



AWS Kompetenz für Industriesoftware Technologiepartner Validierungscheckliste

Mai 2018
Version 1.0

Inhaltsverzeichnis

Einführung	3
Kompetenzprogramm für AWS-Industriesoftware	3
Erwartungen der Parteien	Error! Bookmark not defined.
Programmteilnahme und Vorteile.....	4
Auswirkung von Fusionen, Akquisitionen und Veräußerungen	4
Definitionen	4
Kompetenzkategorien für Industriesoftware	6
Voraussetzungen für das Kompetenzprogramm für AWS-Industriesoftware	7
Checkliste für Technologiepartner-Validierung.....	10
AWS-Ressourcen	20

Einführung

Ziel des AWS-Kompetenzprogramms ist die Anerkennung von APN-Partnern, die ihren technischen Sachverstand unter Beweis stellen und ihren Kunden in spezialisierten Lösungsbereichen nachweislich zum Erfolg verholfen haben. Die Partnervalidierungscheckliste ("Checkliste") richtet sich an APN-Partner, die sich als AWS-Kompetenzpartner bewerben möchten. In der Checkliste finden Sie die Kriterien, die im Rahmen des AWS-Kompetenzprogramms zu erfüllen sind. Nachdem sich ein APN-Partner für eine bestimmte Kompetenz beworben hat, werden seine Fähigkeiten validiert. AWS behält sich das Recht vor, jederzeit Änderungen an diesem Dokument vorzunehmen.

AWS Kompetenzprogramm für Industriesoftware

AWS Kompetenzpartner für Industriesoftware bieten Kunden gezielte Lösungen für einen oder mehrere der wesentlichen Abläufe in Prozess- und diskreten Fertigungsindustrien: Produktdesign, Produktionsdesign, Produktion und Betriebsabläufe. In Prozess- und diskreten Fertigungsindustrien tätige Unternehmen können mithilfe dieser speziellen Softwarelösungen Produktinnovationen beschleunigen und gleichzeitig die Fertigungs- und Betriebskosten innerhalb ihrer Wertschöpfungskette reduzieren.

Erwartungen an die Teilnehmer

Von APN-Partner wird erwartet, dass sie das vorliegende Dokument vor der Einreichung einer Bewerbung für das AWS-Kompetenzprogramm eingehend lesen. Dies gilt auch, wenn sie alle Voraussetzungen erfüllen. Sollten irgendwelche Punkte in diesem Dokument unklar sein oder eine weitere Erläuterung erfordern, wenden Sie sich bitte zunächst an Ihren Partner Development Representative (PDR) oder Ihren Partner Development Manager (PDM). Falls weitere Unterstützung notwendig ist, kontaktiert Ihr PDR/PDM die für das Programm zuständige Stelle.

Wenn Sie als APN-Partner eine Bewerbung für das Programm einreichen möchten, füllen Sie bitte in der Checkliste der vorliegenden Dokument die Spalte für die Selbstbewertung als Partner aus.

So reichen Sie Ihre Bewerbung ein:

1. Melden Sie sich unter [APN Partner Central \(https://partnercentral.awspartner.com/\)](https://partnercentral.awspartner.com/) als Alliance Lead an.
2. Wählen Sie auf der linken Seite "View My APN Account" aus.
3. Blättern Sie weiter zum Abschnitt mit den Programmdetails.
4. Klicken Sie neben der AWS-Kompetenz, für die Sie sich bewerben möchten, auf "Update".
5. Füllen Sie die Bewerbung für das Programm aus, und klicken Sie auf "Submit".
6. Senden Sie die abgeschlossene Selbstbewertung per E-Mail an competency-checklist@amazon.com. Die Selbstbewertung muss folgende Angaben enthalten:
 - Die Kategorie der Lösung: Produktdesign, Produktionsdesign, Produktion oder Betriebsabläufe
 - Den Bereitstellungstyp: mandantenfähige SaaS, SaaS für Einzelmandanten, Managed Service oder Bereitstellung beim Kunden
 - Eine Dokumentation der vier Fallbeispiele gemäß (s. nachfolgenden Definitionen)

Falls Sie Fragen zu den obigen Anweisungen haben, wenden Sie sich bitte an Ihren APN Partner Development Representative/Manager.

AWS ist bestrebt, sämtliche Fragen innerhalb von fünf (5) Werktagen zu prüfen und zu beantworten, damit Sie mit der Planung Ihrer Validierung beginnen oder weitere Informationen anfordern können.

APN-Partner sollten zur Vorbereitung auf die Validierung die Checkliste durchgehen, die Selbstbewertung ausfüllen und die erforderliche Dokumentation zusammenstellen.

AWS empfiehlt APN-Partnern die Benennung von Ansprechpartnern, die im Rahmen der Validierung ausführliche Angaben zu den geforderten Informationen machen können. Als bewährte Methode für APN-Partner gilt es, die folgenden Mitarbeiter für die Validierung zur Verfügung zu stellen: einen oder mehrere AWS-Ingenieure/-Architekten mit umfassenden technischen Kenntnissen, die nähere Angaben zu den für die jeweilige Kompetenz eingereichten Fallbeispiele machen können, einen für Betriebsabläufe und den Support zuständigen Betriebsleiter sowie einen Verantwortlichen im Bereich Geschäftsentwicklung, für die Durchführung der Übersichtspräsentation.

Programmteilnahme und Vorteile

AWS kann einem APN-Partner jederzeit nach eigenem Ermessen den Status eines AWS-Kompetenzpartners entziehen, falls AWS feststellt, dass der APN-Partner die Anforderungen des AWS-Kompetenzprogramms oder die von AWS-Kompetenzpartnern erwarteten hohen Standards nicht erfüllt. Wenn einem APN-Partner der Status als AWS-Kompetenzpartner entzogen wird, erlöschen für den APN-Partner mit sofortiger Wirkung (i) jegliche Nutzungsrechte an den Vorteilen des AWS-Kompetenzprogramms, (ii) jegliche Nutzungsrechte an sämtlichen ihm in Verbindung mit dem AWS-Kompetenzprogramm zur Verfügung gestellten Unterlagen und Materialien sowie (iii) die Berechtigung zur Bezeichnung oder Tätigkeit als AWS-Kompetenzpartner.

Auswirkung von Fusionen, Akquisitionen und Veräußerungen

Im Rahmen des AWS-Kompetenzprogramms werden neben den Lösungen von APN-Partnern auch deren Geschäfts- und Bereitstellungsmodelle validiert. Diese werden durch Fusionen, Akquisitionen und Veräußerungen häufig erheblich beeinflusst. Das kann zur Folge haben, dass sich APN-Partner nach einer Fusion, Akquisition oder Veräußerung ihres Unternehmens neu bewerben und einer erneuten Validierung unterziehen müssen. Weitere Informationen entnehmen Sie bitte den nachfolgenden Richtlinien.

Akquisition/Fusion

Ein AWS-Kompetenzpartner übernimmt einen Nicht-Kompetenzpartner: Es muss vorerst nichts unternommen werden. Der AWS-Kompetenzpartner ist angehalten, jegliche Auswirkungen auf seine AWS-Kompetenzlösung im Rahmen einer nachfolgenden Validierung zu erläutern.

Ein Nicht-Kompetenzpartner übernimmt einen AWS-Kompetenzpartner: Der übernehmende APN-Partner muss eine neue Bewerbung einreichen und sich einer Validierung unterziehen, um als AWS-Kompetenzpartner anerkannt zu werden. In diesem Verfahren werden die neuen Geschäfts- und Bereitstellungsmodelle sowie die Integration der übernommenen technischen Fähigkeiten validiert. Wir empfehlen, dies umgehend zu veranlassen, um die weitere Anerkennung als AWS-Kompetenzprogramm sicherzustellen.

