DEUTSCHE VERWALTUNGSCLOUD
EIN PRODUKT DES IT-PLANUNGSRATS

Version 0.9
12.02.2025

Handreichung zum Reifegradmodell für Kunden

Alle Produkte des IT-Planungsrats werden von der FITKO (Föderale IT-Kooperation) gesteuert. Diese Aufgabe erfüllt sie im Auftrag des IT-Planungsrats.

DEUTSCHE VERWALTUNGSCLOUD
EIN PRODUKT DES IT-PLANUNGSRATS

Inhaltsverzeichnis

1 Zweck des Dokuments

Das vorliegende Dokument dient dem besseren Verständnis und Handhabung des DVC Reifegradmodells aus der Kundenperspektive. Es erklärt, wie das DVC Reifegradmodell zu interpretieren ist und welche Bedeutung die einzelnen Bestandteile haben. Zudem zeigt es, wie die verschiedenen Reifegrade genutzt werden können, um anhand der individuellen Kundenanforderungen einen geeigneten Service zu identifizieren.
Dieses Dokument beginnt mit der Erklärung, wie ein konkretes Ergebnis der Reifegradeinschätzung zu interpretieren ist. Kapitel 3 und 4 gehen auf die einzelnen Bestandteile und deren Bedeutung ein. Zuletzt geben wir einen Ausblick über mögliche zukünftige Anpassungen des Reifegradmodells.

2 Wie ist das Reifegradmodell zu interpretieren?

Ziel des Reifegradmodells ist, Interessenten einen einfachen Überblick über den Stand des jeweiligen Services und der anbietenden Organisation hinsichtlich der DVC-Kriterien zu bieten. Die Reifegradprüfung basiert auf Selbstauskünften der Service-Anbieter. Die Service-Anbieter bestätigen die Korrektheit ihrer Angaben. Diese Selbstauskünfte werden von Experten der DVC plausibilisiert und stichprobenartig geprüft. Die erreichten Reifegrade und Stufen während der Reifegradprüfung werden von Seiten der DVC nicht bewertet. Der Ergebnisbericht der Reifegradprüfung wird nach Freigabe durch die Service-Anbieter mit dem jeweiligen Service auf dem Cloud Service-Portal veröffentlicht und ist auch Bestandteil der Serviceunterlagen bei einer Bestellung.
Die Entscheidung, welche Stufe in den jeweiligen Kriterien Ihren Anforderungen entspricht, liegt bei Ihnen. Es gilt zu bedenken, dass eine höhere Stufe oft auch mit höheren Kosten verbunden ist und deshalb nicht für alle Anforderungen immer die höchste Stufe benötigt wird. Prüfen Sie hierfür anhand der Stufen und Reifegrade, ab wann Ihre Anforderungen erfüllt sind, und suchen Sie dann dementsprechend passende Services.
Alle im DVC-Cloud-Serviceportal angebotenen Services erfüllen mindestens ein definiertes Set an Minimalkriterien:

Kriterium DVC Stufenmodell	Beschreibung Minimalkriterium	Minimal-kriterium
Neuer Programmstand	Neue Programmstände werden eine angemessene Zeit im Voraus inkl. Zeitpunkt und Dauer des geplanten Wartungsfensters angekündigt. (In sicherheitsrelevanten Notfällen ist die angemessene Zeit deutlich reduziert. Eine Ankündigung muss dennoch erfolgen).	✓
Mandantentrennung	Der Service unterstützt eine nach aktuellem Stand der Technik sichere Art der Mandantentrennung.	✓
Bestellprozess	Der Service ist im Self-Service bestellbar.	✓
Störung	Für den Service existieren dedizierte Kanäle zur strukturierten Annahme von Störungen.	✓
Benutzerdokumentation	Eine Benutzer-Dokumentation für alle wesentlichen Funktionen ist vorhanden und für Kunden des CSP online verfügbar.	✓
Transport-Verschlüsselung	Alle Verbindungen zum Service sind gemäß BSI TR-02102 transportverschlüsselt.	✓
Backups	Im Service erfolgt ein regelmäßiges Backup der Kundendaten (inkl. Disaster Recovery).	✓
Authentisierung	Der Service besitzt ein Authentisierungsverfahren.	✓
Autorisierung	Der Service besitzt ein Autorisierungsverfahren.	✓
Datenschutz	Der Service ist DSGVO-konform.	✓
Leistungsort	Die Speicherung und sonstige Verarbeitung von Daten des Kunden (einschließlich Metadaten) erfolgt ausschließlich innerhalb der EU und des EWR sowie der Schweiz.	✓

