aws partner network | competency

AWS-Einzelhandelskompetenz
Validierungscheckliste für Technologiepartner

Dezember 2019
Version 1.0

Dieses Dokument dient lediglich Informationszwecken und stellt kein Angebot und keine vertraglichen Verpflichtungen, Garantien oder Zusicherungen von AWS dar. Alle hier beschriebenen Vorteile liegen im alleinigen Ermessen von AWS und können ohne Ankündigung geändert oder aufgehoben werden. Dieses Dokument ist nicht Teil einer Vereinbarung zwischen AWS und seinen Kunden und/oder APN-Partnern und ändert auch keine Vereinbarung, die möglicherweise bereits besteht.

Inhalt

Einführung

Mit dem AWS-Kompetenzprogramm sollen Partner im AWS-Partnernetzwerk ("APN-Partner") mit technischer Fachkenntnis und nachgewiesenen Kundenerfolgen in speziellen Lösungsbereichen gewürdigt werden. Die Validierungscheckliste für Kompetenzpartner ("Checklist") wurde für APN-Partner konzipiert, die Interesse an einer Teilnahme am AWS-Kompetenzprogramm haben. Diese Checklist enthält die Kriterien, die erforderlich sind, um die Bezeichnung im Rahmen des AWS-Kompetenzprogramms zu erhalten. APN-Partner absolvieren nach der Bewerbung für eine bestimmte Kompetenz ein Audit zu ihren Kompetenzen. AWS nutzt unternehmensinternes Fachwissen und zieht für die Durchführung des Audits einen externen Partner hinzu. AWS behält sich das Recht vor, jederzeit Änderungen an diesem Dokument vorzunehmen.

Erwartungen der beteiligten Parteien

Es wird erwartet, dass APN-Partner sich im Detail mit diesem Dokument vertraut machen, bevor sie sich für das AWS-Kompetenzprogramm bewerben, selbst wenn alle Voraussetzungen erfüllt sind. Sollten bestimmte Abschnitte in diesem Dokument unklar sein und weiterer Erläuterungen bedürfen, wenden Sie sich zunächst an den für Sie zuständigen AWS Partner Development Representative (PDR) oder AWS Partner Development Manager (PDM). Ihr PDR/PDM wird sich an das Programmbüro wenden, wenn weitere Unterstützung erforderlich sein sollte.

Wenn Sie als APN-Partner bereit sind, eine Programmbewerbung einzureichen, müssen Sie die Spalte "Partner Self-Assessment" in der Checkliste ausfüllen, die im weiteren Verlauf dieses Dokuments näher beschrieben wird.

So übermitteln Sie Ihre Bewerbung:

1. Melden Sie sich als Alliance Lead auf APN Partner Central (https://partnercentral.awspartner.com/) an.
2. Wählen Sie "View My APN Account" links auf der Seite aus.
3. Führen Sie einen Bildlauf zum Abschnitt "Program Details" aus.
4. Wählen Sie “Update” neben der AWS-Kompetenz aus, für die Sie sich bewerben möchten.
5. Füllen Sie die Programmbewerbung aus, und klicken Sie dann auf "Submit".
6. Senden Sie die ausgefüllte Selbsteinschätzung per E-Mail an competency-checklist@amazon.com.
    - Die Selbsteinschätzung muss Folgendes enthalten:
        - Die Kategorie der Lösung (Kundenbindung, Absatzförderung und -planung, Lieferkette und Vertrieb, physischer, digitaler und virtueller Speicher, fortschrittliche Datenwissenschaft für den Einzelhandel und Kerngeschäftsanwendungen für den Einzelhandel)
        - Die Art der Bereitstellung (SaaS oder durch Kunden in AWS bereitgestellt)
        - Dokumentation für die AWS-Fallstudien (siehe Definitionen unten)

Bei Fragen zu den oben genannten Anweisungen wenden Sie sich bitte an den für Sie zuständigen PDR/PDM. AWS wird sich Ihre Fragen anschauen und ist bemüht, innerhalb von fünf Werktagen auf Ihre Fragen zu antworten, um einen Zeitplan für Ihr Audit zu erstellen oder weitere Informationen anzufordern.

APN-Partner sollten sich auf das Audit vorbereiten, indem sie die Checklist studieren, anhand der Checkliste eine Selbsteinschätzung durchführen und Nachweise erbringen, die sie dem Prüfer am Tag des Audits vorlegen.

AWS empfiehlt, dass APN-Partner Einzelpersonen benennen, die sich im Rahmen des Audits detailliert zu den Anforderungen äußern können. Es hat sich bewährt, dass APN-Partner Personen mit den folgenden Zuständigkeiten für das Audit bereitstellen: mindestens einen hochspezialisierten und von AWS zertifizierten Techniker/Architekt, einen Betriebsleiter, der für die Abläufe und die Supportelemente zuständig ist, sowie einen leitenden Mitarbeiter im Bereich Geschäftsentwicklung, der den Übersichtsvortrag durchführt. APN-Partner sollten vor der Vereinbarung eines Termins für das Audit sicherstellen, dass sie berechtigt sind, alle Informationen, die im Nachweis oder in den Präsentationen enthalten sind, gegenüber dem Prüfer (von AWS oder einem externen Partner) preisgeben dürfen.

AWS-Kompetenzprogramm für den Einzelhandel

AWS-Kompetenzpartner im Bereich Einzelhandel bieten Lösungen für den Einzelhandel an, von Kundenbindung, Absatzförderung und -planung, Einzelhandelslieferkette und -vertrieb, physischem, digitalen und virtuellen Speicher, fortschrittlicher Datenwissenschaft für den Einzelhandel bis zu Kerngeschäftsanwendungen für den Einzelhandel.