Ein AWS-Kompetenzpartner übernimmt einen anderen AWS-Kompetenzpartner: Es muss vorerst nichts unternommen werden. Die Validierung des konsolidierten Unternehmens erfolgt im Rahmen der Kompetenzverlängerung eines der beiden ursprünglichen Unternehmen (je nachdem, welche Verlängerung zuerst fällig wird).

Veräußerung

Ein AWS-Kompetenzpartner veräußert einen Teil seines Unternehmens, das mit seiner ausgeübten AWS-Kompetenz verbunden ist: Das veräußernde Unternehmen sollte signifikante, sich im Wesentlichen auf seinen Status als Kompetenzpartner bezogene, Auswirkungen umgehend offenlegen. Der APN-Partner wird je nach Signifikanz der Auswirkungen mit sofortiger Wirkung aus dem Programm entfernt oder muss die Auswirkungen auf das Unternehmen während der nächsten Kompetenzverlängerung angeben. Das veräußerte Unternehmen muss sich als neuer APN-Partner für das AWS-Kompetenzprogramm bewerben.

Definitionen

APN-Partnerlösung

AWS-Kompetenzen werden APN-Partnern erteilt, die eine spezielle Partnerlösung anbieten, die den Anforderungen einer AWS-Kompetenz entspricht.

AWS-Fallbeispiele

Alle APN-Partner müssen eine Reihe von AWS-Fallbeispielen mit detaillierten Angaben zu abgeschlossenen Bereitstellungen der Partnerlösung einreichen. Ein AWS-Fallbeispiel umfasst eine schriftliche Beschreibung eines abgeschlossenen Kundenprojekts einschließlich individueller Kundenlösungen und Ergebnisse. Die Fallbeispiele sollten Folgendes enthalten: Informationen zum Kunden, eine Übersicht der Herausforderung, Details zur implementierten Lösung, genutzte AWS-Services und Drittanbietertools, das Lieferdatum und die vom Kunden erzielten Ergebnisse.

Zu den AWS-Fallbeispiele ist AWS schriftlich mitzuteilen, ob die Angaben *öffentlich* sind (d. h. öffentlich bekannt gegeben werden dürfen) oder *nicht öffentlich* (d. h. nur innerhalb von AWS und an dessen externe Prüfer zum Zweck der Prüfung oder Bestätigung der Eignung des APN-Partners für das Kompetenzprogramm weitergegeben werden dürfen). Nachdem ein APN-Partner als AWS-Kompetenzpartner anerkannt wurde, werden *öffentliche* AWS-Fallbeispiele auf der AWS-Website als Referenz für erfolgreiche Partner-Kunden-Beziehungen bereitgestellt.

Validierung der Geschäftsanforderungen von AWS

Alle APN-Partner müssen sich für die Anerkennung einer AWS-Kompetenz einer Validierung der AWS-Geschäftsanforderungen unterziehen. Im Rahmen der Validierung der Geschäftsanforderungen wird bewertet, ob der APN-Partner die nicht technischen Anforderungen der Kompetenz erfüllt. Der APN-Partner muss sich unter anderem auf der Stufe "Advanced" befinden, eine Mindestanzahl relevanter öffentlicher und nicht öffentlicher AWS-Fallbeispiele einreichen, eine AWS-spezifische Landingpage haben und sich aktiv als Vordenker engagieren.

Technische Validierung durch AWS

Alle APN-Partner müssen sich für die Anerkennung einer AWS-Kompetenz einer technischen Validierung durch AWS unterziehen. Bei einer technischen Validierung wird eine APN-Partnerlösung im Hinblick auf bestimmte AWS-Fallbeispiele bewertet. Technische Validierungen dienen zur Bestätigung der Fähigkeiten des APN-Partners hinsichtlich der Entwicklung und Lieferung von Kundenlösungen mit Hilfe von AWS-Services in einem spezifischen Lösungsbereich, für eine bestimmte Anwendung oder einen speziellen vertikalen Markt. Gleichzeitig wird die Einhaltung der im AWS Well-Architected Framework beschriebenen bewährten Praktiken geprüft. Der APN-Partner demonstriert gegenüber externen Prüfern und/oder AWS Partner Solutions Architects wie die Leistung, die in den eingereichten AWS-Fallbeispiele beschrieben ist, erbracht wurde.

Die ausführlichen Anforderungen für die technische Validierung finden Sie in der nachfolgenden kompetenzspezifischen Checkliste für die technische Validierung. Technische Validierungen umfassen drei Elemente:

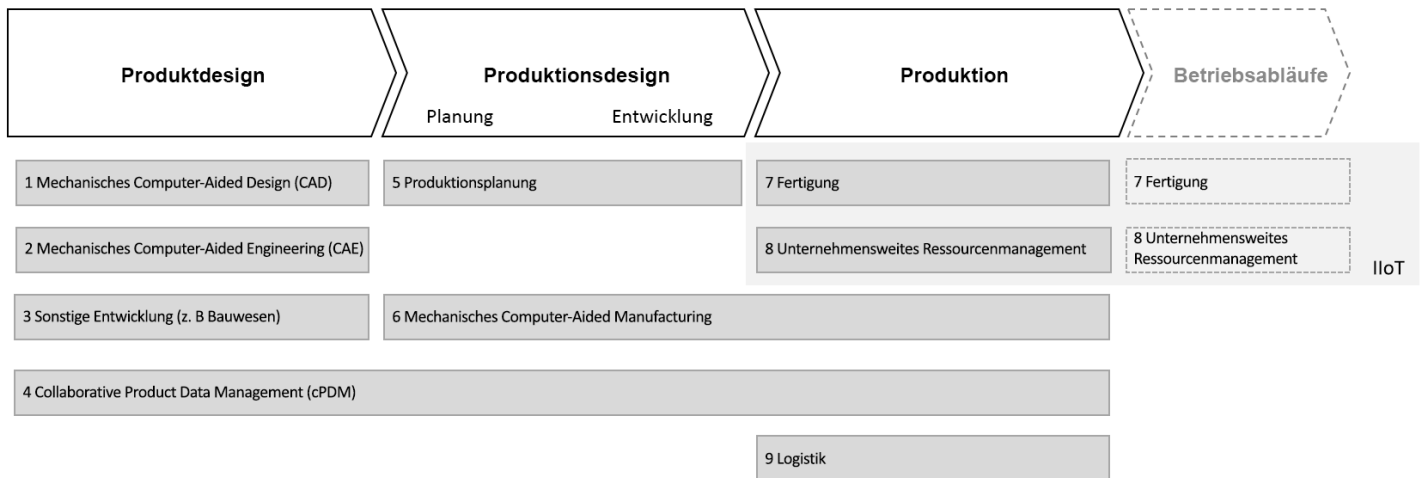
1. **Prüfung der Dokumentation:** Vom APN-Partner wird die Vorlage einer detaillierten technischen Dokumentation zur Partnerlösung und zu jedem der eingereichten AWS-Fallbeispiele erwartet. Externe Prüfer und/oder AWS Partner Solutions Architects ermitteln anhand der Dokumentation, ob der APN-Partner die in der Checkliste aufgeführten Anforderungen für die AWS-Kompetenz erfüllt. Die Dokumentation sollte sowohl öffentliche Informationen (z. B. online oder offline verfügbare Bereitstellungsanleitungen und Installationshandbücher) als auch nicht öffentliche Informationen (z. B. Architekturdiagramme, Designdokumente und Sicherheitsbewertungen) umfassen. Öffentliche Informationen werden hinsichtlich ihrer Übereinstimmung mit bewährten Methoden und der Verwendung der von APN genehmigten Marketingsprache bewertet. Nicht öffentliche Informationen können nach Ermessen des APN-Partners anonymisiert werden.
2. **Prüfung der zugrunde liegenden Architektur:** Bei APN-Partnern, die im Rahmen der Partnerlösung oder AWS-Fallbeispiele eine AWS-Umgebung konfigurieren oder betreiben, wird die der Umgebung zugrunde liegende AWS-Architektur einer kompetenzspezifischen Prüfung unterzogen. Die Anforderungen basieren auf den Grundprinzipien des AWS Well-Architected Frameworks und sind in der Checkliste im Detail aufgeführt.
3. **Kompetenz- und kategoriespezifische technische Anforderungen:** Durch jede Kompetenz und Kategorie soll die spezielle Lösung einer kundenspezifischen Herausforderung hervorgehoben werden. Die Checkliste kann daher kompetenzspezifische Anforderungen zur Hervorhebung bestimmter Methoden und Fähigkeiten enthalten, welche die Lösung dem Kunden bieten muss. Weitere Informationen entnehmen Sie bitte der Checkliste.

