kriterium	Dokumentierter Prozess für das zeitnahe Einspielen von Sicherheitsupdates und Patches, einschließlich definierter Reaktionszeiten nach Kritikalität (CVSS-Punktzahl).
Bewertungsfrage	Liegt ein dokumentiertes Patch-Management-Konzept gemäß BSI OPS.1.1.3 vor?
Mehrwert für die IT-Steuerung	Ermöglicht eine Bewertung der Patch-Disziplin über die erfassten IT-Systeme hinweg und deckt Systeme mit erhöhtem Risiko durch verzögerte Updates auf. Die systematische Erfassung unterstützt die Priorisierung von Maßnahmen und reduziert das Angriffsrisiko über das gesamte Portfolio.
Quellen	BSI IT-Grundschutz OPS.1.1.3 (Patch- und Änderungsmanagement), ISO/IEC 27001:2022, CVSS v4.0
KPIs	1.1.1: Wie hoch ist die durchschnittliche Zeitspanne zwischen der Veröffentlichung eines kritischen Patches (CVSS ≥ 9.0) und dessen produktiver Bereitstellung?
Anwendungsbereich	Software, Dienstleistungen, IT-Infrastruktur

1.2 Sicherheitstests und -validierung

Element	Beschreibung
Kriterium	Regelmäßige Durchführung von Sicherheitstests (Penetrationstests, SAST, DAST) mit dokumentiertem Reifegrad gemäß OWASP ASVS.
Bewertungsfrage	Welches OWASP-ASVS-Konformitätsniveau (L1/L2/L3) wird erreicht? Sind statische und dynamische Analysewerkzeuge (SAST/DAST) im Einsatz?

Mehrwert für die IT-Steuerung	Schafft Vergleichbarkeit des Sicherheitsniveaus über alle IT-Systeme hinweg. Identifiziert IT-Systeme, die noch nicht ausreichend getestet wurden.
Quellen	BSI IT-Grundschutz OPS.1.1.6 (Software-Tests und -Freigaben), OWASP ASVS Version 5.0.0 (Mai 2025), ISO/IEC 27001:2022
KPIs	1.2.1: Anzahl der durchgeführten Penetrationstests
Anwendungsbereich	Software, Dienstleistungen, IT-Infrastruktur

1.3 Software-Stückliste (SBOM)

Element	Beschreibung
Kriterium	Verfügbarkeit einer vollständigen Software-Stückliste (Software Bill of Materials, „SBOM“) in standardisiertem Format (SPDX oder CycloneDX), einschließlich aller direkten und transitiven Abhängigkeiten.
Bewertungsfrage	Kann eine vollständige SBOM im Format SPDX oder CycloneDX gemäß BSI TR-03183-2 bereitgestellt werden? Umfasst diese alle direkten und transitiven Abhängigkeiten?
Mehrwert für die IT-Steuerung	Schafft Transparenz über die eingesetzten Softwarekomponenten im gesamten Portfolio und ermöglicht die schnelle Identifikation betroffener Anwendungen bei Bekanntwerden neuer Schwachstellen (z. B. Log4j-Szenario). Bereitet zudem auf die CRA-Anforderungen ab Dezember 2027 vor.
Quellen	BSI TR-03183-2 v2.1.0 (September 2024), EU Cyber Resilience Act (CRA, vollständige Anwendung ab Dezember 2027), NIS2 Richtlinie (EU) 2022/2555
KPIs	1.3.1: Anzahl der Aktualisierung der SBOM-Liste 1.3.2: % der eingesetzten Komponenten entsprechen den Standards aus der Architektur des Deutschland-Stacks 1.3.3: % der eingesetzten Komponenten kommen aus dem Angebot des Deutschland-Stack
Anwendungsbereich	Software, Dienstleistungen

1.4 Schwachstellenmanagement und Reaktionsprozesse

Element	Beschreibung

Kriterium	Verfügbarkeit einer vollständigen Software-Stückliste (Software Bill of Materials, „SBOM“) in standardisiertem Format (SPDX oder CycloneDX), einschließlich aller direkten und transitiven Abhängigkeiten.
Bewertungsfrage	Kann eine vollständige SBOM im Format SPDX oder CycloneDX gemäß
Mehrwert für die IT-Steuerung	BSI TR-03183-2 bereitgestellt werden? Umfasst diese alle direkten und transitiven Abhängigkeiten?
Quellen	Schafft Transparenz über die eingesetzten Softwarekomponenten im gesamten Portfolio und ermöglicht die schnelle Identifikation betroffener Anwendungen bei Bekanntwerden neuer Schwachstellen (z. B. Log4j-Szenario). Bereitet zudem auf die CRA-Anforderungen ab Dezember 2027 vor.
KPIs	BSI TR-03183-2 v2.1.0 (September 2024), EU Cyber Resilience Act (CRA,
Anwendungsbereich	vollständige Anwendung ab Dezember 2027), NIS2 Richtlinie (EU) 2022/2555

1.5 Sicherer Softwareentwicklungszyklus (SDLC)

Element	Beschreibung
Kriterium	Nachweis eines dokumentierten sicheren Softwareentwicklungszyklus mit Bedrohungsmodellierung, sicheren Coding-Standards und Sicherheitsanforderungen ab Projektbeginn.
Bewertungsfrage	Wird ein dokumentierter „Secure Development Lifecycle“ (SDLC) befolgt? Werden Sicherheitsanforderungen bereits bei der Projektinitiierung definiert? Findet eine Bedrohungsmodellierung statt?
Mehrwert für die IT-Steuerung	Identifiziert Anwendungen, bei denen Sicherheit nicht von Beginn an mitgedacht wurde, was ein wesentlicher Risikofaktor für nachträgliche und kostenintensive Nachbesserungen ist. Unterstützt die Priorisierung von Modernisierungsmaßnahmen.
Quellen	BSI IT-Grundschutz CON.8 (Software-Entwicklung), ISO/IEC 27001:2022, ISO/IEC 27034 (Anwendungssicherheit)
KPIs	1.5.1: Was war das Ergebnis der Bedrohungsmodellierung? 1.5.2: Liste der Maßnahmen, die auf Basis der Bedrohungsmodellierung bereits im Entwicklungsprozess umgesetzt wurden.
Anwendungsbereich	Software, Dienstleistungen

1.6 Anwendungssicherheitskontrollen und Härtung

Element	Beschreibung
Kriterium	Implementierung technischer Sicherheitskontrollen wie: Mehrfaktor-Authentifizierung (MFA), rollenbasierte Zugriffskontrolle (RBAC/ABAC) und Verschlüsselungsstandards (TLS-Version).
Bewertungsfrage	Welche Authentifizierungsmechanismen werden unterstützt (MFA, SSO)? Kann die Anwendung in die BundID oder im behördeninternen Active Directory integriert werden? Welche TLS-Version ist im Einsatz?
Mehrwert für die IT-Steuerung	Schafft Vergleichbarkeit der technischen Sicherheitsausstattung im Portfolio und identifiziert Anwendungen mit veraltetem Sicherheitsniveau (z. B. fehlende MFA, veraltete Verschlüsselung).
Quellen	BSI IT-Grundschutz APP.6 (Allgemeine Software), BSI C5:2020, OWASP Top 10 (2021)
KPIs	1.6.1: Liste der Authentifizierungsmethoden 1.6.2: Liste der verfügbaren Rollen in der Anwendung 1.6.3: TLS-Version bzw. des verwendeten Verschlüsselungsstandards
Anwendungsbereich	Software, Dienstleistungen

1.7 Drittanbieter- und Lieferkettenrisikomanagement

Element	Beschreibung
Kriterium	Vollständige Erfassung aller Drittanbieterkomponenten mit dokumentierter Sicherheitsbewertung der kritischen Zulieferer und End-of-Life-Planung.
Bewertungsfrage	Liegt eine vollständige Inventarliste aller Drittanbieterkomponenten vor? Werden kritische Zulieferer regelmäßig hinsichtlich ihrer Sicherheitslage bewertet? Gibt es einen dokumentierten End-of-Life-Managementprozess?
Mehrwert für die IT-Steuerung	Macht Lieferkettenrisiken im Portfolio sichtbar und ermöglicht eine frühzeitige Identifikation von Abhängigkeiten von unsicheren oder auslaufenden Komponenten. Unterstützt die NIS2-Anforderungen an das Supply-Chain-Risikomanagement.
Quellen	NIS2-Richtlinie Art. 21 (Lieferkettenanforderungen), ISO/IEC 27001:2022, BSI TR-03183-2
KPIs	siehe auch 1.3.1, 1.3.2, 1.3.3

	1.7.1: Anzahl der Drittanbieter in der Lieferkette 1.7.2: Anzahl der Drittanbieterkomponenten und Aufteilung nach proprietär und quelloffen 1.7.3: Anzahl der Drittanbieter, die im Zeitraum bewertet wurden 1.7.4: Anzahl der Drittanbieterkomponenten, die nicht mehr unterstützt werden (End-of-Life)
Anwendungsbereich	Software, Dienstleistungen

1.8 Vorfallreaktion und forensische Fähigkeiten

Element	Beschreibung
Kriterium	Dokumentierter Incident-Response-Plan mit definierten Protokollierungszeiträumen, SIEM-Integrationsfähigkeit und Einhaltung der NIS2-Meldepflichten (24h/72h/30d).
Bewertungsfrage	Ist die Anwendung auf die Einhaltung der NIS2-Meldepflicht innerhalb von 24 Stunden vorbereitet? Welche Protokollierungsfähigkeiten stehen für forensische Untersuchungen zur Verfügung? Ist eine SIEM-Integration vorhanden?
Mehrwert für die IT-Steuerung	Gibt Auskunft über die Reaktionsfähigkeit je IT-System im Falle eines Sicherheitsvorfalls. Identifiziert Systeme ohne ausreichende Logging- und Forensik-Fähigkeiten und unterstützt die portfolioweite NIS2-Compliance.
Quellen	BSI IT-Grundschutz DER.2.1 (Behandlung von Sicherheitsvorfällen), NIS2 Art. 23 (24h/72h/30d Meldekette), ISO/IEC 27001:2022
KPIs	1.8.1: Anzahl der NIS2 Meldungen 1.8.2: Anzahl anderer Sicherheitsvorfälle 1.8.3: Durchschnittliche Zeit von der Identifikation eines Vorfalls bis zur Meldung (in Stunden)
Anwendungsbereich	Software, Dienstleistungen, IT-Infrastruktur

2 Dimension: Physische Sicherheit

Mit Kriterien zur physischen Sicherheit werden Themen wie der Hosting-Standort, die Klassifizierung und Zertifizierung von Rechenzentren, die Anbieterbewertung, Service-Level-Vereinbarungen (SLA), die Sicherheit der Lieferkette, sowie Datenschutzanforderungen erfasst. Für die Bundesverwaltung sind hier insbesondere die Anforderungen an digitale Souveränität, DSGVO-Konformität und die BSI C5-Attestierung maßgeblich.