Kompetenzkategorien im Einzelhandel

APN-Partner müssen außerdem die Segmentkategorie angeben, zu der ihre Lösung passt:

- **Kundenbindung:** Lösungen in den Bereichen Loyalität, Social Channel Management, Customer Relationship Management (CRM), Call Center, Werbung (digital und direkte Mailings), SEO und Zielgruppenbindung, mit denen Marketingführungskräfte im Einzelhandel proaktiv Kunden gewinnen und binden können, sowohl vor als auch nach dem Kauf.

- **Absatzförderung und -planung:** Lösungen in den Bereichen Verkaufsförderung, Aufstockung, Sortimentsplanung, Planogramm/Raumplanung, Promotions- und Preisoptimierung, Kategoriemanagement und Zusammenarbeit mit Zulieferern, die von Teams in der Absatzförderung und -planung genutzt werden können.

- **Lieferkette und Vertrieb:** Lösungen für die Bereiche Lieferkette und Vertrieb, unter anderem für Lagerverwaltungssysteme (Warehouse Management Systems, WMS), Enterprise Resource Planning (ERP), Lagerautomatisierung, Import/Export, Transport und Logistik.

- **Physischer, digitaler und virtueller Speicher:** Lösungen, die die On- oder Offlineerfahrung beim Einkaufen transformieren, wie POS, Bestellverwaltungssysteme (Order Management Systems, OMS), Unified Commerce, E-Commerce, Logistik der letzten Meile, Boundless Store-Erlebnis, digitale Innovationen (AR/VR, ESL, IoT, Beacons, Spracherkennung, Digital Kiosk, Smart Mirror, interaktive Displays), Digital Asset Management (DAM) und Zahlungsarten.

- **Fortschrittliche Datenwissenschaft für den Einzelhandel:** Retail Data Lake, AI/ML und Analyselösungen zur Verbesserung der Betriebseffizienz sowie der Kundeneinblicke und -bindung.

- **Kerngeschäftsanwendungen für den Einzelhandel:** Enterprise-Kernlösungen für den Einzelhandel für C-Suite, Finanzwesen, Beschaffung, Personalwesen, Mitarbeiterverwaltung, Rechtsabteilung und IT.

APN-Partner müssen auch angeben, welche Bereitstellungskategorie für ihre Lösung gilt:

1. **SaaS:** Bedient mehrere Kunden über eine gemeinsame AWS-Infrastruktur. Alle AWS-Konten werden vom APN-Partner verwaltet.

2. **Vom Kunden bereitgestellt:** Wird in einer AWS-Kundenumgebung bereitgestellt. Alle AWS-Konten werden vom Kunden verwaltet.

AWS-Kompetenzprogramm für den Einzelhandel – Voraussetzungen

Die folgenden Elemente werden durch den Manager für das AWS-Kompetenzprogramm validiert. Fehlende oder unvollständige Informationen müssen vor der Terminierung der Technologievalidierungsüberprüfung bereitgestellt werden.

1.0 Teilnahme am APN-Programm		Erfüllt J/N
1.1 Technologiepartnerstufe	APN-Partner müssen die Programmrichtlinien und -definitionen lesen, bevor sie sich für das AWS-Kompetenzprogramm für den Einzelhandel bewerben. Hier finden Sie die Programmdetails	
1.2 Technologiepartnerstufe	Der APN-Partner muss ein APN-Technologiepartner der Stufe "Advanced" sein, bevor er sich für das AWS-Kompetenzprogramm für den Einzelhandel bewirbt.	
1.3 Lösungskategorie	Der APN-Partner muss eine Segmentkategorie für seine Lösung auswählen: ☐ **Kundenbindung** ☐ **Absatzförderung und -planung** ☐ **Lieferkette und Vertrieb** ☐ **Physischer, digitaler und virtueller Speicher** ☐ **Fortschrittliche Datenwissenschaft für den Einzelhandel** ☐ **Kerngeschäftsanwendungen für den Einzelhandel** Der APN-Partner muss eine Bereitstellungskategorie für seine Lösung auswählen: ☐ **SaaS** ☐ **Vom Kunden bereitgestellt**	
1.4 Kundenakzeptanz	Der APN-Partner muss offenlegen, wie viele Kunden seine Lösung insgesamt nutzen.	
2.0 Fallstudien		**Erfüllt J/N**
2.1 Einzelhandelsspezifische Fallstudien	Der APN-Partner muss 4 Fallstudien für eine einzelne Einzelhandelslösung prüfen lassen. Jede der 4 Fallstudien muss sich auf ein Beispiel der APN-Partnerlösung beziehen, die in einer der sechs Segmentkategorien angewendet wird (Kundenbindung, Absatzförderung und -planung, Lieferkette und Vertrieb, physischer, digitaler und virtueller Speicher, fortschrittliche Datenwissenschaft für den Einzelhandel und Kerngeschäftsanwendungen für den Einzelhandel). APN-Partner, die bereits über eine Kompetenz in den Bereichen AWS Digital Customer Experience (DCX), Data & Analytics, IoT, Migration und/oder Machine Learning verfügen, können bis zu 4 Kundenfallstudien wiederverwenden, die für Projekte eingereicht wurden, die hochspezialisierte Lösungen für branchenspezifische Herausforderungen bzw. Beratungspraktiken mit einzigartigem Segmentswissen bezüglich des Einzelhandels aufweisen. Für jede einzelne Fallstudie muss der APN-Partner die folgenden Informationen bereitstellen: ▪ Name des Kunden ▪ Website des Kunden ▪ Kundenproblem ▪ Art und Weise der Bereitstellung der Lösung zur Beantwortung der Herausforderung ▪ Verwendete externe Anwendungen oder Lösungen ▪ Datum, am die Referenz in Produktion gegangen ist ▪ Ergebnisse ▪ Spezifische Architekturdiagramme, Bereitstellungshandbücher und weitere Materialien, in Abhängig von der Art der Lösung, gemäß Beschreibung im nächsten Abschnitt. Diese Informationen werden im Rahmen der Programmbewerbung in APN Partner Central abgefragt. Die im Rahmen dieser Fallstudie bereitgestellten Informationen können privat sein und werden nicht veröffentlicht.	