Elemente der APN-Partnerlösung oder des AWS-Fallbeispiels, die den Anforderungen nicht entsprechen, werden als kritische Befunde identifiziert. Jegliche während der Prüfung ermittelten kritischen Befunde müssen vor Anerkennung der AWS-Kompetenz nachgebessert werden. Falls kritische Befunde in Verbindung mit einem bestimmten AWS-Fallbeispiel nicht nachgebessert werden können, kann das Fallbeispiel möglicherweise nicht für die AWS-Kompetenz erwogen werden.

Kompetenzkategorien für Industriesoftware

APN-Partner müssen zusätzlich die jeweilige Segmentkategorie angeben, der ihre Lösung angehört:

- 1.) **Produktdesign:** In der Designphase verwendete Anwendungen und Services, einschließlich CAD (Computer Aided Design), CAE (Computer Aided Engineering), EDA (Electronic Design Automation) und Bauwesen
- 2.) **Produktionsdesign:** Anwendungen für das Fabriklayout und CAM (Computer-Aided Manufacturing), PLM (Product Lifecycle Management) und PDM (Product Data Management)
- 3.) **Produktion:** Anwendungen für Prozess- und diskrete Fertigungsindustrien wie MES (Manufacturing Execution Systems), MOM (Manufacturing Operations Management), PIMS (Plant Information Management System), Lieferkettenlogistik und Analyseanwendungen für den industriellen Einsatz
- 4.) **Betriebsabläufe:** Industrielle Internet of Things-Anwendungen unter Verwendung von IoT-Technologien für industrielle Prozesse sowie ISVs mit speziellen Industrieanwendungen wie etwa fertigungsspezifischen ERP-Lösungen (Enterprise Resource Planning). Diese Kategorie beinhaltet nicht die IoT-Verbraucheranwendungen aus, die Verbrauchern mithilfe von IoT-Services Produktfunktionen bereitstellen.



APN-Partner müssen außerdem die Bereitstellungskategorie ihrer Lösung angeben:

- 1.) **Mandantenfähige SaaS:** Bedienung mehrerer Kunden über eine gemeinsam genutzte AWS-Infrastruktur. Alle AWS-Konten werden vom APN-Partner verwaltet.
- 2.) **SaaS für Einzelmandanten:** Bedienung mehrerer Kunden, wobei bestimmte in AWS-Konten bereitgestellte Infrastrukturkomponenten kundenspezifisch sind. Alle AWS-Konten werden vom APN-Partner verwaltet.
- 3.) **Managed Service:** Auf AWS für einen einzelnen Kunden bereitgestellt. Alle AWS-Konten werden vom APN-Partner verwaltet.
- 4.) **Bereitstellung beim Kunden:** In der AWS-Umgebung eines Kunden bereitgestellt. Alle AWS-Konten werden vom Kunden verwaltet.

Voraussetzungen für das AWS Kompetenzprogramm für Industriesoftware

Der AWS Kompetenzprogramm Manager validiert die nachfolgend aufgeführten Punkte. Fehlende oder unvollständige Informationen müssen vor der Planung der technologischen Validierung ergänzt werden.

1.0 APN-Programmmitgliedschaft		Zutreffend J/N
1.1 Technologiepartnerstufe	Der APN-Partner befindet sich auf der APN-Technologiepartnerstufe "Advanced", um sich für das Kompetenzprogramm für AWS-Industriesoftware bewerben zu können.	
1.2 Lösungskategorie	<p>Der APN-Partner hat die Segmentkategorie seiner Lösung angegeben:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Produktdesign <input type="checkbox"/> Produktionsdesign <input type="checkbox"/> Produktion <input type="checkbox"/> Betriebsabläufe <p>Der APN-Partner hat die Lieferkategorie seiner Lösung angegeben:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Mandantenfähige SaaS <input type="checkbox"/> SaaS für Einzelmandanten <input type="checkbox"/> Managed Service <input type="checkbox"/> Bereitstellung beim Kunden 	
1.3 Kundenakzeptanz	Der APN-Partner hat die Gesamtzahl der Kunden angegeben, die seine Lösung nutzen.	
2.0 Fallbeispiele		Zutreffend J/N
2.1 Spezielle Fallbeispiele für Industriesoftware	<p>Der APN-Partner hat für jede einzelne zu prüfende Industriesoftwarelösung vier (4) Fallbeispiele. Jedes der vier Fallbeispiele bezieht sich auf ein Anwendungsbeispiel der APN-Partnerlösung in einer der vier Segmentkategorien (Produktdesign, Produktionsdesign, Produktion oder Betriebsabläufe).</p> <p>Der APN-Partner hat zu jeder Fallstudie die folgenden Informationen angegeben:</p> <ul style="list-style-type: none"> ▪ Name des Kunden ▪ Herausforderung des Kunden ▪ Art der Lösungsbereitstellung um die Anforderung zu erfüllen ▪ Von Drittanbietern verwendete Anwendungen oder Lösungen ▪ Datum des Produktionseintritts der Referenz ▪ Ergebnisse ▪ Spezielle Architekturdiagramme, Bereitstellungsleitfäden und sonstige lösungsspezifische Materialien, wie im folgenden Abschnitt beschrieben <p>Diese Informationen werden im Rahmen des Bewerbungsverfahrens für das Programm in APN Partner Central angefordert. Die für dieses Fallbeispiel angegebenen Informationen dürfen privat sein und werden nicht veröffentlicht.</p> <p>Alle vier Fallbeispiele werden während der Dokumentationsprüfung bei der technischen Validierung untersucht. Wenn der APN-Partner für die Bewertung des Fallbeispiels keine vollständige Dokumentation zu allen Punkten der Checkliste bereitstellen kann oder bestimmte Checklistenpunkte nicht erfüllt werden, wird das Fallbeispiel nicht für das Erreichen der Kompetenz erwogen.</p> <p>Fallbeispiele beziehen sich auf Bereitstellungen, die innerhalb der vergangenen 18 Monate erfolgt sind. Die Projekte müssen sich bei Kunden außerdem in Produktion befinden und sind weder Pilotprojekte noch Machbarkeitsstudien (PoC).</p>	
2.2 Öffentlich verfügbare Fallbeispiele	AWS verwendet öffentlich verfügbare Fallbeispiele nach Anerkennung der Kompetenz, um den nachweislichen Erfolg des APN-Partners anhand von messbaren KPIs der Lösung zu demonstrieren. Außerdem soll dadurch das Vertrauen der Kunden in die Erfahrung und das Wissen des APN-Partners bezüglich der Entwicklung und Lieferung von für sie passenden Lösungen gestärkt werden.	