Abbildung 1

2.1 Methodik der Stufen im DVC-Stufenmodell

Die verschiedenen Reifegrade sind nicht mathematisch und nicht untereinander vergleichbar. Das bedeutet, dass eine Aggregation der Werte zu einer Gesamtstufe nicht möglich ist. Eine Aggregation würde voraussetzen, dass alle Abstufungen in etwa gleich schwer und gleich aufwändig sind. Dies ist im vorliegenden Reifegradmodell nicht gegeben, die einzelnen Kriterien stehen für sich. Auch sind die einzelnen Stufen nicht zwischen mehreren Kriterien vergleichbar. Auf eine Aggregation auf einen Gesamtwert, etwa im Sinne eines Durchschnittswerts über alle Kriterien wurde bewusst verzichtet, da die Kriterien für sich stehen und ein niedriger Wert in der einen Kategorie (z.B. Programmversion) nicht mit einem höheren Wert in einer anderen Kategorie (z.B. Verfügbarkeit) kompensiert werden kann.

3 Bestandteile des Reifegradmodells

3.1 Reifegrad des Service

Das Reifegradmodell besteht aus zwei Komponenten: Das DVC-Stufenmodell und den HV-Benchmark kompakt (HVB-kompakt) (alternativ DVC-Erweiterungsmodul). Das DVC-Stufenmodel ist eine Selbsteinschätzung, welche sich auf den Reifegrad eines Services bezieht. Der HVB-kompakt ist ein vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickeltes Reifegradmodell, welches die Organisation genauer betrachtet. Der HVB-kompakt ist zudem gesetzlich verpflichtend für IT-Dienstleistungen für die Bundesverwaltung. Im Rahmen der gesetzlichen Verpflichtung gelten für die Bundesverwaltung Mindestpotenzialstufen im HVV-kompakt. Diese finden im DVC-Kontext keine Anwendung, die Einschätzung, welche Stufe ausreichend ist, liegt auf der Kundenseite.

Bis auf weiteres gibt es die Möglichkeit, als Alternative zum HVB-kompakt eine abgespeckte Version auszufüllen – das sogenannte DVC-Erweiterungsmodul.

3.2 DVC-Stufenmodell: Reifegrad des Service

Die Kriterien des DVC-Stufenmodells dienen der Reifegradbestimmung von Services und betrachten die Dimensionen Funktionelles, Abrechnung, Service & Support, Informationssicherheit & Datenschutz sowie Digitale Souveränität. Da sich die Kriterien immer auf einen konkreten Cloud-Service beziehen, wird hier nicht von einem Reifegradmodell gesprochen, sondern von einem Stufenmodell. Das DVC-Stufenmodell dient dazu, einzelne Services vergleichbar zu machen. Je nach Anwendungsfall müssen dabei nicht alle Kriterien bis auf die höchste Stufe ausgebaut werden. Die Kriterienstufen können aber eine Orientierung für die Ausbauplanung für einzelne Cloud-Services bieten.

3.3 Erweiterungsfragen

Die Erweiterungsfragen dienen der Einschätzung der Organisation des Service-Anbieters. Diese repräsentieren einen Ausschnitt aus dem HVB-kompakt und wurden vor allem zur Aufwandsreduktion eingeführt. Den gesamten HVB-kompakt durchzuführen, ist mit hohen Aufwänden verbunden – wird aber dennoch von Seiten der DVC empfohlen. Anbieter können aber die Aufwände des Onboarding-Prozesses optimieren und zunächst mit den Erweiterungsfragen beginnen. Später werden diese dann zur vollständigen Beantwortung des HVB-kompakts wiederverwendet.