2.1 Standort und Datensouveränität des Rechenzentrums

Element	Beschreibung
Kriterium	Dokumentation des geografischen Standorts aller primären und Backup-Rechenzentren, der geltenden Rechtsordnung sowie der Einhaltung von Datenresidenzanforderungen.
Bewertungsfrage	Wo befinden sich die primären und Backup-Rechenzentren physisch? Welcher Rechtsordnung unterliegt der Datenzugriff? Werden Daten ausschließlich in Deutschland/der EU verarbeitet und gespeichert?
Mehrwert für die IT-Steuerung	Grundvoraussetzung für die Bewertung der digitalen Souveränität. Identifiziert Anwendungen mit Datenverarbeitung außerhalb der EU und damit potenziellem DSGVO-Verstoß. Ermöglicht die Datenerfassung für die spätere Umsetzung des Deutschland-Stacks.
Quellen	DSGVO Art. 44–50 (internationale Datenübermittlung), BSI IT-Grundschutz INF.2 (Rechenzentrum sowie Serverraum), Cloud-Strategie der Bundesverwaltung
KPIs	2.1.1: Anzahl der Rechenzentrumsstandorte, die für die Bereitstellung des IT-Systems oder der Infrastruktur eingesetzt werden
Anwendungsbereich	Software, IT-Infrastruktur

2.2 Rechenzentrumsklassifizierung und Verfügbarkeitsstufe

Element	Beschreibung
Kriterium	Klassifizierung des Rechenzentrums nach EN 50600 Verfügbarkeitsklasse (1–4).
Bewertungsfrage	Welche EN-50600-Verfügbarkeitsklasse weist das Rechenzentrum auf? Welche zertifizierte Verfügbarkeit wird garantiert?

Mehrwert für die IT-Steuerung	Ermöglicht den objektiven Vergleich der Infrastrukturqualität über verschiedene Anbieter und Standorte hinweg. Unterstützt die Dimensionierung der Infrastruktur entsprechend der tatsächlichen Verfügbarkeitsanforderungen und verhindert Über- oder Unterversorgung.
Quellen	EN 50600-1:2019 (Allgemeine Konzepte, Verfügbarkeitsklassen 1–4)
KPIs	2.2.1: Maximale garantierte Verfügbarkeit aller Rechenzentren, die für den Betrieb eines IT-Systems oder einer Infrastruktur eingesetzt werden
Anwendungsbereich	Software, IT-Infrastruktur

2.3 Sicherheitszertifizierung der Cloud-/Hosting-Anbieter

Element	Beschreibung
Kriterium	Nachweis aktueller Sicherheitszertifizierungen des Hosting-Anbieters, insbesondere BSI C5 Typ 2-Testat und ISO 27001-Zertifizierung.
Bewertungsfrage	Verfügt der Anbieter über ein aktuelles BSI C5:2020 Typ 2-Testat? Kann der vollständige Prüfbericht vorgelegt werden? Liegt eine ISO 27001/27017/27018-Zertifizierung vor?
Mehrwert für die IT-Steuerung	Schafft ein einheitliches Sicherheitsniveau für alle Cloud- und Hosting-Dienste im Portfolio. BSI C5 ist für die Bundesverwaltung der maßgebliche Mindeststandard für Cloud-Dienste und IT-Infrastruktur. Software-Anwendungen, die zusammen mit Infrastruktur gekauft werden, müssen für die genutzte Infrastruktur die Atteste der Infrastruktur-Lieferanten vorlegen. Kerndifferenzierungsmerkmal von EU/DE Hosting und Cloud-Anbietern.
Quellen	BSI C5:2020; Nachfolger C5:2026 mit 168 Kriterien in Vorbereitung, ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019
KPIs	2.3.1: Datum der letzten C5-Zertifizierung 2.3.2: Datum der letzten ISO27001-Zertifizierung
Anwendungsbereich	Software, IT-Infrastruktur

2.4 Service-Level-Vereinbarungen (SLA) und Verfügbarkeit

Element	Beschreibung
Kriterium	Dokumentation der vertraglich vereinbarten Verfügbarkeitsgarantie, des Redundanzniveaus und der tatsächlichen historischen Verfügbarkeit.

Bewertungsfrage	Welche konkreten Verfügbarkeitsgarantien sind im SLA vereinbart (z. B. 99,9 %, 99,99 %)? Welches Redundanzniveau ist implementiert (N, N+1, 2N, 2N+1)? Wie war die tatsächliche Verfügbarkeit in den letzten 12 Monaten?
Mehrwert für die IT-Steuerung	Ermöglicht die Bewertung der Angemessenheit der vereinbarten Verfügbarkeit im Verhältnis zu den fachlichen Anforderungen. Identifiziert Über- oder Unterversorgung und unterstützt SLA-basierte Preisverhandlungen.
Quellen	EN 50600-1:2019 (Verfügbarkeitsklassen), EVB-IT Cloud (SLA-Anforderungen)
KPIs	2.4.1: Gemessene Verfügbarkeit über Laufzeit (Jahr) (z.B. 99.98%)
Anwendungsbereich	Software, IT-Infrastruktur

2.5 Physische Sicherheitsinfrastruktur

Element	Beschreibung
Kriterium	Umsetzung physischer Sicherheitsmaßnahmen gemäß ISO 27001 Anhang A.7 und EN 50600-2-5 einschließlich Zutrittskontrolle, Überwachung und Perimeterschutz.
Bewertungsfrage	Wie werden die physischen Sicherheitskontrollen gemäß ISO 27001:2022 Anhang A.7 umgesetzt? Welche Zutrittskontrollmechanismen sind im Einsatz (biometrisch, Mehrfaktor)? Liegt eine EN-50600-2-5-Konformität vor?
Mehrwert für die IT-Steuerung	Stellt sicher, dass die physische Sicherheit der Infrastruktur dem Schutzbedarf der verarbeiteten Daten entspricht. Besonders relevant für VS-NfD-klassifizierte Anwendungen.
Quellen	ISO/IEC 27001:2022 Anhang A.7.1–A.7.14, EN 50600-2-5 (Sicherheitssysteme), BSI IT-Grundschutz INF.2
KPIs	2.5.1: Anzahl der Zutritte 2.5.2: Datum der letzten Prüfung oder Zertifizierung für die physischen Sicherheitsinstallationen 2.5.3: Anzahl der umgesetzten Sicherheitsmaßnahmen
Anwendungsbereich	Software, IT-Infrastruktur

2.6 Lieferketten- und Unterauftragsnehmersicherheit

Element	Beschreibung
Kriterium	Vollständige Dokumentation aller Unterauftragnehmer (Subprozessoren) mit Standorten, Zertifizierungen und DSGVO-Art.-28-Konformität.
Bewertungsfrage	Kann eine vollständige Liste aller Unterauftragnehmer mit Standortangaben vorgelegt werden? Verfügen die Unterauftragnehmer über gleichwertige Zertifizierungen (C5, ISO 27001)? Wie wird die DSGVO-Art.-28(3)-Konformität sichergestellt?
Mehrwert für die IT-Steuerung	Macht die gesamte Lieferkette pro Anwendung transparent und identifiziert Konzentrationsrisiken oder Abhängigkeiten von Anbietern außerhalb der EU. Unterstützt die Einhaltung der DSGVO-Auftragsverarbeitungsanforderungen.
Quellen	DSGVO Art. 28(3) (Anforderungen an Auftragsverarbeiter), BSI C5:2020 Kriterien CLD.6.3.1 und CLD.8.1.5, NIS2-Richtlinie Art. 21
KPIs	2.6.1: Anzahl der Unterauftragnehmer 2.6.2: Datum der letzten Überprüfung der Unterauftragnehmer hinsichtlich Zertifizierung und Konformität 2.6.3: Anzahl der Unterauftragnehmer, deren Anteilsverhältnisse sich über die vergangenen 12 Monate verändert haben (z.B. Verkauf von mehr als 24,9 % der Anteile13)
Anwendungsbereich	Software, Dienstleistungen, IT-Infrastruktur

2.7 Datenschutz- und Privatsphärekontrollen

Element	Beschreibung
Kriterium	Nachweis der Umsetzung technischer Datenschutzmaßnahmen gemäß DSGVO Art. 32, ISO 27018-konformer Schutz personenbezogener Daten sowie Datentrennung.
Bewertungsfrage	Welche technischen Maßnahmen gemäß DSGVO Art. 32 sind implementiert (Verschlüsselung, Pseudonymisierung, Zugriffskontrolle)? Wie wird die Mandantentrennung sichergestellt? Liegt eine ISO 27018-Konformität für den Schutz personenbezogener Daten in der Cloud vor?

[13] Die Schwelle von 24,9 % liegt knapp unterhalb der gesellschaftsrechtlichen Sperrminorität (25 %), ab der Gesellschafter nach deutschem Recht wesentliche Beschlüsse blockieren können (§ 179 Abs. 2 AktG; § 53 Abs. 2 GmbHG). Anteilsveränderungen in diesem Bereich können daher die tatsächliche Kontrolle über den Unterauftragnehmer maßgeblich verändern.

Mehrwert für die IT-Steuerung	Ermöglicht eine portfolioweite Datenschutz-Compliance-Bewertung und identifiziert Anwendungen mit unzureichenden technischen Datenschutzmaßnahmen — insbesondere relevant für bürgernahe Dienste.
Quellen	DSGVO Art. 28 und 32, ISO/IEC 27018:2019, ISO/IEC 27017:2015
KPIs	2.7.1: Datum der letzten Überprüfung der ISO 27018-Konformität
Anwendungsbereich	Software, Dienstleistungen, IT-Infrastruktur

2.8 Betriebliche Resilienz und Notfallvorsorge

Element	Beschreibung
Kriterium	Dokumentation der Wiederherstellungsziele (RPO/RTO), des betrieblichen Informationsmanagements gemäß EN 50600-3-1 und der PUE-/Energieeffizienzkennzahlen.
Bewertungsfrage	Welche Wiederherstellungsziele gelten für diese Anwendung? Sind diese im SLA vertraglich gesichert? Wird das Rechenzentrum gemäß EN 50600-3-1 betrieben?
Mehrwert für die IT-Steuerung	Unterstützt die Business-Continuity-Planung über das gesamte Portfolio und identifiziert IT-Systeme, deren Wiederherstellungsziele nicht den fachlichen Anforderungen entsprechen.
Quellen	EN 50600-3-1 (Management und Betriebsinformation), ISO 22301:2019 (Business Continuity Management), BSI IT-Grundschutz DER.4 (Notfallmanagement)
KPIs	2.8.1: Datum des letzten vollständigen erfolgreichen Wiederherstellungstests 2.8.2: Anzahl der durchgeführten Wiederherstellungstests im Erfassungszeitraum
Anwendungsbereich	Software, IT-Infrastruktur