	<p>Zwei (2) der vier (4) mit den Fallbeispielen verbundenen Bereitstellungen bei Kunden werden vom APN-Partner öffentlich zur Verfügung gestellt. Bei den öffentlich verfügbaren Fallbeispielen kann es sich um formale Fallstudien, Whitepaper, Videos oder Blog-Beiträge handeln.</p>	
	<p>Öffentlich verfügbare Fallbeispiele sind über die Website des APN-Partners leicht auffindbar. Interessenten gelangen über die Startseite des APN-Partners leicht zu den öffentlich verfügbaren Fallbeispielen. Außerdem hat der APN-Partner in seiner Anwendung Links zu den öffentlich verfügbaren Fallbeispielen angegeben.</p>	
	<p>Öffentlich verfügbare Fallbeispiele enthalten Folgendes:</p> <ul style="list-style-type: none"> ▪ Referenzen zum Namen des Kunden und des APN-Partners sowie zu AWS ▪ Herausforderung des Kunden ▪ Art der Lösungsbereitstellung zum Erfüllen der Anforderungen ▪ Verwendungsweise von AWS-Services im Rahmen der Lösung ▪ Ergebnisse 	
<h3>3.0 Internetpräsenz und Vordenkerrolle hinsichtlich AWS-Industriesoftware</h3>		<p>Zutreffend J/N</p>
<p>3.1 AWS-Landingpage des APN-Partners</p>	<p>Die Internetpräsenz eines APN-Partners in Verbindung mit seinen AWS-Industriesoftwarelösungen stärkt das Vertrauen der Kunden in die Fähigkeiten und Erfahrung des APN-Partners im Bereich Industriesoftware.</p> <p>Der APN-Partner hat eine AWS spezifische Landingpage, die Folgendes beinhaltet: eine Beschreibung seiner AWS-Industriesoftwarelösung, Links zu seinen öffentlich verfügbaren Fallbeispielen, eine Auflistung seiner Technologiepartnerschaften sowie sonstige relevante Informationen bezüglich der Erfahrung des APN-Partners mit Industriesoftware und seiner Arbeit mit AWS.</p> <p>Die AWS-spezifische Seite für Industriesoftware ist über die Startseite des APN-Partners zugänglich. Die Startseite des APN-Partners ist nur dann als AWS-Landingpage akzeptabel, wenn es sich bei dem APN-Partner um ein auf Industriesoftwaretechnologie spezialisiertes Unternehmen handelt und die Startseite den Fokus des APN-Partners auf Industriesoftware widerspiegelt.</p>	
<p>3.2 Vordenkerrolle hinsichtlich Industriesoftware</p>	<p>Bei Kompetenzpartnern für AWS-Industriesoftware wird davon ausgegangen, dass sie über umfassenden Sachkenntnissen bezüglich Industriesoftware verfügen und innovative Lösungen unter Verwendung von AWS-Services entwickelt haben.</p> <p>Der APN-Partner hat öffentlich verfügbare Materialien (z. B. Blog-Beiträge, Presseartikel, Videos usw.), die seinen Fokus und seine Kenntnisse hinsichtlich Industriesoftware demonstrieren. Es sind Links zu Materialien verfügbar, die innerhalb der vergangenen 12 Monate veröffentlicht wurden.</p>	
<h3>4.0 Geschäftsanforderungen</h3>		
<p>4.1 Einsatzbereite Toolkits</p>	<p>Der APN-Partner verfügt über eine einsatzbereite Dokumentation und einsatzbereite Vertriebs-Toolkits einschließlich eines klaren Nutzenversprechens für das Produkt. Dies alles kann auch zusammen mit sämtlichen relevanten Informationen (z. B. Vertriebsmaterialien, Präsentationen und Anwendungsfälle von Kunden) an die AWS Sales-Organisation weitergegeben werden, um die Eignung für einen kundenspezifischen Zweck zu ermitteln.</p> <p>Nachweise werden in Form von Vertriebsmaterial einschließlich einer Präsentation, eines One-Pager und einer Checkliste für Anwendungsfälle zur Verfügung gestellt.</p>	
<p>4.2 Produkt-Support/Helpdesk</p>	<p>Der APN-Partner bietet Kunden Produkt-Support per Web-Chat, Telefon oder E-Mail.</p> <p>Nachweise werden in Form einer Beschreibung des Supports zur Verfügung gestellt, der Kunden für ihr Produkt oder ihre Lösung angeboten wird.</p>	
<p>4.3 Produktlistung im AWS Marketplace</p>	<p>Der APN-Partner bietet die Lösung im AWS Marketplace an.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ja <input type="checkbox"/> Nein 	

	Wenn "Ja", stellt der APN-Partner einen Link zur Auflistung im AWS Marketplace zur Verfügung. Wenn "Nein", sind keine weiteren Informationen erforderlich.	
4.4 Vertriebsvergütung für gemeinsame AWS-Abschlüsse	<p>Der APN-Partner hat für seine Verkäufer Vertriebsvergütungspläne für gemeinsame Verkaufschancen mit AWS.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ja <input type="checkbox"/> Nein <input type="checkbox"/> Erläutern: _____ <p>Der Nachweis wird in Form einer kurzen Beschreibung des Vergütungsplans für die Verkäufer des APN-Partners erbracht.</p>	
4.5 Gemeinsame Abschlüsse von AWS und APN-Partner	<p>Der APN-Partner verfügt über ein Verfahren zur Dokumentation und Veröffentlichung gemeinsamer Abschlüsse.</p> <p>Der Nachweis wird in Form einer verbalen Beschreibung des Verfahrens erbracht.</p>	
5.0 Selbstbewertung des APN-Partners		Zutreffend J/N
5.1 Selbstbewertung der Validierungs-Checkliste für das AWS-Kompetenzprogramm	<p>Der APN-Partner hat eine Selbstbewertung hinsichtlich der Erfüllung der Anforderungen der Checkliste für die Technologiepartner-Validierung für AWS-Industriesoftware durchgeführt.</p> <ul style="list-style-type: none"> ▪ Der APN-Partner hat alle Abschnitte der Checkliste ausgefüllt. ▪ Die abgeschlossene Selbstbewertung wurde mit folgendem Betreff per E-Mail an competency-checklist@amazon.com gesendet: "[Name des APN-Partners], Industrial Software Competency Technology Partner Completed Self-Assessment." ▪ Dem APN-Partner wird empfohlen, die abgeschlossene Selbstbewertung vor der Einreichung bei AWS von seinem Partner Solutions Architect, Partner Development Representative (PDR) oder Partner Development Manager (PDM) prüfen zu lassen. Dies soll sicherstellen, dass das AWS-Team des APN-Partners vor der Kompetenzprüfung Empfehlungen ausarbeitet, um eine produktive Prüfung sicherzustellen. 	

Checkliste für Technologiepartner-Validierung

Die externen Prüfer und/oder AWS Partner Solutions Architects validieren die nachfolgend aufgeführten Punkte. Fehlende oder unvollständige Informationen müssen vor der Planung der technologischen Validierung ergänzt werden.