	Alle 4 bereitgestellten Fallstudien werden bei der Dokumentationsprüfung der technischen Validierung überprüft. Die Fallstudie wird aus der Berücksichtigung im Rahmen der Kompetenzen entfernt, wenn der APN-Partner die erforderliche Dokumentation, die für die Bewertung der Studie gegen die einzelnen Checklisten-Posten benötigt wird, nicht bereitstellen kann, oder wenn einzelne Checklisten-Posten nicht erfüllt werden können. Fallstudien müssen die Bereitstellungen beschreiben, die innerhalb der vergangenen 18 Monate ausgeführt wurden, und müssen sich auf Projekte beziehen, die bei Kunden in der Produktion sind. Nicht zulässig sind Pilotprojekte oder Projekte im Status der Machbarkeitsüberprüfung.	
2.2 Öffentlich verfügbare Fallstudien	Öffentlich verfügbare Fallstudien werden von AWS nach Genehmigung der Kompetenz verwendet, um den Erfolg des APN-Partners auf Basis messbarer KPIs nachzuweisen und Kunden die Gewissheit zu geben, dass der APN-Partner über die erforderliche Erfahrung und das nötige Wissen verfügt, um Lösungen für die Kundenprobleme zu entwickeln und bereitzustellen. 2 der 4 Kundenbereitstellungen, die mit den Fallstudien verknüpft sind, müssen durch den APN-Partner als öffentlich verfügbare Fallstudien veröffentlicht werden. Diese öffentlich verfügbaren Fallstudien können in Form von formalen Fallstudien, Whitepapers oder Blog-Posts veröffentlicht werden.	
	Öffentlich verfügbare Fallstudien müssen auf der APN-Partnerwebsite einfach zu finden sein. So muss es beispielsweise möglich sein, über die APN-Partner-Startseite zu den öffentlich verfügbaren Fallstudien zu navigieren, und der APN-Partner muss in seinen Anwendungen Links zu diesen öffentlich verfügbaren Fallstudien implementieren.	
	Öffentlich verfügbare Fallstudien müssen die folgenden Elemente aufweisen: ▪ Bezüge auf den Kundennamen, APN-Partnernamen und AWS ▪ Kundenproblem ▪ Art und Weise der Bereitstellung der Lösung zur Beantwortung der Herausforderung ▪ Art und Weise, wie AWS-Services als Teil der Lösung genutzt wurden ▪ Ergebnisse	
3.0 AWS-Web-Präsenz und Vordenkerposition im Einzelhandel		**Erfüllt J/N**
3.1 APN-Partner-AWS-Landingpage	Mit der Internetpräsenz eines APN-Partners, die sich auf die AWS-Einzelhandelslösungen bezieht, gewinnen Kunden Vertrauen in die Fähigkeiten und die Erfahrung des APN-Einzelhandelspartners. Der APN-Partner muss eine AWS-Landingpage einrichten, auf der er seine AWS-Einzelhandelslösung beschreibt, Links zu seinen öffentlich verfügbaren Fallstudien einbindet, Technologiepartnerschaften auflistet und weitere relevante Informationen bereitstellt, die die Fachkenntnis des APN-Partners in Bezug auf Einzelhandelslösungen unter Beweis stellt und die Arbeit mit AWS hervorhebt. Diese AWS-spezifische Einzelhandelsseite muss über die APN-Partner-Startseite erreichbar sein. Die Startseite selbst wird nicht als eine AWS-Landingpage anerkannt, es sei denn, der APN-Partner ist ein dediziertes Einzelhandels-Technologieunternehmen und die Startseite spiegelt den Fokus des APN-Partners auf den Einzelhandel wider.	
3.2 Vordenkerposition im Einzelhandel	AWS-Kompetenzpartner im Bereich Einzelhandel werden aufgrund ihrer innovativen Lösungen, die AWS-Services nutzen oder die Verwaltung dieser unterstützen, als Experten mit umfassender Fachkompetenz im Bereich Einzelhandel anerkannt. APN-Partner müssen für die Öffentlichkeit zugänglich Materialien (z. B. Blog-Posts, Presseartikel, Videos usw.) bereitstellen, mit denen sie den Fokus und die Fachkenntnis des APN-Partners in Bezug auf den Einzelhandel unter Beweis stellen. Es müssen Links zu Materialbeispielen bereitgestellt werden, die in den vergangenen zwölf Monaten veröffentlicht wurden.	