3.4 HV-Benchmark Kompakt – Reifegrad der Organisation

Die Einschätzung der Organisation erfolgt nach dem Hochverfügbarkeits-Benchmark kompakt (HVB-kompakt). Verwendet wird der HVB-kompakt 5.0 in der aktuellen Version 2.0 vom 29.11.2023. Der HVB-kompakt ist ein Bewertungsschema zur Ermittlung des Informationssicherheitsniveaus von IT-Dienstleistungen und Rechenzentren. Der HVB-kompakt ist eine komprimierte Version des HV-Benchmarks (HVB). Der HVB-kompakt verwendet gegenüber dem vollständigen HVB eine leicht modifizierte Methodik und ist um Revisionselemente ergänzt. Mittels eines modular aufgebauten Bewertungsschemas von relevanten Aspekten, sogenannten Indikatoren, und unter Nutzung eines Reifegradmodells kann die Verlässlichkeit einer zu betrachtenden IT-Dienstleistung oder eines Rechenzentrums relativ einfach gemessen und bewertet werden.

Hinweis: Ihre Verpflichtungen

In DVC-Stufenmodell finden Sie auch Stufen zu gesetzlichen Verpflichtungen wie z.B. Barrierefreiheit und der Datenschutzgrundverordnung. Auch wenn Sie hier einen Überblick erhalten, welche Stufe der Anbieter bereits erfüllt, entbindet Sie dies ausdrücklich nicht von Ihrer Sorgfaltspflicht sowie Ihrer gesetzlichen Prüf- und Auditierungspflicht.

4 Beschreibung der Dimensionen des DVC-Stufenmodells

In den nachfolgenden Abschnitten erhalten Sie einen Überblick über die einzelnen Dimensionen des DVC-Stufenmodells sowie der darin enthaltenen Kriterien. Für eine Übersicht über die einzelnen Kriterienstufen werfen Sie bitte einen Blick in das DVC-Stufenmodell unter https://deutsche-verwaltungscloud.de/Informationen/Reifegradmodell/

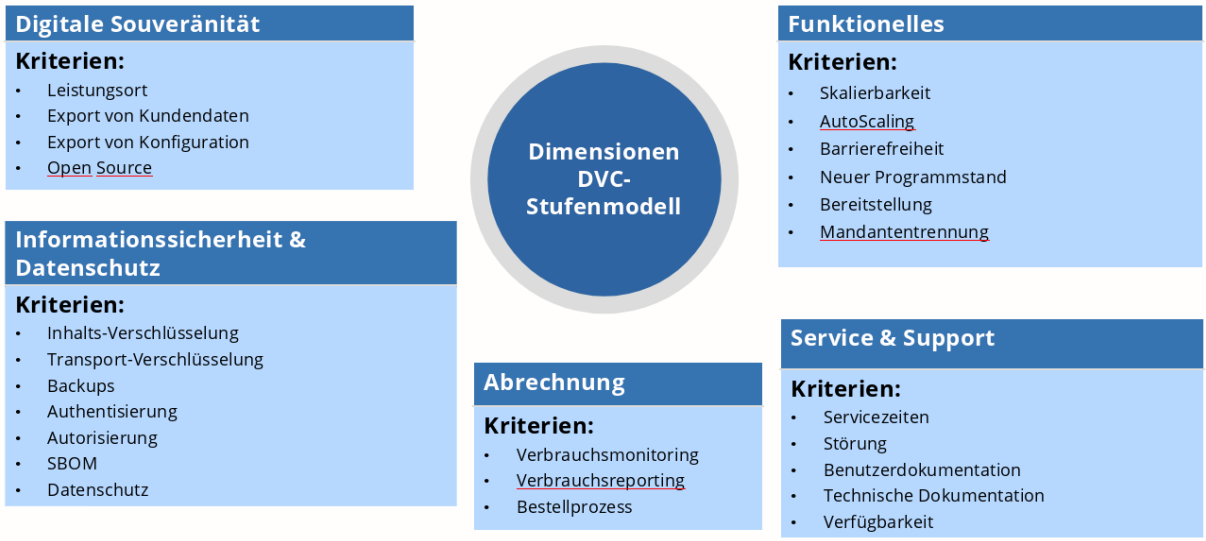

Abbildung 2

4.1 Dimension Funktionelles

Die Dimension Funktionelles behandelt funktionelle Kriterien, die als charakteristische Eigenschaften von Cloud-Services angesehen werden können. Diese wurden auf Basis der NIST Kriterien[1] Themen Skalierbarkeit, Bereitstellungszeit, Programmstände oder Mandantentrennung entwickelt. Zudem wurden auch weitere gesetzlich relevante Themen adressiert.