		Gilt für:				Zutreffend J/N
Technische Validierung		Mandantenfähige SaaS	SaaS für Einzelmandanten	Managed Service	Bereitstellung beim Kunden	
Erforderliche Dokumentation						
Im Rahmen der Selbstbewertung für eine Kompetenz müssen die folgende Dokumentationen eingereicht werden.						
Architekturdiagramm	<p>Je nach Bereitstellungskategorie sind ein oder mehrere Architekturdiagramme erforderlich.</p> <p>Jedes Architekturdiagramm muss Folgendes beinhalten:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Die Hauptelemente der Architektur und deren Zusammenspiel im Rahmen der für Kunden bereitgestellten Partnerlösung <input type="checkbox"/> Alle verwendeten AWS-Services mit Angabe der entsprechenden AWS-Servicesymbole <input type="checkbox"/> Die Bereitstellungsart der AWS-Services einschließlich VPCs, AZs, Subnetzen und Verbindungen zu Systemen außerhalb von AWS. <input type="checkbox"/> Außerhalb von AWS bereitgestellte Elemente, z. B. lokale Komponenten oder Hardware. 	Ja, eins für die gesamte Lösung und eins für jedes Fallbeispiel	Ja, eins für die gesamte Lösung und eins für jedes Fallbeispiel	Ja, eins für jedes Fallbeispiel	Ja, eins für jedes Fallbeispiel	
Bereitstellungsleitfaden	Der Bereitstellungsleitfaden enthält bewährte Methoden zur Bereitstellung der Partnerlösung auf AWS und umfasst alle im Leitfaden für die grundlegenden Bereitstellungsanforderungen aufgeführten Abschnitte.	Nein	Nein	Nein	Ja, eine für die Lösung.	
Abgeschlossene Validierungs-Checkliste	Der APN-Partner hat zu jedem der vier Fallbeispiele für die Partnerlösung die folgende Checkliste ausgefüllt.	Ja	Ja	Ja	Ja	
1.0 Sicherheit						
Die Säule "Sicherheit" des Well-Architected-Framework befasst sich mit dem Schutz von Informationen und Systemen. Zu den wichtigsten Themen zählen die Vertraulichkeit und Datenintegrität, die Rechteverwaltung einschließlich der Festlegung und Verwaltung individueller Berechtigungen, der Schutz von Systemen sowie das Einrichten von Kontrollen zur Erkennung von Sicherheitsvorfällen.						
1.1 Root-Anwender des AWS-Kontos nicht für Routineaktivitäten genutzt	Der Root-Anwender des AWS-Kontos wird nicht für Routineaktivitäten genutzt. Erstellen Sie im Anschluss an Ihr AWS-Konto IAM-Benutzerzugänge , und verwenden Sie diese für alle Routineaktivitäten. Bewahren	Ja	Ja	Ja	Nein	

	<p>Sie die Anmeldeinformationen für das AWS-Root-Konto nach der Erstellung Ihrer IAM-Benutzerkonten sicher auf. Verwenden Sie das AWS-Root-Konto ausschließlich für Konto- und Serviceverwaltungsaufgaben, die nur vom Root-Anwender des AWS-Kontos ausgeführt werden können. Weitere Informationen zum Einrichten von IAM-Benutzern und -gruppen für die tägliche Verwendung erhalten Sie im Artikel über das Erstellen Ihrer ersten IAM-Admin-Benutzer und -Gruppe.</p>					
<p>1.2 Multi-Factor Authentication (MFA) für Root-Anwender des AWS-Kontos aktiviert</p>	<p>Die MFA wurde für den Root-Anwender Ihres AWS-Kontos aktiviert. Da der Root-Anwender Ihres AWS-Kontos sensible Vorgänge in Ihrem AWS-Konto ausführen kann, trägt eine zusätzliche Authentifizierungsebene zum erweiterten Schutz Ihres Kontos bei. Sie können aus mehreren MFA-Typen wie der virtuellen MFA und der Hardware-MFA wählen.</p>	Ja	Ja	Ja	Nein	
<p>1.3 IAM-Benutzerkonten für alle Routineaktivitäten verwendet</p>	<p>Der Root-Anwender des AWS-Kontos wird ausschließlich für Aufgaben genutzt, die nur er ausführen kann. Sie erstellen stattdessen für jeden Benutzer, der Administratorzugriff benötigt, einen neuen IAM-Benutzer. Diese Benutzer fügen Sie anschließend einer Administratorgruppe hinzu, um ihnen Administratorrechte zu erteilen. Der Administratorgruppe weisen Sie die verwaltete Richtlinie für den Administratorzugriff zu. Die Benutzer der Administratorgruppe sollten daraufhin die Gruppen, Benutzer usw. für das AWS-Konto einrichten. Alle zukünftigen Interaktionen sollten über die Benutzer des AWS-Kontos und deren eigene Schlüssel und nicht über den Root-Anwender erfolgen. Für die Ausführung bestimmter Konto- und Serviceverwaltungsaufgaben müssen Sie sich jedoch als Root-Anwender anmelden.</p>	Ja	Ja	Ja	Nein	
<p>1.4 Multi-Factor Authentication (MFA) für alle interaktiven IAM-Benutzer aktiviert</p>	<p>Sie haben die MFA für alle interaktiven IAM-Benutzer aktiviert. Bei der MFA wird ein eindeutiger Authentifizierungscode bzw. ein Einmal-Passwort (One-Time Password, OTP) für Benutzer generiert. Die Benutzer müssen neben</p>	Ja	Ja	Ja	Nein	

	ihren normalen Anmeldeinformationen (Benutzername und Passwort) auch das OTP angeben. Das MFA-Gerät kann eine spezielle Hardware oder ein virtuelles Gerät sein, das beispielsweise in einer App auf einem Smartphone ausführbar ist.					
1.5 IAM-Anmeldeinformationen regelmäßig rotiert	Sie ändern Ihre Passwörter und Zugriffsschlüssel regelmäßig und stellen sicher, dass alle IAM-Benutzer Ihres Kontos dies ebenfalls tun. Sie begrenzen damit den Zeitraum, in dem die Anmeldeinformationen für den Zugriff auf Ihre Ressourcen genutzt werden können, falls ein Passwort oder ein Zugriffsschlüssel ohne Ihr Wissen kompromittiert wird. Sie können auf Ihr Konto eine Passworrichtlinie anwenden, um das Rotieren der Passwörter aller Ihrer IAM-Benutzer zu erzwingen . Außerdem können Sie festlegen, wie oft die Benutzer diese rotieren müssen. Weitere Informationen zum Rotieren der Zugriffsschlüssel für IAM-Benutzer erhalten Sie im Abschnitt zum Rotieren der Zugriffsschlüssel .	Ja	Ja	Ja	Nein	
1.7 Starke Passworrichtlinie für IAM-Benutzer festgelegt	Sie haben eine starke Passworrichtlinie für Ihre IAM-Benutzer festgelegt. Wenn Sie Benutzern erlauben, ihr Passwort zu ändern, fordern Sie die Erstellung starker Passwörter, die regelmäßig rotiert werden müssen. Sie können in der IAM-Konsole auf der Seite mit den Kontoeinstellungen eine Passworrichtlinie für Ihr Konto erstellen. Die Passworrichtlinie ermöglicht es Ihnen, Passwortanforderungen wie etwa die Mindestlänge, erforderliche nicht alphabetische Zeichen und die Rotationshäufigkeit festzulegen. Weitere Informationen finden Sie im Abschnitt zum Einrichten einer Kontopassworrichtlinie für IAM-Benutzer .	Ja	Ja	Ja	Nein	
1.8 IAM-Anmeldeinformationen nicht an mehrere Benutzer weitergegeben	Sie erstellen für jeden Benutzer, der Zugriff auf Ihr AWS-Konto benötigt, ein individuelles IAM-Benutzerkonto . Sie haben auch für sich selbst einen IAM-Benutzer festgelegt und ihm Administratorrechte erteilt. Diesen verwenden Sie für Ihre gesamte Arbeit. Indem Sie für die Personen, die auf Ihr Konto zugreifen, individuelle IAM-	Ja	Ja	Ja	Nein	