4.0 Geschäftliche Anforderungen		
4.1 Einsatzbereite Toolkits	Der APN-Partner verfügt über eine praxistaugliche Dokumentation und Verkäufer-Toolkits mit einem klaren Produktnutzenversprechen, das der AWS-Vertriebsorganisation mit allen relevanten Informationen, die zur Feststellung der Eignung für eine Kundenchance erforderlich sind (z. B. Verkaufshilfen, Präsentationen und Kundennutzungsfälle), übermittelt werden kann. Der Nachweis muss in Form von Verkaufsmaterialien erfolgen, einschließlich einer Präsentation, eines Einseiters und einer Checkliste für den Anwendungsfall.	
4.2 Produktsupport/ Helpdesk	APN-Partner bieten Kunden Support über Web-Chat, Telefon oder per E-Mail an. Der Nachweis muss in Form der Beschreibung des Supports erbracht werden, der Kunden für ihr Produkt oder ihre Lösung angeboten wird.	
4.3 Produkt ist auf AWS Marketplace gelistet	Der APN-Partner bietet Lösungen über AWS Marketplace an. ☐ Ja ☐ Nein Falls "Ja", muss der APN-Partner einen Link zum AWS Marketplace-Listing bereitstellen. Falls "Nein", sind keine weiteren Informationen erforderlich.	
4.4 Umsatzvergütung für gemeinsame AWS-Verkaufsmöglichkeiten	Der APN-Partner hat Umsatzvergütungspläne für seine gemeinsamen AWS-Verkaufsmöglichkeiten. ☐ Ja ☐ Nein ☐ Erklärung: _____ Der Nachweis muss in Form einer kurzen Beschreibung des Vergütungsplans für die Verkäufer des APN-Partners erfolgen.	
4.5 Gemeinsame AWS-/ APN-Partner-Erfolge	Der APN-Partner hat einen Prozess zur Dokumentation und Veröffentlichung von gemeinsamen Erfolgen. Der Nachweis muss in Form einer verbalen Beschreibung des Prozesses erfolgen.	
5.0 APN-Partner-Selbsteinschätzung		**Erfüllt J/N**
5.1 Selbsteinschätzung zur Validierungscheckliste des AWS-Kompetenzprogramms	Der APN-Partner muss eine Selbsteinschätzung in Bezug auf die Erfüllung der Validierungscheckliste für AWS-Einzelhandels-Technologiepartner durchführen. ▪ Der APN-Partner muss alle Abschnitte der Checkliste ausfüllen. ▪ Die ausgefüllte Selbsteinschätzung muss per E-Mail an die Adresse **competency-checklist@amazon.com** gesendet werden. Dabei gilt die folgende Konvention für die E-Mail-Betreffzeile: "[APN-Partnername], Selbsteinschätzung als Einzelhandels-Kompetenztechnologiepartner abgeschlossen." ▪ Es wird empfohlen, dass der APN-Partner die ausgefüllte Selbsteinschätzung vor der Übermittlung an AWS durch den zugewiesenen Partner Solutions Architect, Partner Development Representative (PDR) oder Partner Development Manager (PDM) überprüfen lässt. Damit soll sichergestellt werden, dass das AWS-Team beim APN-Partner einbezogen wird und daran arbeitet, vor der Überprüfung Empfehlungen bereitzustellen und eine produktive Überprüfungserfahrung zu gewährleisten.	

Einzelhandels-Kompetenzprogramm: Validierungscheckliste für Technologiepartner

Die folgenden Aspekte werden durch einen externen Prüfer und/oder AWS Partner Solutions Architects validiert. Fehlende oder unvollständige Informationen müssen vor der Vereinbarung eines Termins für die Technologievalidierungsprüfung bereitgestellt werden.

		Gilt für:		
Technische Validierung		SaaS	Vom Kunden auf AWS bereitgestellt	Erfüllt J/N
Architekturdiagramm	Je nach Bereitstellungskategorie ist mindestens ein Architekturdiagramm erforderlich. Jedes Architekturdiagramm muss die folgenden Elemente enthalten: ☐ Die wichtigsten Elemente der Architektur und wie sie sich zusammenschließen, um die Partnerlösung den Kunden bereitzustellen ☐ Alle verwendeten AWS-Services über die entsprechenden AWS-Service-Symbole. ☐ Art und Weise der Bereitstellung der AWS-Services, darunter Amazon Virtual Private Cloud (VPCs), Availability Zones (AZs), Teilbereiche und Verbindungen zu Systemen außerhalb von AWS. ☐ Enthält Elemente, die außerhalb von AWS bereitgestellt wurden, z. B. standortbasierte Komponenten oder Hardware-Geräte.	Ja – eines für die ganze Lösung und eines für die Fallstudie	Ja – eines für jede einzelne Fallstudie	
Bereitstellungshandbuch	Das Bereitstellungshandbuch muss die bewährten Methoden für die Bereitstellung der APN-Partnerlösung auf AWS enthalten, sowie alle Abschnitte, die in den "Handbüchern für die Basisanforderungen für die Bereitstellung" aufgeführt sind.	Nein	Ja – eines für die Lösung.	
Ausgefüllte Validierungscheckliste	Für jede der 4 Fallstudien, die für die Partnerlösung eingereicht wurden, muss der APN-Partner eine ausgefüllte Version der folgenden Checkliste bereitstellen, um zu belegen, welche Checklistenposten erfüllt sind.	Ja	Ja	
1.0 Sicherheit **Die Säule zur Sicherheit setzt den Fokus auf den Schutz von Informationen und Systemen. Zu den wichtigsten Themen zählen Vertraulichkeit und Integrität von Daten, das Nutzen der Berechtigungsverwaltung, um zu identifizieren und zu verwalten, wer welche Aufgaben ausführen darf, und das Aufbauen von Kontrollen zur Erkennung von Sicherheitsereignissen.**				
1.1 Stammbenutzer für AWS-Konto für Routineaktivitäten nicht verwendet	Der Stammbenutzer für das AWS-Konto darf für Routineaktivitäten nicht verwendet werden. Nach der Erstellung Ihres AWS-Kontos sollten Sie sofort AWS Identity and Access Management (IAM)-Benutzerkonten erstellen und diese IAM-Benutzerkonten für alle Routineaktivitäten verwenden. Sobald Ihre IAM-Benutzerkonten erstellt wurden, sollten Sie die Anmeldeinformationen für das AWS-Stammkonto sicher speichern und sie nur für wenige Konto- und Serviceverwaltungsaufgaben verwenden, für die ein Stammbenutzer für das AWS-Konto erforderlich ist. Weitere Informationen zur Einrichtung von IAM-Benutzerkonten und -gruppen für den alltäglichen Bedarf finden Sie unter Erstellen Ihres ersten Administratorbenutzers und Ihrer ersten Administratorgruppe in IAM.	Ja	Nein	