- **Skalierbarkeit** wurde als ein zentrales Kriterium für Cloud-Services und Bestandteil der NIST Kriterien in das DVC-Stufenmodell aufgenommen.

[1] siehe https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf, abgerufen am 27.08.2024

- **AutoScaling** bedeutet, dass der Anbieter automatisiert auf Gegebenheiten reagieren kann. Dies wird im Rahmen des DVC-Stufenmodells abgefragt, weil diese auch von NIST (Kriterium Rapid Elasticy) und dem BSI (im Rahmen der Cloud Computing Grundlagen) verlangt werden und zum aktuellen Stand der Technik gehören[2].
- **Barrierefreiheit** ist gesetzlich verpflichtend und für eine inklusive Nutzung der Services relevant. Barrierefreiheit ist für alle Funktionen relevant, welche eine Nutzerinteraktion ermöglichen.
- Cloud-Services haben eine höhere Frequenz an **Änderungen des Programmstands**, da der jeweilige Service jedoch in den Geschäftszeiten nutzbar bleiben muss, sind diese festzulegen und entsprechende Updates ausschließlich außerhalb vorzunehmen. Zudem hängt die Stufe von der Dauer des Wartungsfensters ab.
- Die **Bereitstellungszeiten** wurden als ein weiteres wesentliches Merkmal von Cloud-Services aufgenommen.
- Die **Mandantentrennung** ist zur Erfüllung der Anforderungen aus IT-Sicherheit, Datenschutz, Cloud Security Alliance und BSI Cloud Computing eine grundlegende Anforderung an Cloud-Services.

4.2 Dimension Abrechnung

Zur Dimension Abrechnung gehören drei Kriterien:

- **Verbrauchsmonitoring** ist essenziell, um eine dynamische Abrechnung zu ermöglichen; dies wird auch im Rahmen von NIST dem BSI (Cloud Computing Grundlagen) verlangt und gehört zum aktuellen Stand der Technik.
- Ein vorhandenes **Verbrauchs-Reporting** ist wichtig sowohl für dynamische Abrechnung als auch die für Kontrolle der Abrechnung; auch hierbei handelt es sich um ein NIST Kriterium sowie einen Bestandteil der BSI Cloud Computing Grundlagen.
- Ein vorhandener **Bestellprozess** ist ebenfalls NIST Kriterium und Bestandteil der BSI Cloud Computing Grundlagen. Cloud-Services sollten im Self-Service bestellbar sein und im Fall von „Pay-as-you-Go“ (flexibles, verbrauchabhängiges Abrechnungsmodell) auch Verbrauchsmonitoring und -reporting unterstützen. Zudem können auch die bestellten Tarife dynamisch anpassbar sein. In dieser Dimension wird deutlich, dass nicht pauschal für alle

[2] siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen.html, abgerufen am 27.08.2024

Anwendungsfälle eine höhere Stufe erstrebenswert ist, sondern die Anforderungen des Kunden an den Service im Vordergrund stehen.

4.3 Dimension Service & Support

Diese Dimension betrachtet u.a. die Themen der Servicezeiten, Verfügbarkeit und Umgang mit Störungsmeldungen. Eine Dokumentation für die einzelnen Cloud-Services ist ebenfalls von Bedeutung und wird in dieser Dimension geprüft.

- Die Angabe fester **Servicezeiten** für die Kunden ist ein wichtiges Kriterium in der Dimension Service & Support und wurde den EVB-IT Cloud AGB entnommen.
- Störung: Es ist gängige Praxis, dass ein **Störungssupport** vom Anbieter angeboten wird und damit die Nutzerfreundlichkeit unterstreicht.
- Das Führen einer nachvollziehbaren **Benutzerdokumentation** ist bei Werkverträgen gesetzlich verpflichtend und unterstreicht ebenfalls die Nutzerfreundlichkeit.
- Ebenfalls ist vom Anbieter aus Gründen der Nutzerfreundlichkeit eine **technische Dokumentation** anzubieten.
- Die **Verfügbarkeit** des Services sollte gemäß HV Kompendium BSI Band G angegeben werden, da dies einen wichtigen Entscheidungsgrund für einen Kauf durch einen Kunden darstellt.