	<p>Benutzer erstellen, können Sie jedem IAM-Benutzer eindeutige Anmeldeinformationen zuweisen. Außerdem haben Sie die Möglichkeit, jedem IAM-Benutzer individuelle Berechtigungen zu erteilen. Bei Bedarf können Sie die Berechtigungen eines IAM-Benutzers jederzeit ändern oder entziehen. Geben Sie nicht die Anmeldeinformationen Ihres Root-Anwenders weiter, da sich diese mitunter nur schwer entziehen lassen und Benutzer damit unbegrenzten Zugriff erhalten.</p>					
<p>1.9 IAM-Richtlinien auf geringste Berechtigungen reduziert</p>	<p>Sie befolgen die standardmäßige Sicherheitsempfehlung und erteilen die geringsten Berechtigungen. Sie erteilen somit nur die für eine Aufgabe erforderlichen Berechtigungen. Nachdem Sie die Aufgaben von Benutzern ermittelt haben, erstellen Sie entsprechende Richtlinien, mit denen die Benutzer nur diese Aufgaben ausführen können. Erteilen Sie zunächst nur die minimal erforderlichen Berechtigungen, und gewähren Sie zusätzliche Berechtigungen nach Bedarf. Dies ist sicherer, als wenn Sie anfänglich zu umfassende Berechtigungen erteilen und diese später eingrenzen müssen. Für das Erteilen der richtigen Berechtigungen ist eine gewisse Recherche erforderlich. Ermitteln Sie, was zum Ausführen der jeweiligen Aufgabe erforderlich ist, welche Aktionen ein bestimmter Service unterstützt und welche Berechtigungen zum Ausführen dieser Aktionen erforderlich sind.</p>	<p>Ja</p>	<p>Ja</p>	<p>Ja</p>	<p>Nein</p>	
<p>1.10 Keine Verwendung von fest programmierten Anmeldeinformationen (z. B. Zugriffsschlüsseln)</p>	<p>Vermeiden Sie gemäß den bewährten Verwaltungsmethoden für AWS-Zugriffsschlüssel die Verwendung von fest programmierten Anmeldeinformationen. Wenn Sie programmgesteuert auf AWS zugreifen, können Sie Ihre Identität und die Identität Ihrer Anwendungen mithilfe eines Zugriffsschlüssels überprüfen. Mit Ihren Zugriffsschlüssel erhält jeder Benutzer dieselben Zugriffsrechte auf Ihre AWS-Ressourcen wie Sie. Daher</p>	<p>Ja</p>	<p>Ja</p>	<p>Ja</p>	<p>Ja</p>	

	achtet AWS akribisch auf den Schutz Ihrer Zugriffsschlüssel. Auch Sie sollten dies im Rahmen des Modells der gemeinsamen Verantwortung tun.					
1.11 Alle Anmeldeinformationen während der Speicherung verschlüsselt	Sie stellen grundsätzlich die Verschlüsselung aller Anmeldeinformationen während der Speicherung sicher.	Ja	Ja	Ja	Ja	
1.12 AWS-Zugriffsschlüssel nur von interaktiven Benutzern verwendet	AWS-Zugriffsschlüssel sollten ausschließlich wie folgt verwendet werden: (1) von Benutzern für den Zugriff auf AWS-Services mit sicherer Speicherung auf einem Gerät, das vom jeweiligen Benutzer kontrolliert wird (2) von einem Service für den Zugriff auf AWS-Services, jedoch nur, wenn a) die Verwendung einer EC2-Instance-Rolle, einer ECS-Aufgabenrolle oder eines ähnlichen Mechanismus nicht durchführbar ist, b) die AWS-Zugriffsschlüssel mindestens wöchentlich rotiert werden und c) die IAM-Richtlinie stark einschränkend ist, um i) nur den Zugriff auf bestimmte Methoden und Ziele zuzulassen und ii) den Zugriff auf die Subnetze einzuschränken, von denen aus auf die Ressourcen zugegriffen wird. CloudTrail muss für alle AWS-Konten und in jeder Region aktiviert sein. Die Transparenz Ihrer AWS-Kontoaktivität ist für die Befolgung bewährter Sicherheits- und Betriebsmethoden ausschlaggebend. Sie können mit CloudTrail auf Kontoaktivitäten innerhalb Ihrer AWS-Infrastruktur reagieren und Aktivitäten anzeigen, suchen, archivieren und analysieren. Sie können ermitteln, wer oder was eine Aktion ausgeführt hat, welche Ressourcen genutzt wurden, wann das Ereignis eingetreten ist sowie weitere Details, die Ihnen die Analyse und die Reaktion auf Aktivitäten in Ihrem AWS-Konto erleichtern. CloudTrail-Protokolle werden in einem Bucket eines anderen AWS-Kontos gespeichert , für das nur sehr begrenzte Zugriffsrechte etwa für Prüfungen oder Recovery erteilt werden.	Ja	Ja	Ja	Ja	
1.13 CloudTrail für alle AWS-Konten in jeder Region aktiviert	CloudTrail muss für alle AWS-Konten und in jeder Region aktiviert sein. Die Transparenz Ihrer AWS-Kontoaktivität ist für die Befolgung bewährter Sicherheits- und Betriebsmethoden ausschlaggebend. Sie können mit CloudTrail auf Kontoaktivitäten innerhalb Ihrer AWS-Infrastruktur reagieren und Aktivitäten anzeigen, suchen, archivieren und analysieren. Sie können ermitteln, wer oder was eine Aktion ausgeführt hat, welche Ressourcen genutzt wurden, wann das Ereignis eingetreten ist sowie weitere Details, die Ihnen die Analyse und die Reaktion auf Aktivitäten in Ihrem AWS-Konto erleichtern. CloudTrail-Protokolle werden in einem Bucket eines anderen AWS-Kontos gespeichert , für das nur sehr begrenzte Zugriffsrechte etwa für Prüfungen oder Recovery erteilt werden.	Ja	Ja	Ja	Nein	
1.14 CloudTrail-Protokolle in einem S3-Bucket eines anderen AWS-Kontos gespeichert	CloudTrail-Protokolle werden in einem Bucket eines anderen AWS-Kontos gespeichert , für das nur sehr begrenzte Zugriffsrechte etwa für Prüfungen oder Recovery erteilt werden.	Ja	Ja	Ja	Nein	
1.15 Versioning oder MFA Delete für S3-Bucket für CloudTrail-Protokolle aktiviert	Der Inhalt des Buckets für CloudTrail-Protokolle ist durch Versioning oder MFA Delete geschützt.	Ja	Ja	Ja	Nein	