1.2 Multi-Factor Authentication (MFA) wurde für Stammbenutzer auf dem AWS-Konto aktiviert	Multi-Factor Authentication (MFA) muss für Ihren Stammbenutzer auf dem AWS-Konto aktiviert werden. Da Ihr Stammbenutzer auf dem AWS-Konto vertrauliche Aktivitäten in Ihrem AWS-Konto ausführen kann, kann das Hinzufügen einer zusätzlichen Authentifizierungsebene helfen, Ihr Konto besser zu schützen. Es sind mehrere MFA-Typen verfügbar, darunter virtuelle MFA und Hardware-MFA.	Ja	Nein	
1.3 Für alle Routineaktivitäten verwendete IAM-Benutzerkonten	Der Stammbenutzer für das AWS-Konto darf nur verwendet werden, wenn dies unabdingbar ist. Erstellen Sie für alle anderen Aktivitäten für jede Person, die Administratorrechte benötigt, einen neuen IAM-Benutzer. Definieren Sie diese Benutzer anschließend als Administratoren, indem Sie die Benutzer in eine Administratorgruppe setzen, mit der Sie die verwaltete Richtlinie "AdministratorAccess" verknüpfen. Anschließend sollten die Benutzer in der Administratorgruppe die Gruppen, Benutzer usw. für das AWS-Konto einrichten. Alle künftigen Interaktionen sollten über die Benutzer des AWS-Kontos und ihre eigenen Schlüssel, statt über den Stammbenutzer erfolgen. Für einige Konto- und Serviceverwaltungsaufgaben müssen Sie sich jedoch mit den Anmeldeinformationen des Stammbenutzers anmelden.	Ja	Nein	
1.4 Multi-Factor Authentication (MFA) für alle interaktiven IAM-Benutzer aktiviert	Sie müssen MFA für alle interaktiven IAM-Benutzer aktivieren. Mit MFA verfügen Benutzer über ein Gerät, das einen eindeutigen Authentifizierungscode (ein Einmal-Passwort oder OTP) generiert. Benutzer müssen ihre normalen Anmeldeinformationen (Benutzername und Passwort) sowie das Einmal-Passwort eingeben. Das MFA-Gerät kann entweder ein spezielles Hardware-Teil oder ein virtuelles Gerät sein, das in einer App auf einem Smartphone ausgeführt wird.	Ja	Nein	
1.5 Regelmäßige Änderung von IAM-Anmeldeinformationen	Sie müssen Ihre Passwörter und Zugriffsschlüssel regelmäßig ändern und sicherstellen, dass alle IAM-Benutzer in Ihrem Konto Ihrem Beispiel folgen. Auf diese Weise können Sie die zulässige Nutzungsdauer für Anmeldeinformationen für den Zugriff auf Ihre Ressourcen beschränken, falls einmal ein Passwort oder ein Zugriffsschlüssel ohne Ihr Wissen kompromittiert wurde. Sie können Ihr Konto mit einer Passwort-Richtlinie belegen, die all Ihre IAM-Benutzer zum Ändern ihrer Passwörter auffordert, und Sie können wählen, wie häufig Ihre Benutzer ihre Passwörter ändern müssen. Weitere Informationen zum Ändern von Zugriffsschlüsseln für IAM-Benutzer finden Sie unter Rotieren der Zugriffsschlüssel.	Ja	Nein	
1.6 Richtlinie für starke Passwörter für IAM-Benutzer vorhanden	Sie müssen eine Richtlinie für starke Passwörter für Ihre IAM-Benutzer konfigurieren. Wenn Sie Benutzern genehmigen, ihre eigenen Passwörter zu ändern, müssen Sie sie zur Verwendung von starken Passwörtern und zum regelmäßigen Ändern ihrer Passwörter verpflichten. Auf der Seite "Account Settings" in der IAM-Konsole können Sie eine Passwort-Richtlinie für Ihre Konten erstellen. Sie können die Passwort-Richtlinie verwenden, um Passwort-Anforderungen zu definieren, z. B. eine Mindestlänge, ob nicht-alphanumerische Zeichen zulässig sind, wie häufig ein Passwort geändert werden muss usw. Weitere Informationen finden Sie unter Einrichten einer Kontopasswortrichtlinie für IAM-Benutzer.	Ja	Nein	