3 Dimension: Funktionalität

3.1 Funktionale Eignung (ISO/IEC 25010:2023)

Element	Beschreibung
Kriterium	Bewertung der funktionalen Eignung anhand der drei Teilmerkmale: funktionale Vollständigkeit (Anforderungsabdeckung), funktionale Korrektheit (Fehlerrate) und funktionale Angemessenheit (Aufgabenunterstützung).
Bewertungsfrage	Welcher Anteil der dokumentierten Anforderungen ist vollständig umgesetzt? Wie hoch ist die Fehlerrate nach Schweregrad? Unterstützt die Anwendung die Nutzenden angemessen bei der Aufgabenerledigung?
Mehrwert für die IT-Steuerung	Schafft eine objektive, normbasierte Vergleichbarkeit der Funktionsqualität im Portfolio. Identifiziert IT-Systeme mit Funktionslücken oder hoher Fehlerrate als Kandidaten für Modernisierung oder Ablösung.
Quellen	ISO/IEC 25010:2023 (Merkmal 1: Funktionale Eignung), ISO/IEC 25040:2024 (5-Stufen-Evaluierungsprozess)
KPIs	3.1.1: Deckungsgrad (%) der Funktionen vs. Anforderungen 3.1.2: Gemeldete Fehler (Anzahl) über Erfassungszeitraum (z.B. IT-Tickets) 3.1.3: „Net-Promoter-Score“ der Nutzenden, die durch eine Kurzumfrage im Erfassungszeitraum erhoben wurde zur Bestimmung der funktionalen Angemessenheit
Anwendungsbereich	Software, Dienstleistungen

3.2 Anwendungsklassifizierung und Nutzerreichweite

Element	Beschreibung
Kriterium	Klassifizierung der Anwendung als öffentlich oder intern, Erfassung der Gesamtnutzerzahl und Differenzierung nach Nutzertypen (Beschäftigte, Bürgerinnen und Bürger, andere Behörden).
Bewertungsfrage	Handelt es sich um einen öffentlich zugänglichen OZG-Dienst oder eine interne Fachanwendung? Wie viele aktive Nutzende hat die Anwendung (letzte 30 Tage, 12 Monate)? Wie verteilen sich diese auf die Nutzergruppen (interne Mitarbeitende, Bürgerinnen und Bürger, andere Behörden)?

Mehrwert für die IT-Steuerung	Grundlage für die Priorisierung im Portfolio — bürgernahe Anwendungen mit hoher Nutzerzahl erfordern andere Investitions- und Qualitätsanforderungen als interne Hilfswerkzeuge. Unterstützt die Kapazitätsplanung und Kostenallokation.
Quellen	OZG-Rahmenarchitektur, DIN SPEC 66336 (OZG-Servicestandard)
KPIs	3.2.1: Anzahl der Nutzenden über den Erfassungszeitraum (Anzahl der Sitzungen) 3.2.2: Durchschnittliche Zeit, die Nutzende mit der Anwendung verbringen (Minuten / Stunden) 3.2.3: Anzahl der Nutzenden nach Gruppen (Mitarbeitende, Bürgerinnen und Bürger, andere Behörden)
Anwendungsbereich	Software, Dienstleistungen

3.3 Funktionale Kategorisierung und Dienstart

Element	Beschreibung
Kriterium	Zuordnung der Anwendung zu OZG-Lebenslagen und Funktionsbausteinen, Bewertung des EfA-Nachnutzungspotenzials (Einer für Alle).
Bewertungsfrage	Welcher OZG-Lebenslage ist die Anwendung zugeordnet? Welchen Funktionsbausteinen der OZG-Rahmenarchitektur entspricht sie? Besteht Potenzial für eine Nachnutzung im Rahmen des EfA-Prinzips?
Mehrwert für die IT-Steuerung	Identifiziert funktionale Redundanzen über Ressortgrenzen hinweg und zeigt Nachnutzungspotenziale auf. Reduziert Doppelentwicklungen und unterstützt die Standardisierung gemäß OZG-Rahmenarchitektur.
Quellen	OZG-Rahmenarchitektur (Funktionsbausteine), IT-Rahmenarchitektur des Bundes, EfA-Prinzip
KPIs	-
Anwendungsbereich	Software, Dienstleistungen

3.4 Integration und Interoperabilität

Element	Beschreibung
Kriterium	Erfassung aller Schnittstellen (Anzahl, Typ, Richtung), Integration mit föderalen Basiskomponenten (BundID, Servicekonto, Portalverbund), Konformität

	mit dem European Interoperability Framework (EIF) und den Komponenten aus dem Deutschland-Stack.
Bewertungsfrage	Wie viele Systemschnittstellen bestehen (eingehend/ausgehend)? Welche föderalen Basiskomponenten sind integriert (BundID, Portalverbund etc.)? Entspricht die Anwendung den Anforderungen der Architekturrichtlinie des Bundes? Werden Dienste und Standards aus dem Deutschland-Stack genutzt?
Mehrwert für die IT-Steuerung	Macht die Integrationslandschaft sichtbar und identifiziert isolierte Anwendungen oder fehlende Anbindungen an Basiskomponenten. Unterstützt die Planung von Konsolidierungs- und Integrationsmaßnahmen.
Quellen	Architekturrichtlinie des Bundes, Föderale IT-Architekturrichtlinien V1 (FIT-AB), European Interoperability Framework (EIF), Deutschland-Stack Architektur
KPIs	3.4.1: Anteil der Funktionalitäten der Anwendung, der durch Basiskomponenten oder Deutschland-Stack-Dienste abgedeckt wird (%) 3.4.2: Anzahl der Systemschnittstellen, die für die Integration mit anderen Systemen offenstehen 3.4.3: Anteil der Funktionalitäten der Anwendung, die über Schnittstellen genutzt werden können (%)
Anwendungsbereich	Software, Dienstleistungen

3.5 Lebenszyklusprozessreife (ISO/IEC 12207)

Element	Beschreibung
Kriterium	Bewertung der Prozessreife über die 30 Prozesse der ISO/IEC 12207 (Vereinbarung, Organisation, Technisches Management, Technik) und Zuordnung zur aktuellen Lebenszyklusphase.
Bewertungsfrage	In welcher Lebenszyklusphase befindet sich die Anwendung (Planung, Entwicklung, Betrieb, Wartung, Ablösung)? Sind die Prozesse gemäß ISO/IEC 12207 dokumentiert?
Mehrwert für die IT-Steuerung	Ermöglicht die Einschätzung der Prozessreife je Anwendung und identifiziert solche, die sich dem End-of-Life nähern oder bei denen wesentliche Lebenszyklusprozesse nicht etabliert sind.
Quellen	ISO/IEC/IEEE 12207:2017 (Software Life Cycle Processes)
KPIs	-
Anwendungsbereich	Software, Dienstleistungen

3.6 Nutzungsqualität (Quality in Use)

Element	Beschreibung
Kriterium	Bewertung der Nutzungsqualität anhand der fünf Merkmale: Effektivität, Effizienz, Zufriedenheit, Risikofreiheit und Kontextabdeckung gemäß ISO/IEC 25010:2023.
Bewertungsfrage	Wurde eine Nutzungsqualitätsbewertung gemäß ISO/IEC 25010:2023 durchgeführt? Wie bewerten die Nutzenden Effektivität und Zufriedenheit? Liegen Nutzerbefragungsergebnisse vor?
Mehrwert für die IT-Steuerung	Ergänzt die technische Bewertung um die Perspektive der Nutzenden. Anwendungen mit niedriger Nutzungsqualität sind Kandidaten für Verbesserungen oder Ablösung, unabhängig von ihrer technischen Qualität.
Quellen	ISO/IEC 25010:2023 (Quality-in-Use-Modell), DIN SPEC 66336 (OZG-Servicestandard, Nutzendenperspektive)
KPIs	3.6.1: Datum der letzten Nutzungsqualitätsbewertung 3.6.2: Bewertung der Effektivität im Erfassungszeitraum 3.6.3: Bewertung der Zufriedenheit im Erfassungszeitraum
Anwendungsbereich	Software, Dienstleistungen

3.7 Sicherheitsklassifizierung

Element	Beschreibung
Kriterium	Zuordnung der Anwendung zur Verschlusssachenstufe (offen, VS-NfD, VS-Vertraulich, Geheim, Streng Geheim) und Ableitung der entsprechenden Sicherheitsanforderungen.
Bewertungsfrage	Welche VS-Einstufung gilt für die in der Anwendung verarbeiteten Daten? Werden die daraus resultierenden Sicherheitsanforderungen (z. B. VS-NfD-konforme Infrastruktur) vollständig umgesetzt?
Mehrwert für die IT-Steuerung	Stellt sicher, dass die Sicherheitsmaßnahmen der Einstufung entsprechen. Identifiziert Anwendungen, bei denen die Infrastruktur nicht dem Schutzbedarf der verarbeiteten Daten genügt.
Quellen	BSI Verschlusssachenanweisung (VSA), ISO/IEC 25010:2023 (Merkmal 6: Sicherheit), BSI IT-Grundschutz ISMS.1
KPIs	-

Anwendungsbereich	Software, Dienstleistungen, Infrastruktur

3.8 Standardisierungs- und Architekturkonformität

Element	Beschreibung
Kriterium	Bewertung der Konformität mit OZG-Rahmenarchitektur, Standards des Deutschland-Stacks, Architekturrichtlinie des Bundes und DIN SPEC 66336, sowie der Erfassung der integrierten Basiskomponenten.
Bewertungsfrage	Entspricht die Anwendung den Vorgaben der OZG-Rahmenarchitektur und der Architekturrichtlinie des Bundes? Erfüllt sie den OZG-Servicestandard (DIN SPEC 66336)? Welche Basiskomponenten sind angebunden?
Mehrwert für die IT-Steuerung	Schafft Transparenz über den Standardisierungsgrad im Portfolio und identifiziert Anwendungen, die noch nicht die verbindlichen Architekturvorgaben, eine Voraussetzung für die weitere Digitalisierung, erfüllen.
Quellen	OZG-Rahmenarchitektur, Architekturrichtlinie des Bundes (ersetzt SAGA 5), DIN SPEC 66336, Föderale IT-Architekturrichtlinien V1, Deutschland-Stack
KPIs	siehe 3.4.1, 3.4.2, 3.4.3
Anwendungsbereich	Software, Infrastruktur, Dienstleistungen

4 Dimension: Betrieb

4.1 Vertragstypklassifizierung und -dokumentation (EVB-IT)

Element	Beschreibung
Kriterium	Zuordnung des zugehörigen Vertrags zu einem der 12 EVB-IT-Vertragstypen mit vollständiger Vertragsdokumentation (Vertragsformular, AGB, Muster).
Bewertungsfrage	Welcher EVB-IT-Vertragstyp liegt vor (Kauf, Überlassung Typ A/B, Cloud, Dienstleistung, Pflege, System, Erstellung, Systemlieferung, Rahmenvereinbarung)? Liegen alle zugehörigen Vertragsunterlagen vollständig vor?
Mehrwert für die IT-Steuerung	Schafft eine einheitliche vertragliche Klassifizierung über das gesamte Portfolio und stellt die Einhaltung der Vergabeanforderungen gemäß VV zu §55 BHO sicher. Ermöglicht die Identifikation fehlender oder unvollständiger Vertragsdokumentationen.
Quellen	EVB-IT 2.0 (12 Vertragstypen, verbindlich gemäß VV zu §55 BHO), UfAB 2018 (Version VI)
KPIs	-
Anwendungsbereich	Software, IT-Infrastruktur, Dienstleistungen