4.4 Dimension Informationssicherheit & Datenschutz

Diese Dimension betrachtet einzelne Kriterien, welche nicht bereits im Rahmen der Anbieter-Prüfung durch den HV-Benchmark kompakt abgedeckt werden können, da sie für jeden Service einzeln zu prüfen sind. Der Kunde kann anhand seiner geplanten Anwendungsbereiche dann einfach prüfen, ob eine höhere Informationssicherheit benötigt wird. Zudem wird sichergestellt, dass alle Cloud-Services DSGVO-konform sind. Informationssicherheit & Datenschutz ist eine zentrale Dimension in der Entscheidungsfindung zu Cloud-Services:

- **Inhalts-Verschlüsselung** hat als Schutzziel eine umfassende Vertraulichkeit für die Kunden/ Nutzenden und ist zudem Empfehlung des BSI zum Umgang mit Daten in der Cloud.
- **Transport-Verschlüsselung** ist ein HTTPS State-of-the-Art und hat ebenfalls als Schutzziel eine umfassende Vertraulichkeit. Heutzutage ist es üblich, dass die meisten Browser bereits bei fehlender Transportverschlüsselung warnen.
- Das automatische Erstellen von **Backups** ist Teil der BSI-Empfehlungen zum Umgang mit Daten in der Cloud. Hierbei liegt der Fokus auf den Backups von Kundendaten während der

gesamten Nutzungsdauer. Je nach Stufe kann der Kunde entweder selbst einen Recovery-Prozess auslösen oder lediglich der Anbieter.

- **Authentisierung** hat als Schutzziel eine umfassende Vertraulichkeit für die Kunden/ Nutzenden und ist Bestandteil der Ziel-Architektur der DVC mit IAM.
- **Autorisierung**: hat als Schutzziel eine umfassende Vertraulichkeit für die Kunden/ Nutzenden und ist Bestandteil der Ziel-Architektur der DVC mit IAM.
- **Software-Bill-of-Materials (SBOM)** schafft Transparenz bzgl. der Software-Architektur und wird perspektivisch gesetzlich verpflichtend. Die SBOM muss alle verwendeten Software-Komponenten dokumentieren.
- **Datenschutz** im Sinne der DSGVO zielt auf den Schutzbedarf der Daten ab.

4.5 Dimension Digitale Souveränität

Digitale Souveränität ist eine Kernanforderung der gesamten DVC und umfasst die Themen, die zur Sicherstellung der Entscheidungsfreiheit im Einsatz von Cloud-Services gehören. Dazu zählen neben dem Leistungsstandort auch die Möglichkeiten eines Betreiberwechsels oder Open Source-basierte Services:

- Der **Leistungsort der Erbringung** des konkreten Services ist wesentlich für digitale Souveränität und Datenschutz.
- Der **Export von Kundendaten** minimiert das Risiko eines Vendor Lock-ins.
- Der **Export von Konfigurationen** minimiert das Risiko eines Vendor Lock-ins und fördert die Wechselfähigkeit.
- **Open-Source** basierte Cloud Services können einen Beitrag zur Minimierung der Abhängigkeit von kommerziellen Anbietern leisten.

5 Zukünftige Versionen des Reifegradmodells

Die verschiedenen Stufen und Kriterien des DVC-Stufenmodells unterliegen dem technologischen Wandel und den politischen Rahmenbedingungen und werden in den nächsten Jahren auf dieser Basis weiterentwickelt. Die Kriterienstufen orientieren sich an bereits etablierten Standards und der aktuellen Rechtslage. So wurden bei der Entwicklung u.a. Vorgaben des BSI und EVB-IT Cloud verwendet, sofern möglich. Die Begrifflichkeiten orientieren sich ebenfalls an etablierten Definitionen.

Ebenso ist es denkbar, für bestimmte Themenfelder oder gleichartige Anforderungen sogenannte Reifegradprofile zu erstellen, die nachgenutzt werden können.