<p>1.16 EC2-Sicherheitsgruppen stark eingeschränkt</p>	<p>Alle EC2-Sicherheitsgruppen schränken den Zugriff so weit wie möglich ein. Dies umfasst mindestens (1) die Implementierung von Sicherheitsgruppen zur Einschränkung des Datenverkehrs zwischen Internet und VPC, (2) die Implementierung von Sicherheitsgruppen zur Einschränkung des Datenverkehrs innerhalb der VPC und (3) die Erteilung der geringsten Berechtigung in allen Fällen.</p>	Ja	Ja	Ja	Ja	
<p>1.17 S3-Buckets in Ihrem Konto mit entsprechenden Zugriffsebenen</p>	<p>Sie stellen die Einrichtung entsprechender Kontrollen sicher, um den Zugriff auf jeden S3-Bucket zu steuern. Bei Verwendung von AWS gilt als bewährte Methode, den Zugriff auf Ihre Ressourcen einzuschränken, und zwar ausschließlich auf die Benutzer, die die Ressourcen tatsächlich benötigen – gemäß dem Prinzip der geringsten Berechtigung.</p>	Ja	Ja	Ja	Ja	
<p>1.18 S3-Buckets nicht für öffentlichen Zugriff konfiguriert</p>	<p>Sie stellen sicher, dass nicht öffentlich zugängliche Buckets ordnungsgemäß nur für den nicht öffentlichen Zugriff konfiguriert sind. Standardmäßig sind alle S3-Buckets privat und nur für Benutzer mit ausdrücklich erteilten Zugriffsrechten zugänglich. In den meisten Anwendungsfällen ist kein weitreichender öffentlicher Zugriff erforderlich, um Dateien aus Ihrem S3-Bucket zu lesen – es sei denn, Sie stellen darin öffentliche Komponenten bereit (z. B. Bilder für eine öffentliche Website). Als bewährte Methode gilt, der Öffentlichkeit niemals Zugriff auf Ihren S3-Bucket zu gewähren.</p>	Ja	Ja	Ja	Ja	
<p>1.19 Überwachungsmechanismus zum Schutz vor einer Offenlegung von S3-Buckets oder -Objekten</p>	<p>Sie verfügen über Überwachungs- oder Benachrichtigungsverfahren, um bei einer Offenlegung von S3-Buckets informiert zu werden. Hierfür eignet sich unter anderem Trusted Advisor. Trusted Advisor prüft Buckets im Amazon Simple Storage Service (Amazon S3) auf öffentliche Zugriffsberechtigungen. Bucket-Berechtigungen, die allen Benutzern das Auflisten von Objekten gewähren, können zu unerwartet hohen Gebühren führen, wenn Objekte im Bucket häufig von</p>	Ja	Ja	Ja	Nein	

	<p>nicht vorgesehenen Benutzern aufgelistet werden. Durch Bucket-Berechtigungen, die allen Benutzern das Hochladen und Löschen von Objekten gewähren, entstehen potenzielle Sicherheitslücken, da alle Benutzer in einem Bucket Objekte hinzufügen, ändern oder entfernen können. Bei der Trusted Advisor-Prüfung werden explizite Bucket-Berechtigungen und damit verbundene Bucket-Richtlinien überprüft, welche die Bucket-Berechtigungen möglicherweise außer Kraft setzen.</p>					
<p>1.20 Überwachungsmechanismus zur Erkennung von Änderungen in EC2-Instances und Containern</p>	<p>Jegliche Änderungen an Ihren EC2-Instances oder Containern können auf nicht autorisierte Aktivitäten hindeuten. Sie werden als Mindestmaßnahme in einem dauerhaften Speicher protokolliert, um zukünftige forensische Untersuchungen zu ermöglichen. Der für diesen Zweck genutzte Mechanismus muss mindestens (1) jegliche Änderungen an Betriebssystem- oder Anwendungsdateien in den EC2-Instances oder Containern der Lösung erkennen und (2) Aufzeichnungen dieser Änderungen in einem dauerhaften Speicher außerhalb der EC2-Instance oder des Containers protokollieren. Geeignete Mechanismen sind unter anderem (a) die Integritätsprüfung von Dateien über die geplante Konfigurationsverwaltung (z. B. Chef oder Puppet) oder ein spezielles Tool (z. B. OSSEC oder Tripwire) oder (b) die Erweiterung von Konfigurationsverwaltungstools auf die Validierung der EC2-Hostkonfiguration einschließlich Benachrichtigungen bei Aktualisierungen wichtiger Konfigurationsdateien oder -pakete durch (protokollierte No-Op-)Frühwarnereignisse, um die kontinuierliche Verfügbarkeit des Service auf allen relevanten Hosts während der Laufzeit sicherzustellen, oder (c) die Bereitstellung eines Systems zum Erkennen von Eindringversuchen auf Hosts, wie etwa eine Open Source-Lösung, zum Beispiel OSSEC mit ElasticSearch und Kibana oder eine Partnerlösung.</p>	<p>Ja</p>	<p>Ja</p>	<p>Ja</p>	<p>Nein</p>	

	Hinweis: Das regelmäßige Rotieren von EC2-Instances oder Containern ist kein geeigneter Mechanismus.					
1.21 Alle Daten klassifiziert	Alle in der Anwendung verarbeiteten und gespeicherten Kundendaten werden einbezogen und entsprechend klassifiziert, um ihre Sensibilität und die passenden Verarbeitungsmethoden zu ermitteln.	Ja	Ja	Ja	Ja	
1.22 Alle sensiblen Daten verschlüsselt	Alle als sensibel klassifizierten Kundendaten sind während der Übertragung und Speicherung verschlüsselt.	Ja	Ja	Ja	Ja	
1.23 Kryptografische Schlüssel sicher verwaltet	Alle kryptografischen Schlüssel sind während der Speicherung und Übertragung verschlüsselt. Der Zugriff auf die Schlüssel wird mithilfe einer AWS-Lösung wie KMS oder einer Partnerlösung wie HashiCorp Vault gesteuert.	Ja	Ja	Ja	Ja	
1.24 Alle Daten während der Übertragung verschlüsselt	Alle Daten sind während der Übertragung über eine VPC-Grenze hinweg verschlüsselt.	Ja	Ja	Ja	Ja	
1.25 Maßnahme bei Sicherheitsvorfällen definiert und geprobt	Für den Umgang mit Sicherheitsvorfällen wie etwa der Gefährdung von AWS-Konten wurden Maßnahmen festgelegt. Die Maßnahmen werden durch die Implementierung von Verfahren getestet und geprobt, beispielsweise im Rahmen einer Sicherheitsübung. Die Maßnahmen wurden innerhalb der vergangenen 12 Monate geprobt, um sicherzustellen, dass (a) die erforderlichen Benutzer Zugriff auf die Umgebung haben, (b) die entsprechenden Tools verfügbar sind und (c) die entsprechenden Benutzer wissen, wie auf die im Plan aufgeführten Sicherheitsvorfälle zu reagieren ist.	Ja	Ja	Ja	Nein	

2.0 Zuverlässigkeit

Die Säule "Zuverlässigkeit" befasst sich mit der Verhinderung von System- und Anwendungsausfällen und im Bedarfsfall mit der schnellen Systemwiederherstellung nach einem Ausfall. Die Geschäfts- und Kundenanforderungen zu erfüllen, steht dabei im Vordergrund. Zu den wichtigsten Themen zählen grundlegende Elemente der Einrichtung, projektübergreifende Anforderungen, die Recovery-Planung und die Handhabung von Änderungen.