4.2 Lieferanten- und Wartungsdienstleister-Identifikation

Element	Beschreibung
Kriterium	Vollständige Dokumentation des primären Lieferanten (juristische Person, Kontakt) und des Wartungsdienstleisters (intern/extern) je Anwendung.
Bewertungsfrage	Wer ist der primäre Lieferant (vollständige juristische Bezeichnung, Ansprechpartner)? Wer erbringt die Wartung und den Support (intern oder externer Dienstleister)?
Mehrwert für die IT-Steuerung	Schafft ein zentrales Lieferantenregister und identifiziert Konzentrationsrisiken (z. B. übermäßige Abhängigkeit von einem einzelnen Anbieter). Unterstützt das strategische Lieferantenmanagement und die Verhandlungsposition.
Quellen	EVB-IT Vertragsanforderungen, ISO/IEC 19770-1:2017 (IT Asset Management), COBIT 2019 APO10 (Managed Vendors)
KPIs	-

Anwendungsbereich	Software, IT-Infrastruktur, Dienstleistungen

4.3 Vertragsdokumentationsvollständigkeit

Element	Beschreibung
Kriterium	Nachweis der Vollständigkeit aller vertraglichen Pflichtdokumente gemäß EVB-IT und UfAB, einschließlich Vertragslaufzeit und Kündigungsfristen.
Bewertungsfrage	Liegen alle EVB-IT-Pflichtdokumente vor (Vertragsformular, AGB, erforderliche Muster)? Wurden die UfAB-2018-Richtlinien bei der Beschaffung eingehalten? Wann läuft der Vertrag aus? Welche Kündigungsfristen gelten?
Mehrwert für die IT-Steuerung	Stellt die Vergabekonformität sicher und macht Vertragslaufzeiten portfolioweit sichtbar. Ermöglicht die rechtzeitige Planung von Vertragsverlängerungen oder Neuausschreibungen.
Quellen	EVB-IT 2.0, UfAB 2018, VV zu §55 BHO
KPIs	-
Anwendungsbereich	Software, IT-Infrastruktur, Dienstleistungen

4.4 Fachverantwortung und organisatorische Zuordnung

Element	Beschreibung
Kriterium	Eindeutige Zuordnung der Fachverantwortung (Ressort, Abteilung, Referat) und Dokumentation der Zuständigkeiten gemäß BSI ORP.1.
Bewertungsfrage	Welches Ressort bzw. welche Organisationseinheit ist fachlich verantwortlich für diese Anwendung? Sind die Zuständigkeiten gemäß BSI ORP.1 dokumentiert? Wer ist der benannte Anwendungsverantwortliche?
Mehrwert für die IT-Steuerung	Stellt sicher, dass jede Anwendung eine:n eindeutige:n Verantwortliche:n hat. Verhindert „verwaiste“ Anwendungen ohne klare Zuständigkeit — ein häufiges Risiko in großen Portfolios.
Quellen	BSI IT-Grundschutz ORP.1 (Organisation), ORP.4 (Identitäts- und Berechtigungsmanagement), ISO/IEC 38500:2024 (Prinzip: Verantwortlichkeit)
KPIs	4.4.1: Datum der letzten Änderung des oder der Anwendungsverantwortlichen
Anwendungsbereich	Software, IT-Infrastruktur, Dienstleistungen

4.5 IT-Service-Management-Prozessreife

Element	Beschreibung
Kriterium	Grad der Implementierung von IT-Service-Management-Prozessen gemäß ITIL 4 und/oder ISO/IEC 20000-1-Konformität.
Bewertungsfrage	Welche ITIL-4-Praktiken sind implementiert (Incident Management, Change Enablement, Asset Management)? Liegt ein ISO-20000-1-konformes Service-Management-System vor?
Mehrwert für die IT-Steuerung	Bewertet die betriebliche Reife je Anwendung und identifiziert solche ohne strukturiertes Service-Management — ein Indikator für erhöhte Betriebsrisiken und Ineffizienzen.
Quellen	ISO/IEC 20000-1:2018 (ITSM-Anforderungen, zertifizierbar), ITIL 4
KPIs	-
Anwendungsbereich	Software, Dienstleistungen

4.6 IT-Asset-Management-Konformität

Element	Beschreibung
Kriterium	Erfüllungsgrad der ISO/IEC-19770-1-Prozessbereiche (27 Bereiche).
Bewertungsfrage	Sind die Software-Asset-Informationen vollständig (SWID-Tags gemäß ISO 19770-2, Lizenzansprüche, Installationsnachweise)? Welcher SAM-Reifegrad (Tier 1–4) wurde erreicht?
Mehrwert für die IT-Steuerung	Schafft die Grundlage für eine verlässliche Lizenzverwaltung und reduziert das Risiko von Lizenzverstößen. Unterstützt die finanzielle Dimension durch akkurate Bestandsdaten.
Quellen	ISO/IEC 19770-1:2017 (IT Asset Management Systems, 27 Prozessbereiche, Tier-basiertes Reifegradmodell), ISO/IEC 19770-2 (SWID-Tags)
KPIs	-
Anwendungsbereich	Software, IT-Infrastruktur, Dienstleistungen

4.7 Governance-Struktur

Element	Beschreibung
Kriterium	Umsetzungsgrad der Governance-Ziele gemäß COBIT 2019 und/oder ISO/IEC 38500.
Bewertungsfrage	Welche COBIT-2019-Governance-Ziele werden für diese Anwendung umgesetzt (EDM01 Governance-Rahmen, APO09 Managed Service Agreements, BAI09 Managed Assets)? Ist die IT-Governance gemäß ISO 38500 etabliert?
Mehrwert für die IT-Steuerung	Stellt sicher, dass IT-Investitionen an den Zielen der Verwaltung ausgerichtet sind und die Governance-Anforderungen des Bundes erfüllt werden. Unterstützt die Rechenschaftspflicht gegenüber dem Bundesrechnungshof.
Quellen	COBIT 2019, ISO/IEC 38500:2024 (6 Governance-Prinzipien)
KPIs	4.7.1: Umsetzungsgrad der Governance Ziele (%)
Anwendungsbereich	Software, IT-Infrastruktur, Dienstleistungen

4.8 Vergabeprozesskonformität

Element	Beschreibung
Kriterium	Einhaltung der UfAB-2018-Vergabephasen (Planung, Gestaltung, Durchführung) und Vollständigkeit der Vergabedokumentation.
Bewertungsfrage	Wurden alle UfAB-Phasen durchlaufen (Bedarfsanalyse, Ausschreibungsphase, Bewertungsphase)? Ist die Vergabedokumentation vollständig und prüfungsfähig?
Mehrwert für die IT-Steuerung	Stellt die Vergabekonformität sicher und schafft Prüfungssicherheit gegenüber dem Bundesrechnungshof. Identifiziert Vergabeverfahren mit Dokumentationslücken.
Quellen	UfAB 2018 Version VI (649 Seiten), GWB Teil 4, VgV, UVgO, BHO §55
KPIs	-
Anwendungsbereich	Software, IT-Infrastruktur, Dienstleistungen

5 Dimension: Finanzen

Die finanzielle Dimension umfasst die Lizenzierung, die Kostenstruktur, das Geschäftsmodell, die Wirtschaftlichkeitsbetrachtung gemäß BHO, sowie die Kostenoptimierung. Sie bildet die Grundlage für eine haushaltskonforme und wirtschaftliche Steuerung des IT-Portfolios.

5.1 Lizenzvolumen und Kostenmanagement

Element	Beschreibung
Kriterium	Erfassung des Gesamtlizenzvolumens (Lizenzen/Nutzerplätze), der Kosten pro Lizenz/Nutzerplatz und der Auslastungsquote (aktive/gesamt × 100 %).
Bewertungsfrage	Wie viele Lizenzen bzw. Nutzerplätze sind vertraglich vereinbart? Was kostet eine einzelne Lizenz / ein Nutzerplatz? Wie hoch ist die tatsächliche Auslastungsquote (Anteil der aktiv genutzten Lizenzen)?
Mehrwert für die IT-Steuerung	Identifiziert Überlizenzierung und ungenutzte Lizenzen — ein typisches Einsparpotenzial von 15–30 % in großen IT-Portfolios. Schafft die Grundlage für eine bedarfsgerechte Lizenzplanung.
Quellen	ISO/IEC 19770-1:2017 (SAM-Prozesse), EVB-IT Vertragstypen (insb. EVB-IT Überlassung Typ A/B)
KPIs	5.1.1: Gesamtlizenzvolumens (Lizenzen/Nutzerplätze) 5.1.2: Kosten pro Lizenz/Nutzerplatz 5.1.3: Anzahl der aktiven Lizenzen und Nutzerplätze (zur Berechnung der Auslastungsquote: aktive/gesamt × 100)
Anwendungsbereich	Software, IT-Infrastruktur, Dienstleistungen

5.2 Vertragstyp und Geschäftsmodell

Element	Beschreibung
Kriterium	Zuordnung des EVB-IT-Vertragstyps mit finanziellen Implikationen und Klassifizierung des Geschäftsmodells (Kauf/Eigentum, Miete, As-a-Service).
Bewertungsfrage	Welcher EVB-IT-Vertragstyp mit welcher Finanzstruktur liegt vor (einmalige vs. periodische Zahlungen)? Handelt es sich um Kauf und Eigentum, Miete/Leasing oder ein As-a-Service-Modell (mit oder ohne Infrastruktur-Bundling)?

Mehrwert für die IT-Steuerung	Schafft Transparenz über die Finanzstruktur des Portfolios und unterstützt die strategische Steuerung der Beschaffungsmodelle.
Quellen	EVB-IT Kauf, Überlassung Typ A (dauerhaft), Typ B (periodisch), Cloud (Abo-Modell), Pflege S (Wartungsgebühren), Dienstleistung
KPIs	-
Anwendungsbereich	Software, IT-Infrastruktur, Dienstleistungen

5.3 Gesamtbetriebskosten (TCO) je Anwendung

Element	Beschreibung
Kriterium	Vollständige Erfassung der Lebenszykluskosten (Beschaffung, Betrieb, Wartung, Ablösung) je Anwendung gemäß WiBe-Methodik.
Bewertungsfrage	Wie hoch sind die initialen Beschaffungskosten? Wie hoch sind die jährlichen wiederkehrenden Kosten (Wartung, Support, Hosting)? Wie hoch sind die vollständigen Lebenszykluskosten?
Mehrwert für die IT-Steuerung	Ermöglicht den TCO-Vergleich über das gesamte Portfolio und identifiziert Anwendungen mit unverhältnismäßig hohen Betriebskosten als Kandidaten für Konsolidierung oder Migration.
Quellen	WiBe 5.0 (Kostenkomponenten), ISO/IEC 19770-1:2017 (Asset-Lebenszyklus), ITIL 4 Service Financial Management
KPIs	5.3.1: Beschaffungskosten 5.3.2: jährliche wiederkehrenden Kosten (Wartung, Support, Hosting) 5.3.3: vollständige Lebenszykluskosten
Anwendungsbereich	Software, Dienstleistungen

5.4 Wirtschaftlichkeitsbetrachtung (WiBe)

Element	Beschreibung
Kriterium	Durchführung und Dokumentation einer Wirtschaftlichkeitsbetrachtung gemäß §7 BHO nach der WiBe-5.0-Methodik, einschließlich Kapitalwertberechnung und qualitativem Nutzwert.