1.7 Keine gemeinsame Verwendung von IAM-Anmeldeinformationen durch mehrere Benutzer	Sie müssen jeweils ein individuelles IAM-Benutzerkonto für alle Benutzer erstellen, die den Zugriff auf Ihr AWS-Konto benötigen. Erstellen Sie auch einen IAM-Benutzer für Sie selbst, verknüpfen Sie diesen Benutzer mit Administratorberechtigungen, und verwenden Sie diesen IAM-Benutzer für alle Ihre Aktivitäten. Durch das Erstellen individueller IAM-Benutzer für Personen, die auf Ihr Konto zugreifen möchten, können Sie für jeden IAM-Benutzer einen einmaligen Satz mit Sicherheitsanmeldeinformationen einrichten. Sie können außerdem verschiedene Berechtigungen für die einzelnen IAM-Benutzer einrichten. Bei Bedarf können Sie die Berechtigungen eines IAM-Benutzers jederzeit ändern oder widerrufen. (Wenn Sie die Anmeldeinformationen für Ihren Stammbenutzer preisgeben, kann es mitunter schwierig sein, diese Informationen zu widerrufen, und es ist nicht möglich, die jeweiligen Berechtigungen zu beschränken.)	Ja	Nein	
1.8 Herunterskalierung der IAM-Richtlinien auf die geringsten Rechte	Sie müssen der Standardsicherheitsempfehlung für das Gewähren von geringsten Rechten folgen. Dies bedeutet, dass nur die Berechtigungen gewährt werden, die für die Ausführung einer Aufgabe zwingend erforderlich sind. Bestimmen Sie, welche Aufgaben Benutzer ausführen müssen, und entwickeln Sie anschließend Richtlinien für diese Aufgaben, damit Benutzer ausschließlich zur Ausführung dieser Aufgaben berechtigt sind. Beginnen Sie mit einem Mindestberechtigungssatz, und gewähren Sie bei Bedarf weitere Berechtigungen. Dieser Ansatz ist sicherer, als mit Berechtigungen zu starten, die sich als zu milde herausstellen und daher später stark eingeschränkt werden müssen. Die Definition des richtigen Berechtigungssatzes erfordert ein gewisses Maß an Recherche. Bestimmen Sie, welche Berechtigungen für eine bestimmte Aufgabe erforderlich sind, welche Aktionen von einem bestimmten Service unterstützt werden und welche Berechtigungen erforderlich sind, um diese Aktionen auszuführen.	Ja	Nein	
1.9 Keine Verwendung von hartcodierten Anmeldeinformationen (z. B. Zugriffsschlüssel)	Sie müssen den bewährten Methoden für die Verwaltung von AWS-Zugriffsschlüsseln folgen und die Verwendung von hartkodierten Anmeldeinformationen vermeiden. Wenn Sie programmgesteuert auf AWS zugreifen, verwenden Sie einen Zugriffsschlüssel, um Ihre Identität und die Identität Ihrer Anwendungen zu überprüfen. Jede Person, die auf Ihren Zugriffsschlüssel zugreifen kann, besitzt dieselbe Stufe für den Zugriff auf AWS-Ressourcen wie Sie selbst. Daher hat AWS sich für erhebliche Längen zum Schutz Ihrer Zugriffsschlüssel entschieden. Und um Ihrem Anteil an unserem Modell einer gemeinsamen Verantwortung gerecht zu werden, sollten Sie diesem Beispiel folgen.	Ja	Ja	
1.10 Verschlüsselung aller Anmeldeinformationen beim Speichern	Mit dieser grundlegenden Anforderung soll die Verschlüsselung aller gespeicherten Anmeldeinformationen gewährleistet werden.	Ja	Ja	
1.11 Verwendung von AWS-Zugriffsschlüsseln nur von interaktiven Benutzern	Es sollten keine AWS-Zugriffsschlüssel verwendet werden, mit Ausnahme der folgenden Fälle: 1. Werden von Personen verwendet, um auf AWS-Services zuzugreifen und werden auf einem Gerät gespeichert, das von diesen Personen kontrolliert wird. 2. Wird von einem Service verwendet, um auf AWS-Services zuzugreifen, jedoch nur in Fällen, in denen: a) es nicht möglich ist, eine Amazon EC2-Instance-Rolle, eine Amazon Elastic Container Service (Amazon ECS)-	Ja	Ja	