2.1 Hochverfügbare Netzwerkkonnektivität	Die Netzwerkkonnektivität der Lösung ist hochverfügbar. Wenn die Verbindung zu Kundennetzwerken über ein VPN oder Direct Connect erfolgt, unterstützt die Lösung redundante Verbindungen, auch wenn die Kunden diese nicht immer implementieren.	Ja	Ja	Ja	Ja	
2.2 Skalierungsmechanismen	Die Skalierungsmechanismen für die Infrastruktur erfüllen	Ja	Ja	Ja	Ja	

für die Infrastruktur erfüllen Geschäftsanforderungen	<p>die Geschäftsanforderungen entweder durch (1) die Implementierung von Auto-Scaling-Mechanismen auf jeder Ebene der Architektur oder (2) die Bestätigung, dass aufgrund der aktuellen Geschäftsanforderungen einschließlich der Kostenanforderungen und der voraussichtlichen Benutzerzunahme keine Auto-Scaling-Mechanismen erforderlich sind UND die manuellen Skalierungsverfahren vollständig dokumentiert sind und regelmäßig getestet werden.</p>					
2.3 AWS- und Anwendungsprotokolle zentral verwaltet	<p>Alle Protokollinformationen von der Anwendung und der AWS-Infrastruktur werden in einem zentralen System konsolidiert.</p>	Ja	Ja	Ja	Nein	
2.4 AWS- und Anwendungsüberwachung und -benachrichtigungen zentral verwaltet	<p>Die Anwendung und die AWS-Infrastruktur werden zentral überwacht. Generierte Benachrichtigungen werden an die für die jeweiligen Betriebsabläufe zuständigen Mitarbeiter gesendet.</p>	Ja	Ja	Ja	Nein	
2.5 Infrastruktur-Provisioning und -verwaltung automatisiert	<p>Die Lösung verwendet für das Provisioning und die Verwaltung der AWS-Infrastruktur ein automatisiertes Tool wie CloudFormation oder Terraform. Die AWS-Konsole wird nicht für Routineänderungen an der AWS-Produktionsinfrastruktur verwendet.</p>	Ja	Ja	Ja	Ja	
2.6 Regelmäßige Datensicherungen	<p>Sie führen regelmäßige Sicherungen in einem dauerhaften Speicher durch. Durch Sicherungen gewährleisten Sie, dass Ihre Daten nach einem administrativen, logischen oder physischen Fehler wiederhergestellt werden können. Amazon S3 und Amazon Glacier sind optimale Sicherungs- und Archivierungsservices. Beides sind dauerhafte, preisgünstige Speicherplattformen. Beide bieten unbegrenzte Kapazität und erfordern kein Volume- oder Medienmanagement, wenn die Sicherungsdatensätze anwachsen. Dank des nutzungsbasierten Preismodells und der niedrigen Kosten pro GB/Monat eignen sich diese Services gut für die Datensicherheit.</p>	Ja	Ja	Ja	Ja	

2.7 Recovery-Mechanismen regelmäßig und nach signifikanten architektonischen Änderungen getestet	Sie testen die Recovery-Mechanismen und -Verfahren regelmäßig und nach signifikanten Änderungen Ihrer Cloud-Umgebung. AWS bietet umfassende Ressourcen für die Sicherung und Wiederherstellung Ihrer Daten.	Ja	Ja	Ja	Nein	
2.8 Stabile Lösung bei Ausfall einer Availability Zone	Die Lösung bleibt auch bei einem Ausfall aller Services innerhalb einer einzelnen Availability Zone verfügbar.	Ja	Ja	Ja	Ja	
2.9 Ausfallsicherheit der Lösung getestet	Die Ausfallsicherheit der Infrastruktur bei einer Unterbrechung in einer einzelnen Availability Zone wurde innerhalb der vergangenen 12 Monate im Rahmen einer Sicherheitsübung in der Produktion getestet.	Ja	Ja	Ja	Nein	
2.10 Disaster Recovery (DR)-Plan festgelegt	Es wurde ein gut definierter Disaster Recovery-Plan (Notfallwiederherstellungs-Plan) einschließlich eines Wiederherstellungspunkts (Recovery Point Objective, RPO) und einer Wiederherstellungsdauer (Recovery Time Objective, RTO) festgelegt. Sie haben einen RPO und eine RTO für alle relevanten Services festgelegt, die beide dem SLA entsprechen, den Sie Ihren Kunden anbieten.	Ja	Ja	Ja	Ja	
2.11 Wiederherstellungsdauer (Recovery Time Objective, RTO) unter 24 Stunden	Die RTO liegt bei wichtigen Services grundsätzlich unter 24 Stunden.	Ja	Ja	Ja	Nein	
2.12 Disaster Recovery (DR)-Plan ausreichend getestet	Sie testen Ihren DR-Plan regelmäßig und nach umfassenden Aktualisierungen bezüglich des Wiederherstellungspunkts (Recovery Point Objective, RPO) und der Wiederherstellungsdauer (Recovery Time Objective, RTO). Vor der Genehmigung der Stufe "Advanced" als APN-Partner von AWS haben Sie mindestens einen DR-Test durchgeführt.	Ja	Ja	Ja	Nein	
2.13 Disaster Recovery (DR)-Plan beinhaltet Wiederherstellung in anderem AWS-Konto	Ihr DR-Plan beinhaltet eine Strategie für die Wiederherstellung in einem anderen AWS-Konto. Dies wird in Ihren regelmäßigen Recovery-Tests geprüft. Sie haben den DR-Plan in den vergangenen 12 Monaten mindestens einmal vollständig getestet, einschließlich des Recoverys in einem anderen AWS-Konto. Hinweis: Verfahren für die Datenwiederherstellung in Testumgebungen oder den	Ja	Ja	Ja	Nein	

Datenexport für Benutzer eignen sich zwar zur Überprüfung von Sicherungen, ermöglichen aber keine vollständige Wiederherstellung in einem anderen AWS-Konto.						
--------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--

3.0 Operational Excellence

Die Säule "Operational Excellence" befasst sich mit der Ausführung und Überwachung der bereitgestellten Systeme. Ziel sind die Generierung eines tatsächlichen Mehrwerts für das Geschäft sowie die beständige Optimierung der Prozesse und Verfahren. Zu den wichtigsten Themen zählen die Verwaltung und Automatisierung von Änderungen, die Reaktion auf Vorfälle und Ereignisse sowie die Definition von Standards für die erfolgreiche Verwaltung des täglichen Betriebs.

3.1 Bereitstellung von Codeänderungen automatisiert	Die Lösung nutzt für die Codebereitstellung in der AWS-Infrastruktur eine automatisierte Methode. Aktualisierungen werden nicht in interaktiven SSH- oder RDP-Sitzungen in der AWS-Infrastruktur bereitgestellt.	Ja	Ja	Ja	Nein	
3.2 Runbooks und Eskalationsverfahren definiert	Sie haben Run-books entwickelt, um die für unterschiedliche Anwendungs- und AWS-Ereignisse verwendeten Standardverfahren zu definieren. Außerdem haben Sie ein Eskalationsverfahren für die Verarbeitung von Systembenachrichtigungen und -alarmen festgelegt, um auf die von Kunden gemeldeten Vorfälle reagieren zu können. Das Eskalationsverfahren beinhaltet gegebenenfalls auch die Eskalation an den AWS Support.	Ja	Ja	Ja	Nein	
3.3 AWS Business Support für das AWS-Konto aktiviert	Sie haben den Business Support aktiviert. Der Business Support (oder höher) ist eine Voraussetzung des AWS-Partnernetzwerks für die Stufe "Advanced" von Technologiepartnern. Um sich für die Stufe "Advanced" zu qualifizieren, haben Sie den Business Support mindestens für eines Ihrer AWS-Konten aktiviert.	Ja	Ja	Ja	Nein	

AWS-Ressourcen:

Website für AWS Well-Architected <https://aws.amazon.com/architecture/well-architected/>

AWS-Whitepaper <https://aws.amazon.com/whitepapers/>

APN-Blog <https://aws.amazon.com/blogs/apn/>

AWS-Blog <https://aws.amazon.com/blogs/>