Bewertungsfrage	Wurde eine WiBe-Analyse gemäß §7 BHO durchgeführt? In welcher Phase befindet sie sich (V0/V1/V2/V3/Wirkbetrieb)? Wie hoch ist der berechnete Kapitalwert? Wurde der WiBe-Kalkulator 5.0 eingesetzt?
Mehrwert für die IT-Steuerung	Stellt die Einhaltung der BHO-Wirtschaftlichkeitsanforderungen sicher und schafft eine objektive Grundlage für Investitionsentscheidungen. Erforderlich für die Prüfung durch den Bundesrechnungshof.
Quellen	WiBe 5.0 (Kapitalwertmethode, Phasen V0–V3 und Wirkbetrieb), BHO §7 (Wirtschaftlichkeit und Sparsamkeit), WiBe-Kalkulator 5.0
KPIs	5.4.1: WiBe Phase 5.4.2: WiBe Kapitalwert
Anwendungsbereich	Software, IT-Infrastruktur, Dienstleistungen

5.5 Haushaltskonformität und Prognosegenauigkeit

Element	Beschreibung
Kriterium	Bewertung der Übereinstimmung von Budgetplanung und tatsächlichen Ausgaben sowie Konformität mit §34 BHO (Ausgabenbewirtschaftung).
Bewertungsfrage	Wie groß ist die Abweichung zwischen geplanten und tatsächlichen Ausgaben? Entspricht die Investition den BHO-Anforderungen (§7 Wirtschaftlichkeit, §34 Ausgabenbewirtschaftung)? Wurde die Mittelfreigabe ordnungsgemäß erteilt?
Mehrwert für die IT-Steuerung	Unterstützt die Haushaltsdisziplin und -planung. Identifiziert Anwendungen mit systematischen Kostenüberschreitungen und verbessert die Prognosegenauigkeit für zukünftige Haushaltsperioden.
Quellen	BHO §7 und §34, VV-BHO (Verwaltungsvorschriften zur BHO)
KPIs	5.5.1: Kosten über Plan im Erfassungszeitraum (+/- %)
Anwendungsbereich	Software, IT-Infrastruktur, Dienstleistungen

5.6 Kostenoptimierungspotenzial

Element	Beschreibung
Kriterium	Ermittlung von Einsparmöglichkeiten durch den Abbau von Überlizenzierung, „Rightsizing“ oder Vertragskonsolidierung.

Bewertungsfrage	Gibt es ungenutzte Lizenzen, die zurückgegeben werden können? Können Verträge konsolidiert werden?
Mehrwert für die IT-Steuerung	Identifiziert konkrete Einsparpotenziale im Portfolio. Unterstützt die datengestützte Priorisierung von Optimierungsmaßnahmen.
Quellen	FinOps Foundation (Effective Savings Rate, Unit Economics), ITIL 4 Service Financial Management, COBIT 2019 APO06 (Manage Budget and Costs)
KPIs	-
Anwendungsbereich	Software, IT-Infrastruktur, Dienstleistungen

5.7 Stückkosten und leistungsbezogene Verrechnung

Element	Beschreibung
Kriterium	Berechnung der Kosten pro Nutzendem, pro Transaktion und pro Funktion, einschließlich der Zuordnung von Gemeinkosten.
Bewertungsfrage	Wie hoch sind die Kosten pro Nutzendem bzw. pro Beschäftigtem? Wie hoch sind die Kosten pro Transaktion? Wie skalieren die Kosten mit steigender Nutzung? Was sind die wesentlichen Kostentreiber?
Mehrwert für die IT-Steuerung	Ermöglicht eine leistungsbezogene Kostenallokation und den Vergleich von Anwendungen gleicher Funktionalität. Unterstützt die Umstellung auf Showback-/Chargeback-Modelle.
Quellen	ITIL 4 Service Financial Management, FinOps Unit Economics, COBIT 2019 EDM02 (Value Optimization)
KPIs	5.7.1: Kosten pro Nutzendem (Durchschnitt über den Erfassungszeitraum) 5.7.2: Kosten pro Transaktion (Durchschnitt über den Erfassungszeitraum) 5.7.3: Kosten pro Funktion (Durchschnitt über den Erfassungszeitraum)
Anwendungsbereich	Software, Dienstleistungen

6 Dimension: Nachhaltigkeit

Die Nachhaltigkeitsdimension adressiert den Energieverbrauch, die CO_2-Emissionen, Um-we kennzahlen und Anforderungen an ressourceneffiziente Software und Infrastruktur. Sie gewinnt zunehmend an Bedeutung durch die Vorgaben der klimaneutralen Bundesverwaltung, die AVV Klima und das Energieeffizienzgesetz (EnEfG).

6.1 Gesamtenergieverbrauch

Element	Beschreibung
Kriterium	Messung des Gesamtenergieverbrauchs der Anwendung oder IT-Infrastruktur in kWh pro Jahr.
Bewertungsfrage	Kann der Anbieter gemessene Energieverbrauchsdaten für die Gesamtanwendung oder Infrastruktur vorlegen? Können diese Anhand von repräsentativen Nutzungsszenarien weiter detailliert werden? Welche Messmethode wurde angewendet?
Mehrwert für die IT-Steuerung	Schafft Transparenz über den Energieverbrauch im IT-Portfolio und ermöglicht die Identifikation energieintensiver Anwendungen. Unterstützt die Einhaltung des Energieeffizienzgesetzes (EnEfG).
Quellen	Blauer Engel DE-UZ 215 „Ressourcen- und energieeffiziente Softwareprodukte“ (Januar 2020), EnEfG (Energieeffizienzgesetz)
KPIs	6.1.1: Gesamtenergieverbrauch der Anwendung
Anwendungsbereich	Software, IT-Infrastruktur

6.2 Rechenzentrum Power Usage Effectiveness (PUE)

Element	Beschreibung
Kriterium	PUE-Wert des Rechenzentrums (PUE = Gesamtenergie Rechenzentrum / IT-Geräte-Energie) einschließlich der Messstufe (PUE0/PUE1/PUE2/PUE3).
Bewertungsfrage	Wie hoch ist der aktuelle PUE-Wert des Rechenzentrums? Auf welcher Messstufe (PUE1, PUE2, PUE3) gemäß ISO/IEC 30134-2 bzw. EN50600-4-2:2016 wird gemessen?
Mehrwert für die IT-Steuerung	Ermöglicht den Effizienzvergleich verschiedener Co-Location- oder Hosting-Standorte und unterstützt die Auswahl energieeffizienter Rechenzentren bei Neubeschaffungen oder Migrationen.

Quellen	ISO/IEC 30134-2:2016, EN 50600-4-2:2016, EU Energieeffizienzrichtlinie (EU) 2023/1791
KPIs	6.2.1: Durchschnittlicher operativer PUE-Wert aller Rechenzentren, die für die Bereitstellung der IT-Infrastruktur oder des Systems genutzt werden
Anwendungsbereich	Software, IT-Infrastruktur

6.3 Erneuerbare-Energien-Faktor (REF)

Element	Beschreibung
Kriterium	REF = Erneuerbare Energie / Gesamtenergie des Rechenzentrums; Zielwert 1,0 (100 % erneuerbare Energien).
Bewertungsfrage	Welcher Anteil der Energie des Rechenzentrums stammt aus erneuerbaren Quellen (REF-Wert)? Wird das Rechenzentrum zu 100 % mit erneuerbarer Energie betrieben?
Mehrwert für die IT-Steuerung	Unterstützt die Bewertung der Klimaneutralität der IT-Infrastruktur und die Auswahl von Anbietern mit hohem Anteil erneuerbarer Energien. Relevant für die Berichterstattung der klimaneutralen Bundesverwaltung.
Quellen	ISO/IEC 30134-3:2016, EN 50600-4-3:2016+A1:2019, EU-Energieeffizienz-richtlinie (EU) 2023/1791
KPIs	6.3.1: Durchschnittlicher operativer REF-Wert aller Rechenzentren, die für die Bereitstellung der IT-Infrastruktur oder des Systems genutzt werden
Anwendungsbereich	Software, IT-Infrastruktur

6.4 Energieverbrauch pro Nutzendem/Lizenz

Element	Beschreibung
Kriterium	Normierter Energieverbrauch: Gesamtenergie der Anwendung (kWh) / Anzahl aktiver Nutzenden oder Lizenzen.
Bewertungsfrage	Wie hoch ist der Energieverbrauch pro aktivem Nutzenden? Wie hat sich dieser Wert über die letzten drei Hauptversionen entwickelt?
Mehrwert für die IT-Steuerung	Ermöglicht den normalisierten Effizienzvergleich zwischen Anwendungen unterschiedlicher Größe und Nutzerzahl. Identifiziert Anwendungen mit über-

	durchschnittlichem Energieverbrauch pro Nutzendem als Optimierungskandidaten.
Quellen	Blauer Engel DE-UZ 215 (Normierungsanforderungen), ISO/IEC 21031:2024 (funktionale Einheit R)
KPIs	6.4.1: Energieverbrauch pro Lizenz oder Nutzendem (Durchschnitt, kWh)
Anwendungsbereich	Software, Dienstleistungen, IT-Infrastruktur

6.5 Ressourceneffizienz und Hardware-Langlebigkeit

Element	Beschreibung
Kriterium	Bewertung der Hardwareanforderungen, der Abwärtskompatibilität und der Modularität gemäß Blauer-Engel-Kriterien.
Bewertungsfrage	Welche Hardware-Mindestanforderungen bestehen? Kann die Software ohne Leistungseinbußen auf Hardware betrieben werden, die 3 Jahre und älter ist? Ist die Software modular aufgebaut und unterstützt sie Datenportabilität?
Mehrwert für die IT-Steuerung	Identifiziert Anwendungen, die vorzeitigen Hardwareersatz erzwingen und fördert die Auswahl ressourceneffizienter Software. Reduziert Hardwarekosten und elektronischen Abfall.
Quellen	Blauer Engel DE-UZ 215 (Kriterien: Abwärtskompatibilität, Modularität, Datenportabilität), AVV Klima (Klimafreundliche Beschaffung)
KPIs	-
Anwendungsbereich	Software, Dienstleistungen