	Aufgabenrolle oder einen vergleichbaren Mechanismus zu verwenden, b) die AWS-Zugriffsschlüssel mindestens einmal pro Woche geändert werden und c) die IAM-Richtlinie fest umrissen und wie folgt definiert ist: i) Es wird ausschließlich Zugriff auf spezifische Methoden und Ziele gewährt, ii) und der Zugriff ist beschränkt auf Teilnetze, über die auf die Ressourcen zugegriffen wird.			
1.12 AWS CloudTrail für alle AWS-Konten in allen Regionen aktiviert	AWS CloudTrail muss auf allen AWS-Konten und in jeder Region aktiviert werden. Der Einblick in Ihre AWS-Kontoaktivität ist ein wesentlicher Aspekt für Sicherheit und bewährte Methoden in Unternehmen. Sie können AWS CloudTrail zum Anzeigen, Suchen, Herunterladen, Archivieren, Analysieren und Antworten auf Kontoaktivitäten in Ihrer gesamten AWS-Infrastruktur verwenden. Sie können identifizieren, welche Person oder welcher Vorgang welche Aktion ausgeführt hat, welche Ressourcen betroffen sind und wann das Ereignis auftrat. Außerdem können Sie weitere Details anzeigen, die Ihnen helfen, Aktivitäten in Ihrem AWS-Konto zu analysieren und auf diese zu reagieren.	Ja	Nein	
1.13 Speicherung von CloudTrail-Protokollen in einem S3-Bucket, der im Besitz eines anderen AWS-Kontos ist	AWS CloudTrail-Protokolle müssen in ein Bucket im Besitz eines anderen AWS-Konto platziert werden, das für einen extrem eingeschränkten Zugriff konfiguriert ist, z. B. nur für Audits und Wiederherstellung.	Ja	Nein	
1.14 Versionierung oder MFA Delete im CloudTrail S3-Protokoll-Bucket aktiviert	Die Inhalte des AWS CloudTrail-Protokoll-Buckets müssen mit Versionierung oder MFA Delete geschützt werden.	Ja	Nein	
1.15 Amazon EC2-Sicherheitsgruppen eng dimensioniert	Alle Amazon EC2-Sicherheitsgruppen sollten den Zugriff auf das erforderliche Mindestmaß beschränken. Dazu gehört als Mindestanforderung: 1. Implementieren von Sicherheitsgruppen zur Beschränkung des Datenverkehrs zwischen dem Internet und Amazon VPC 2. Implementieren von Sicherheitsgruppen zur Beschränkung des Datenverkehrs innerhalb von Amazon VPC und 3. In allen Fällen Definieren von Einstellungen mit den größtmöglichen Beschränkungen.	Ja	Ja	
1.16 Amazon S3-Buckets in Ihrem Konto mit entsprechenden Zugriffsebenen ausgestattet	Sie müssen sicherstellen, dass die entsprechenden Kontrollen vorhanden sind, um den Zugriff auf die einzelnen Amazon S3-Buckets zu steuern. Wenn Sie AWS verwenden, hat es sich bewährt, den Zugriff auf Ihre Ressourcen auf jene Personen zu beschränken, die den Zugriff unbedingt benötigen (nach dem Prinzip des geringsten Rechts).	Ja	Ja	
1.17 Keine falsche Konfiguration von Amazon S3-Buckets für den öffentlichen Zugriff	Sie müssen sicherstellen, dass diese Buckets, die den öffentlichen Zugriff nicht gewähren sollten, so konfiguriert sind, dass ein öffentlicher Zugriff verhindert wird. Standardmäßig sind alle Amazon S3-Buckets privat. Der Zugriff ist nur für Benutzer möglich, denen der Zugriff ausdrücklich gewährt wurde. In den meisten Anwendungsfällen ist ein breit angelegter öffentlicher Zugriff zum Lesen von Dateien in Ihren Amazon S3-Buckets nicht erforderlich. Eine Ausnahme ist die Verwendung von Amazon S3 zum Hosten öffentlicher Werte (z. B. zum Hosten von Bildern zur Verwendung auf einer öffentlichen Website). Es hat sich bewährt, den Zugriff für die Öffentlichkeit grundsätzlich zu verhindern.	Ja	Ja	
1.18 Entwicklung eines Überwachungsmechanismus zur Ermittlung des Zeitpunkts für die Veröffentlichung von S3-Buckets oder Objekten	Überwachung oder Alarmierung müssen aktiviert sein, um zu identifizieren, wann Amazon S3-Buckets öffentlich werden. Eine Option, die sich dafür eignet, ist die Verwendung von AWS Trusted Advisor. AWS Trusted Advisor prüft Buckets in Amazon S3 mit offenen Zugriffsberechtigungen. Bucket-	Ja	Nein	

	Berechtigungen, die allen Benutzern Listenzugriff gewähren, können zu unerwartet umfangreicheren Gebühren führen, wenn Objekte in dem Bucket häufig durch unbeabsichtigte Benutzer aufgeführt werden. Bucket-Berechtigungen, die allen Benutzern den Zugriff zum Hochladen/Löschen einräumen, bergen ein hohes Potenzial für Sicherheitsrisiken, indem alle Personen Elemente in einem Bucket hinzufügen, ändern oder löschen können. Die Trusted Advisor-Prüfung untersucht explizite Bucket-Berechtigungen und zugeordnete Bucket-Richtlinien, die die Bucket-Berechtigungen möglicherweise überschreiben.			
1.19 Überwachungsmechanismus für die Erkennung von Änderungen in Amazon EC2-Instances und Containern	Alle Änderungen an Ihren Amazon S3-Instances oder Containern weisen möglicherweise auf unberechtigte Aktivitäten hin. Als Mindestanforderung müssen diese Aktivitäten in Form eines Protokolls auf einen dauerhaften Speicherort abgelegt werden, um künftige forensische Untersuchungen zu ermöglichen. Der für den Zweck verwendete Mechanismus muss die folgenden Mindestanforderungen erfüllen: 1. Ermittlung von Änderungen am BS oder den Anwendungsdateien in den Amazon S3-Instances oder Containern, die in der Lösung verwendet werden. 2. Speichern dieser Änderungen auf einem externen Speicherplatz außerhalb von der Amazon S3-Instance oder dem Container. Beispiele für geeignete Mechanismen: a: Bereitstellung einer Dateiintegritäts-prüfung über die geplante Konfigurationsverwaltung (z. B. Chef, Puppet usw.) oder ein spezielles Tool (z. B. OSSEC, Tripwire usw.) oder b: Ausweitung der Konfigurationsverwaltungs-Tools auf die Validierung der Amazon S3-Host-Konfiguration und Warnungen bei Aktualisierungen an wichtigen Konfigurationsdateien oder Paketen mit so genannten Canary-(logged no-op)-Ereignissen, die konfiguriert werden, um sicherzustellen, dass der Service während der Laufzeit auf allen betroffenen Hosts betriebsbereit bleibt. Bereitstellung eines Systems zur Angriffserkennung auf dem Host, wie z. B. eine Open-Source-Lösung wie OSSEC with ElasticSearch and Kibana oder eine Partnerlösung. Beachten Sie, dass die folgenden Mechanismen diese Anforderung nicht erfüllen: Häufig geänderte Amazon S3-Instances oder Container	Ja	Nein	
1.20 Klassifizierung aller Daten	Alle im Workload verarbeiteten und gespeicherten Kundendaten werden berücksichtigt und klassifiziert, um deren Vertraulichkeit und die entsprechenden Methoden für die Verarbeitung zu bestimmen.	Ja	Ja	
1.21 Verschlüsselung aller vertraulichen Daten	Alle als vertraulich klassifizierten Kunden werden bei der Übertragung und der Speicherung verschlüsselt.	Ja	Ja	
1.22 Sichere Verwaltung von kryptografischen Schlüsseln	Alle kryptografischen Schlüssel werden beim Speichern und der Übertragung verschlüsselt, und der Zugriff auf die Schlüssel wird über eine AWS-Lösung, wie z. B. AWS Key Management Service (KMS), oder eine Partnerlösung, wie z. B. HashiCorp Vault, gesteuert.	Ja	Ja	
1.23 Verschlüsselung aller Daten während der Übertragung	Alle Daten, die über die Grenzen der Amazon Virtual Private Cloud hinaus übertragen werden, sind verschlüsselt.	Ja	Ja	
1.24 Definition und Probe der Reaktion auf Sicherheitsvorfälle	Es muss ein Reaktionsprozess auf Sicherheitsvorfälle für die Behandlung von Vorfällen definiert werden, wie z. B. AWS-Kontokompromittierungen. Dieser Prozess muss getestet werden, indem Verfahren zum Proben der Vorfallsreaktion implementiert werden, z. B. durch das Absolvieren einer Sicherheitsübung im Rahmen eines Game Days. Eine solche Probe darf höchstens zwölf	Ja	Nein	