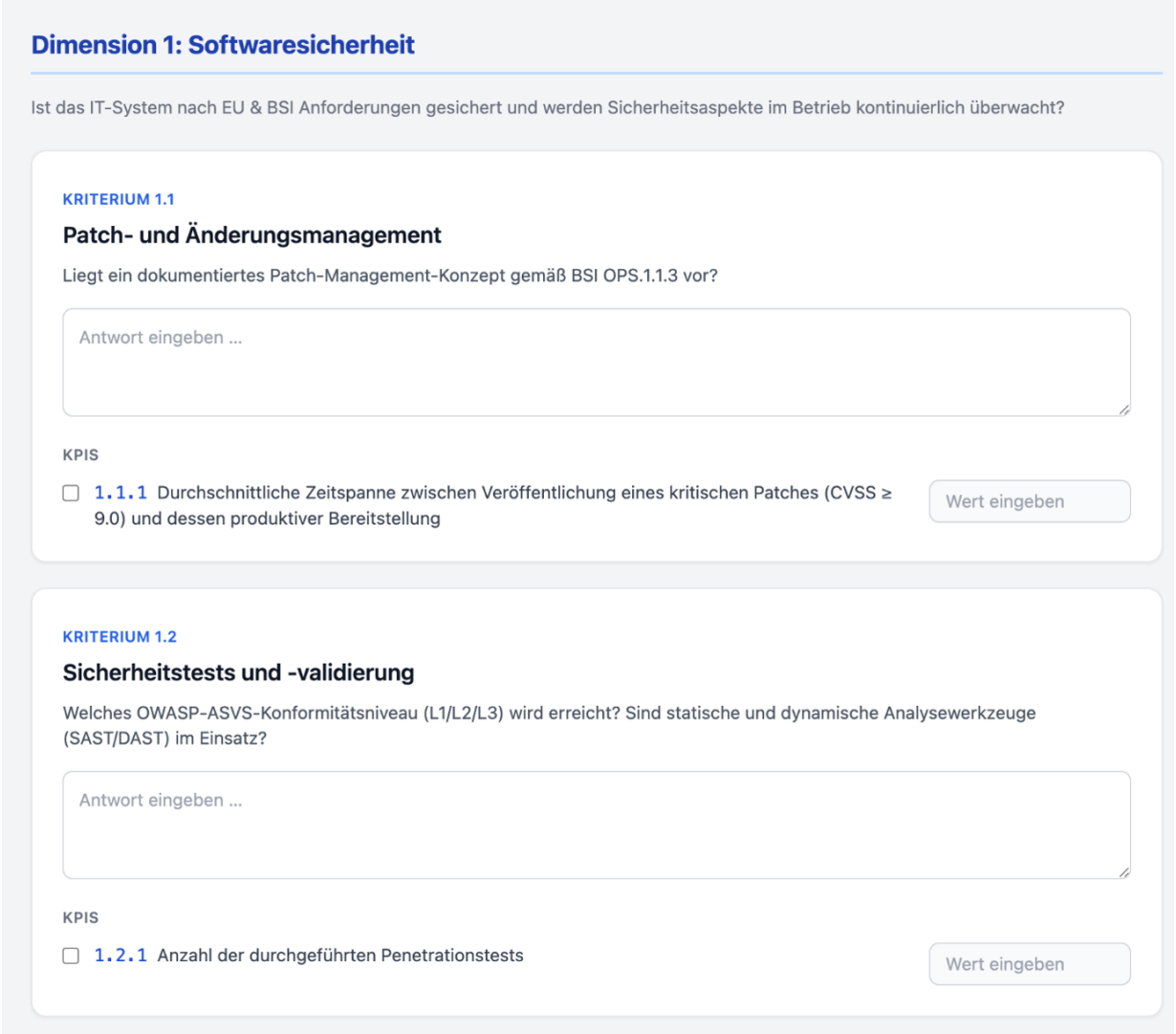
Illustrative Beispiele

Zustellung des Fragebogens an Lieferanten

Als Teil des Vertragswerks erhält der Lieferant einen Fragebogen, welcher den Anforderungen entsprechend konfiguriert werden kann. Dies kann als Teil der digitalen EVB-IT Vertragswerkzeuge angeboten werden.

Im Fragebogen werden sowohl qualitative Antworten auf die Kriterien als auch quantitative Kennzahlen für die automatisierte Bewertung erfasst.

Abbildung: Illustrative Darstellung des Ersterfassungsbogens

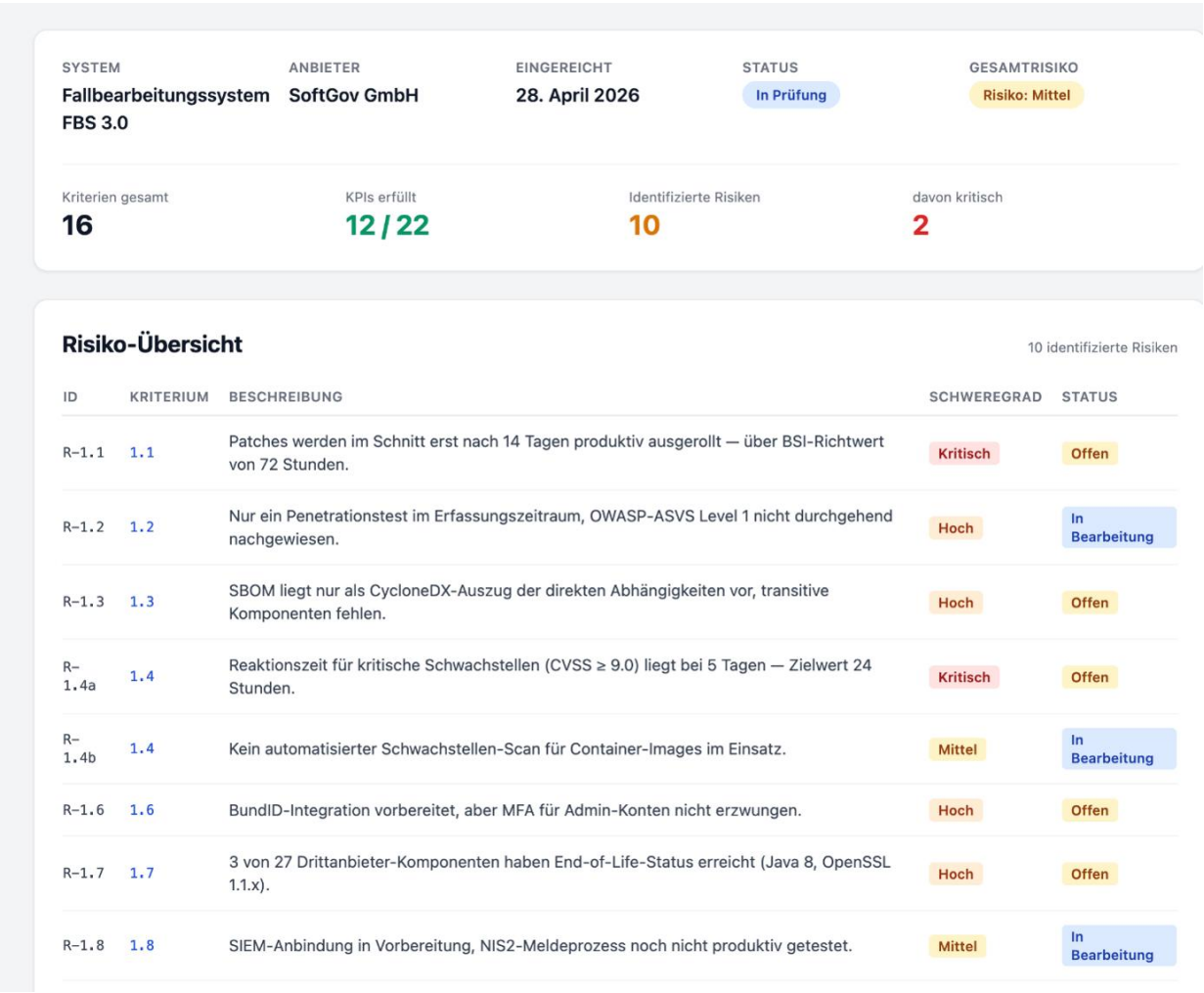


Quelle: Leitmotiv

Auswertung der Ersterfassung

Auf Basis der erfassten Informationen zur Beschaffung kann eine Bewertung, entweder mit Hilfe von automatisierten Werkzeugen oder manuell, vorgenommen werden. Über die Kenn-zahlen kann eine Zielabweichung einfach festgestellt werden.

Abbildung: Darstellung der Auswertung der Informationen aus der Ersterfassung



SYSTEM	ANBIETER	EINGEREICHT	STATUS	GESAMTRISIKO
Fallbearbeitungssystem FBS 3.0	SoftGov GmbH	28. April 2026	In Prüfung	Risiko: Mittel

Kriterien gesamt	KPIs erfüllt	Identifizierte Risiken	davon kritisch
16	12 / 22	10	2

Risiko-Übersicht — 10 identifizierte Risiken

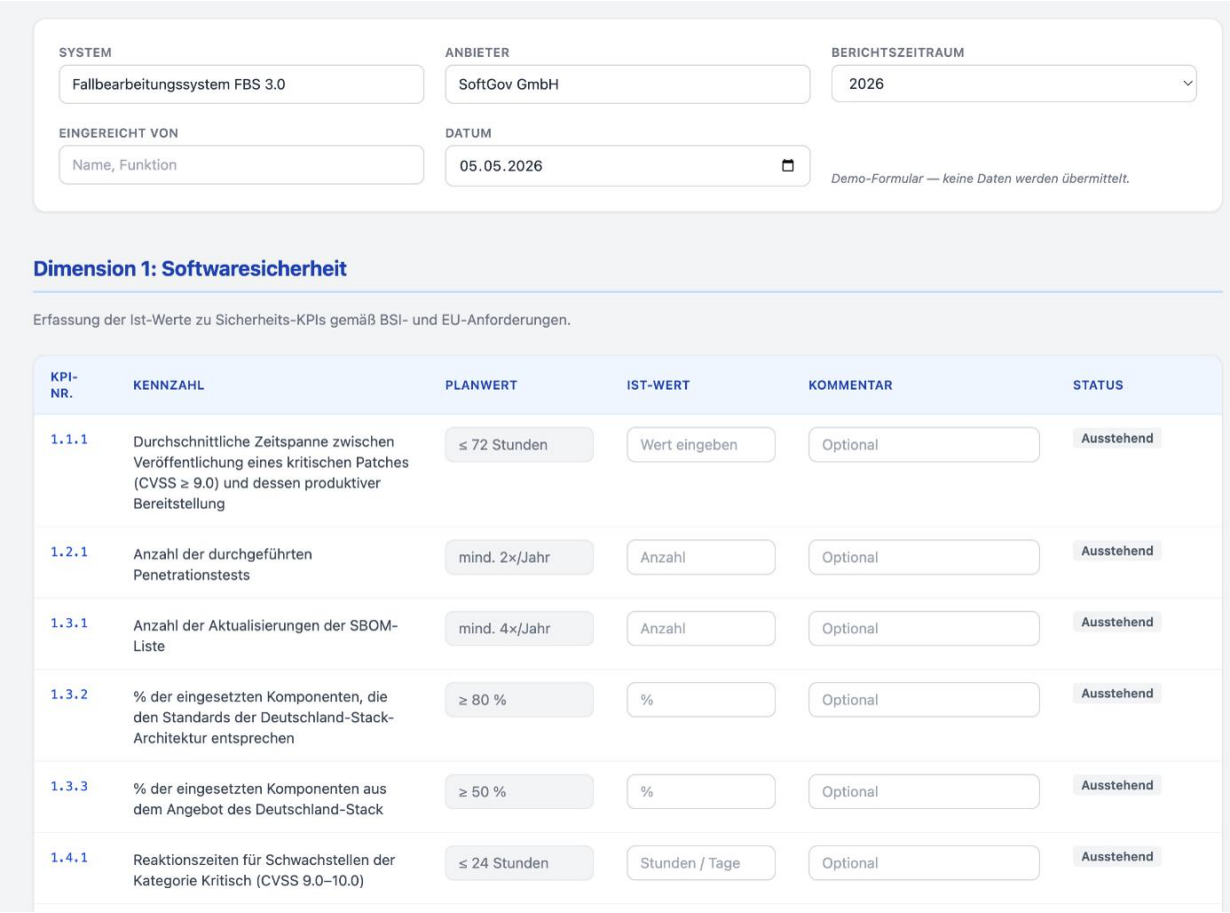
ID	KRITERIUM	BESCHREIBUNG	SCHWEREGRAD	STATUS
R-1.1	1.1	Patches werden im Schnitt erst nach 14 Tagen produktiv ausgerollt — über BSI-Richtwert von 72 Stunden.	Kritisch	Offen
R-1.2	1.2	Nur ein Penetrationstest im Erfassungszeitraum, OWASP-ASVS Level 1 nicht durchgehend nachgewiesen.	Hoch	In Bearbeitung
R-1.3	1.3	SBOM liegt nur als CycloneDX-Auszug der direkten Abhängigkeiten vor, transitive Komponenten fehlen.	Hoch	Offen
R-1.4a	1.4	Reaktionszeit für kritische Schwachstellen (CVSS ≥ 9.0) liegt bei 5 Tagen — Zielwert 24 Stunden.	Kritisch	Offen
R-1.4b	1.4	Kein automatisierter Schwachstellen-Scan für Container-Images im Einsatz.	Mittel	In Bearbeitung
R-1.6	1.6	BundID-Integration vorbereitet, aber MFA für Admin-Konten nicht erzwungen.	Hoch	Offen
R-1.7	1.7	3 von 27 Drittanbieter-Komponenten haben End-of-Life-Status erreicht (Java 8, OpenSSL 1.1.x).	Hoch	Offen
R-1.8	1.8	SIEM-Anbindung in Vorbereitung, NIS2-Meldeprozess noch nicht produktiv getestet.	Mittel	In Bearbeitung

Quelle: Leitmotiv

Jährlicher Erfassungsbogen

Für das Vertragsmanagement wird den Zulieferern jährlich ein Erfassungsbogen zugestellt. Dieser umfasst ausschließlich die quantitativen Werte für die Kennzahlen, um eine mögliche Zielabweichung festzustellen. Die zu erreichenden Werte werden bei Vertragsabschluss mit dem Lieferanten festgelegt.

Abbildung: Monitoring Fragebogen, Illustrative Darstellung der jährlichen Erfassung der Kennzahlen für das Vertragsmanagement



SYSTEM: Fallbearbeitungssystem FBS 3.0
ANBIETER: SoftGov GmbH
BERICHTSZEITRAUM: 2026
EINGEREICHT VON: Name, Funktion
DATUM: 05.05.2026
Demo-Formular — keine Daten werden übermittelt.

Dimension 1: Softwaresicherheit

Erfassung der Ist-Werte zu Sicherheits-KPIs gemäß BSI- und EU-Anforderungen.

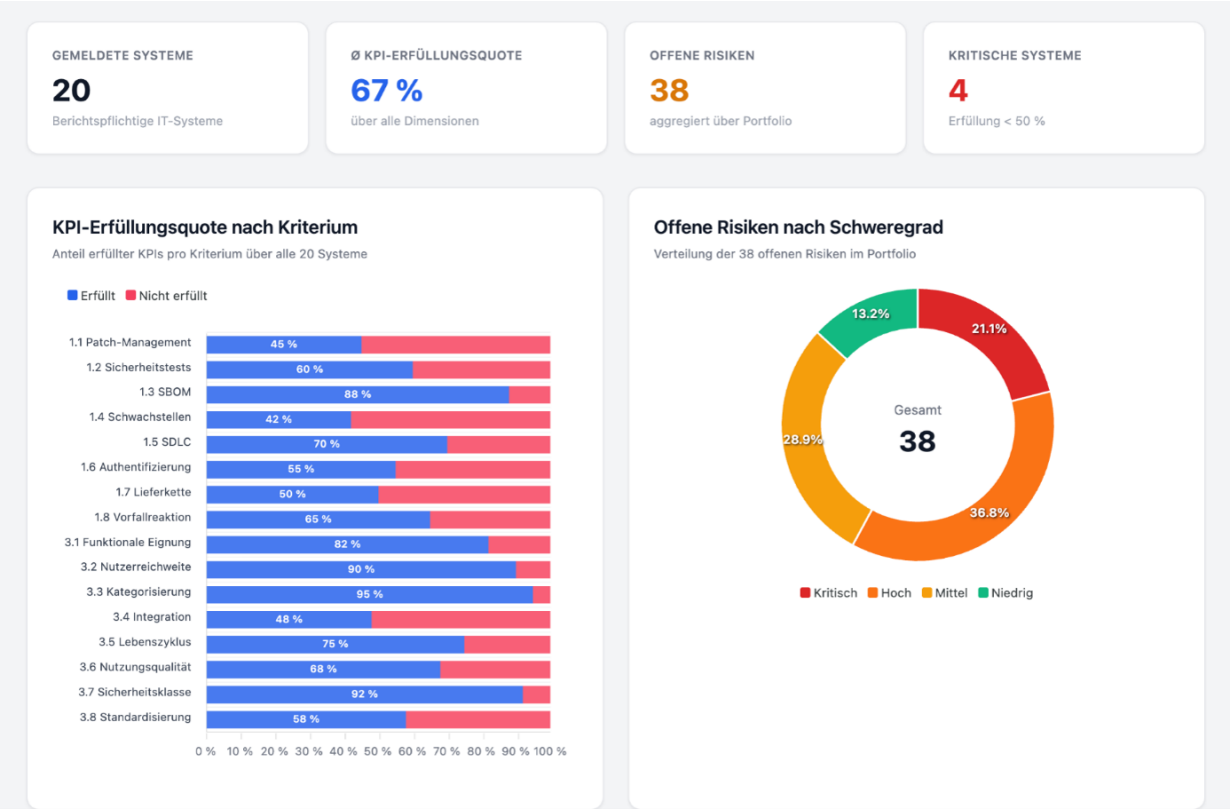
KPI-NR.	KENNZAHL	PLANWERT	IST-WERT	KOMMENTAR	STATUS
1.1.1	Durchschnittliche Zeitspanne zwischen Veröffentlichung eines kritischen Patches (CVSS ≥ 9.0) und dessen produktiver Bereitstellung	≤ 72 Stunden	Wert eingeben	Optional	Ausstehend
1.2.1	Anzahl der durchgeführten Penetrationstests	mind. 2×/Jahr	Anzahl	Optional	Ausstehend
1.3.1	Anzahl der Aktualisierungen der SBOM-Liste	mind. 4×/Jahr	Anzahl	Optional	Ausstehend
1.3.2	% der eingesetzten Komponenten, die den Standards der Deutschland-Stack-Architektur entsprechen	≥ 80 %	%	Optional	Ausstehend
1.3.3	% der eingesetzten Komponenten aus dem Angebot des Deutschland-Stack	≥ 50 %	%	Optional	Ausstehend
1.4.1	Reaktionszeiten für Schwachstellen der Kategorie Kritisch (CVSS 9.0–10.0)	≤ 24 Stunden	Stunden / Tage	Optional	Ausstehend

Quelle: Leitmotiv

Auswertung der Berichte

Durch die Erfassung quantitativer Kennzahlen wird zudem die Möglichkeit geschaffen ein „KPI-Dashboard“ für die Beschaffung und das Controlling bereitzustellen. Damit werden Vetragsabweichungen über das gesamte Portfolio sichtbar gemacht.

Abbildung: Illustrative Darstellung des Monitoring-Dashboards für das Vertragsmanagement



Quelle: Leitmotiv

Anhang A: Übersicht relevanter Standards, Normen und Regulierungen

A.1 BSI und deutsche Standards (Priorität 1)

BSI IT-Grundschutz Kompendium (Edition 2023)

- **ISMS:** ISMS.1 Sicherheitsmanagement
- **ORP (Organisation und Personal):** ORP.1 Organisation, ORP.2 Personal, ORP.3 Sensibilisierung und Schulung, ORP.4 Identitäts- und Berechtigungsmanagement, ORP.5 Compliance Management
- **CON (Konzepte):** CON.1 Kryptokonzept, CON.2 Datenschutz, CON.3 Datensicherungskonzept, CON.6 Löschen und Vernichten, CON.7 Informationssicherheit auf Auslandsreisen, CON.8 Software-Entwicklung, CON.10 Entwicklung von Webanwendungen, CON.11 Geheimschutz
- **OPS (Betrieb):** OPS.1.1.1 Allgemeiner IT-Betrieb, OPS.1.1.2 Ordnungsgemäße IT-Administration, OPS.1.1.3 Patch- und Änderungsmanagement, OPS.1.1.4 Schutz vor Schadprogrammen, OPS.1.1.5 Protokollierung, OPS.1.1.6 Software-Tests und Freigaben, OPS.1.1.7 Systemmanagement, OPS.1.2.2 Archivierung, OPS.1.2.4 Telearbeit, OPS.1.2.5 Fernwartung, OPS.1.2.6 NTP-Zeitsynchronisation, OPS.2.2 Cloud-Nutzung, OPS.2.3 Nutzung von Outsourcing, OPS.3.2 Anbieten von Outsourcing
- **APP (Anwendungen):** APP.2.1–2 (Verzeichnisdienste), APP.5.2–4 (Exchange, UCC), APP.6 Allgemeine Software
- **SYS (Systeme):** SYS.1–4 (Server, Clients, Mobile, Peripherie — 29 Bausteine)
- **IND (Industrielle IT):** IND.1–3 (Industrielle Steuerungssysteme)
- **INF (Infrastruktur):** INF.1 Allgemeines Gebäude, INF.2 Rechenzentrum sowie Serverraum, INF.5–14 (Arbeitsplätze, Verkabelung etc.)
- **DER (Detektion und Reaktion):** DER.1 Detektion von sicherheitsrelevanten Ereig-nissen, DER.2.1 Behandlung von Sicherheitsvorfällen, DER.4 Notfallmanagement

BSI Technische Richtlinien

- **BSI TR-03183-1 (v0.10.0):** Cyber-Resilienz — Allgemeine Anforderungen
- **BSI TR-03183-2 (v2.1.0, September 2024):** Software Bill of Materials (SBOM)
- **BSI TR-03183-3 (v1.0.0, September 2024):** Schwachstellenberichte und -meldungen
- **BSI C5:2020:** Cloud Computing Compliance Criteria Catalogue (121 Kriterien, 17 Themenbereiche)
- **BSI C5:2026 (in Vorbereitung):** 168 Kriterien

Beschaffungs- und Governance-Standards des Bundes

- **EVB-IT 2.0:** 12 Vertragstypen (Kauf, Überlassung Typ A/B, Systemlieferung, System, Dienstleistung, Erstellung, Wartung/Pflege, Cloud, Rahmenvereinbarung) — verbindlich gemäß VV zu §55 BHO
- **UfAB 2018 (Version VI, April 2018):** Unterlage für Ausschreibung und Bewertung von IT-Leistungen
- **WiBe 5.0:** Wirtschaftlichkeitsbetrachtungen gemäß §7 BHO (Kapitalwertmethode, Phasen V0–V3 und Wirkbetrieb); WiBe-Kalkulator 5.0
- **BHO (Bundeshaushaltsordnung):** §7 (Wirtschaftlichkeit und Sparsamkeit), §34 (Ausgabenbewirtschaftung), §55 (Vergabe)
- **VV-BHO:** Verwaltungsvorschriften zur BHO

IT-Architektur des Bundes

- **Deutschland-Stack:** Zielbild, Standards und Referenzarchitektur, 2025, https://deutschland-stack.gov.de/gesamtbild/
- **OZG-Rahmenarchitektur:** Zielbild IT-Planungsrat
- **IT-Architekturrichtlinie des Bundes:** Ersetzt SAGA 5, verbindlich für die Bundesverwaltung
- **Föderale IT-Architekturrichtlinien V1:** Bund-Länder-Kooperationsrichtlinien (FIT-AB)
- **DIN SPEC 66336:** OZG-Servicestandard für digitale Verwaltungsleistungen

Deutsche Umwelt- und Nachhaltigkeitsstandards

- **Blauer Engel DE-UZ 215 (Januar 2020):** „Umweltzeichen für ressourcen- und energieeffiziente Softwareprodukte“ (RAL gGmbH/UBA)
- **AVV Klima (19. Oktober 2021):** Allgemeine Verwaltungsvorschrift zur Beschaffung klimafreundlicher Leistungen
- **EnEfG (Energieeffizienzgesetz):** Anforderungen an Rechenzentren

A.2 EU-Standards und -Verordnungen

Cybersicherheits-Rahmenwerk der EU

- **NIS2-Richtlinie (EU) 2022/2555:** Netz- und Informationssicherheit; deutsche Umsetzung NIS2UmsuCG (Dezember 2025)
- **DORA-Verordnung (EU) 2022/2554:** Digital Operational Resilience Act (anwendbar seit 17. Januar 2025)
- **EU Cybersecurity Act — Verordnung (EU) 2019/881:** Rahmenwerk für EUCS-Zertifizierung

- **EUCC:** EU Common Criteria-basiertes Zertifizierungsschema
- **DSGVO — Verordnung (EU) 2016/679:** Insbesondere Art. 25 (Datenschutz durch Technikgestaltung), Art. 28 (Auftragsverarbeiter), Art. 32 (Sicherheit der Verarbei-tung), Art. 35 (Datenschutz-Folgenabschätzung), Art. 44–50 (Datenübermittlung)

EU-Datengovernance

- **EU Data Act** — Verordnung (EU) 2023/2854: Anwendung ab 12. September 2025
- **Data Governance Act — Verordnung (EU) 2022/868:** Anwendung seit 24. September 2023
- **EU Cyber Resilience Act (CRA):** SBOM-Anforderungen ab September 2026 (vollständige Anwendung ab Dezember 2027)

EU-Umwelt und Nachhaltigkeit

- **Energieeffizienzrichtlinie (EU) 2023/1791:** Berichtspflichten für Rechenzentren

Europäische Rechenzentrumsnormen — EN 50600-Reihe

- **EN 50600-1:2019:** Allgemeine Konzepte (Verfügbarkeitsklassen 1–4)
- **EN 50600-2-Reihe:** Infrastruktur (2-1 Gebäude, 2-2 Stromversorgung, 2-3 Umgebungsbedingungen, 2-4 Verkabelung, 2-5 Sicherheitssysteme)
- **EN 50600-3-1:** Management und Betriebsinformation
- **EN 50600-4-Reihe:** Leistungskennzahlen (4-1 Übersicht, 4-2 PUE, 4-3 REF, 4-6 ERF, 4-7 CER, 4-8 CUE, 4-9 WUE)
- **EN 50600-5-1:2023:** Reifegradmodell für Energiemanagement und ökologische Nachhaltigkeit

Europäische Interoperabilität und Barrierefreiheit

- **European Interoperability Framework (EIF):** COM(2017)134 Anhang II
- **European Accessibility Act — Richtlinie (EU) 2019/882:** Unter Einbeziehung von EN 301 549 und WCAG 2.1 Level AA

A.3 Internationale ISO/IEC-Standards (Priorität 3)

ISO/IEC 27000-Reihe — Informationssicherheit

- **27000:2018:** Überblick und Begriffe
- **27001:2022:** ISMS-Anforderungen (93 Kontrollen; Übergang bis Oktober 2025)
- **27002:2022:** Informationssicherheitsmaßnahmen
- **27003:2017:** ISMS-Implementierungsleitfaden

- **27004:2016:** Überwachung und Messung
- **27005:2022:** Risikomanagement
- **27006/27007**:2020: Zertifizierungsstellen und Auditleitfaden
- **27013/27014:** Integration mit ISO 20000-1; Governance
- **27017:2015:** Cloud-Sicherheitsmaßnahmen
- **27018:2019:** Schutz personenbezogener Daten in öffentlichen Clouds (24 Kontrollen)
- **27031:2011:** ICT-Notfallvorsorge
- **27032:2012:** Cybersicherheitsleitfaden
- **27033 (Teile 1–7):** Netzwerksicherheit
- **27034:** Anwendungssicherheit
- **27035:** Vorfallmanagement
- **27701:2019:** Datenschutz-Informationsmanagement (PIMS)

ISO/IEC 15408 — Common Criteria

- Evaluationskriterien für IT-Sicherheit (EAL1–EAL7)

ISO/IEC 25000-Reihe — SQuaRE (Software-Qualität)

- **25000:2014:** Leitfaden zu SQuaRE
- **25010:2023:** Qualitätsmodelle (9 Produktqualitätsmerkmale einschl. neuem Merk-mal „Safety“; 5 Nutzungsqualitätsmerkmale)
- **25023:** Qualitätsmessung
- **25040:2024:** Evaluierungsprozess (5-Stufen-Rahmenwerk, veröffentlicht September 2024)

ISO/IEC 20000-Reihe — IT-Service-Management

- **20000-1:2018:** SMS-Anforderungen (zertifizierbar)
- **20000-2:2019:** Anwendungsleitfaden
- **20000-3:2019:** Festlegung des Geltungsbereichs
- **TS 20000-11:2021:** Verhältnis zu ITIL 4

ISO/IEC 19770-Reihe — IT-Asset-Management

- **19770-1:2017:** ITAM-Systemanforderungen (27 Prozessbereiche, Tier 1–4 Reifegrad)
- **19770-2:** Software-Identifikation (SWID) Tags
- **19770-3:** Lizenzanspruchsschema
- **19770-4:** Ressourcennutzung

- **19770-5:2015:** Überblick und Begriffe

ISO/IEC 38500 — IT-Governance

- **38500:2024 (3. Ausgabe):** Governance der IT für die Organisation (6 Prinzipien: Verantwortlichkeit, Strategie, Beschaffung, Leistung, Konformität, Menschliches Verhalten)

ISO/IEC 12207 — Software-Lebenszyklus

- **ISO/IEC/IEEE 12207:2017:** Software-Lebenszyklusprozesse (30 Prozesse in 4 Gruppen)
- **ISO/IEC/IEEE 15288:2015:** System-Lebenszyklusprozesse (harmonisiert mit 12207)

ISO/IEC 30134-Reihe — Rechenzentrums-Leistungskennzahlen

- **30134-1:2016:** Überblick
- **30134-2:2016:** Power Usage Effectiveness (PUE) — aktualisiert
- **30134-3:2016:** Renewable Energy Factor (REF)
- **30134-4:2017:** ITEEsv (Server-Energieeffizienz)
- **30134-5:2017:** ITEUsv (Serverauslastung)
- **30134-6:2016:** Energy Reuse Factor (ERF)
- **30134-7:** Cooling Efficiency Ratio (CER)
- **30134-8:** Carbon Usage Effectiveness (CUE)
- **30134-9:** Water Usage Effectiveness (WUE)

ISO/IEC 22237-Reihe

- Internationales Pendant zu EN 50600 (Rechenzentrumseinrichtungen und -infrastrukturen)

ISO Umwelt- und Energiestandards

- **ISO 14001:**2015 (Aktualisierung 2026): Umweltmanagementsysteme
- **ISO 50001:2018:** Energiemanagementsystemen
- **ISO 50002-Reihe (2025):** Energieaudits (Teil 1–3)

ISO Qualitäts- und Risikomanagement

- **ISO 9001:2015:** Qualitätsmanagementsysteme
- **ISO 22301:2019:** Business Continuity Management
- **ISO 31000:2018:** Risikomanagement
- **ISO 55001:2014:** Asset Management

A.4 Bewährte Rahmenwerke aus der Praxis (Priorität 4)

1. COBIT 2019 - ISACA-Rahmenwerk: 40 Governance- und Management-Ziele; 6 Governance-Prinzipien; Design-Faktoren
2. ITIL 4 - Axelos-Rahmenwerk: Service Value System; Service Value Chain; 34 Management-Praktiken (14 allgemeine, 17 Service-, 3 technische); 4 Dimensionen; 7 Leitprinzipien
3. TOGAF 10 (2022) Architecture Development Method (ADM); 4 Architekturdomänen (Business, Anwendung, Daten, Technologie); Enterprise Architecture Content Frame-work
4. FinOps Foundation: Cloud Financial Management: 6 Prinzipien, 3 Phasen (Inform-Optimize-Operate); KPIs einschließlich Effective Savings Rate, Unit Economics, Tagging-Abdeckung

Ansprechperson bei der Agora Digitale Transformation

Dr. Stefan Heumann
Geschäftsführer
stefan.heumann@agoradigital.de

Agora Digitale Transformation

www.agoradigital.de