	Monate her sein, um Folgendes zu bestätigen: a: Die richtigen Personen haben Zugang zur Umgebung. b: Es sind die richtigen Tools verfügbar. c: Die richtigen Personen wissen, was zu tun ist, um auf diverse und in diesem Plan dargestellte Sicherheitsvorfälle zu reagieren.			
1.25 Payment Cart Industry (PCI) Data Security Standards (DSS) – Zertifizierung oder SAQ	Für E-Commerce-, Unified Commerce- und Point of Sale-Anwendungen, bei denen Kartenhalterdaten vorliegen, ist ein Prozess eingerichtet, der eine jährliche Bewertung des Umfangs der Payment Card Industry (PCI) Data Security Standards (DSS) für den Workload vornimmt. Basierend auf dem Bewertungsergebnis wird je nach Bedarf eine PCI DSS-Zertifizierung oder SAQ durchgeführt. Der Nachweis muss in Form eines Compliance-Berichts für die PCI DSS-Zertifizierung oder eines ausgefüllten Fragebogens zur Selbsteinschätzung (Self-Assessment Questionnaire, SAQ) erfolgen.	Ja	Ja	
1.26 End-to-End-Verschlüsselung von PCI-Daten	Für E-Commerce-, Unified Commerce- und Point of Sale-Anwendungen, bei denen Kartenhalterdaten vorliegen, werden die Daten selbst beim Übertragen innerhalb einer Amazon VPC verschlüsselt.	Ja	Ja	
1.27 Schutz vorhanden gegenüber DDoS-Angriffe (Distributed Denial Of Service)	Bereitstellen einer Infrastruktur und eines Service, die DDoS-Angriffe auf allen Ebenen des OSI-Modells (Open Systems Interconnection) entschärfen.	Ja	Nein	
1.28 Vorhandene Mechanismen zur Entschärfung der 10 wichtigsten Angriffe laut Open Web Application Security Project (OWASP)	Bereitstellen einer Infrastruktur und eines Service, die Open Web Application Security Project (OWASP)-Schwächen entschärfen.	Ja	Nein	
2.0 Zuverlässigkeit Die Säule für Zuverlässigkeit setzt den Fokus auf die Fähigkeit, Ausfälle zu vermeiden bzw. sich schneller von aufgetretenen Ausfällen zu erholen, um damit die Anforderungen von Unternehmen und Kunden zu erfüllen. Zu den wichtigsten Themen gehören grundlegende Elemente rund um Einrichtung, projektübergreifende Anforderungen, Wiederherstellungsplanung und Änderungsverwaltung.				
2.1 Hohe Verfügbarkeit der Netzwerkkonnektivität	Die Netzwerkkonnektivität für die Lösung muss hochverfügbar sein. Wenn Sie VPN oder AWS Direct Connect zum Verbinden mit Kundennetzwerken verwenden, muss die Lösung redundante Verbindungen unterstützen, selbst wenn die Kunden diese nicht immer implementieren.	Ja	Ja	
2.2 Infrastrukturskalierungs-mechanismen folgen Geschäftsanforderungen	Infrastrukturskalierungsmechanismen müssen Geschäftsanforderungen folgen. Dazu können Sie die folgenden Aktivitäten verwenden: 1. Implementieren von Auto Scaling-Mechanismen auf den einzelnen Ebenen der Architektur 2. Bestätigen, dass für aktuelle Geschäftsanforderungen, einschließlich Kostenanforderungen und erwarteter Anstieg der Benutzeranzahl, keine Auto Scaling-Mechanismen benötigt werden UND manuelle Skalierungsverfahren vollständig dokumentiert und häufig getestet werden.	Ja	Ja	
2.3 Zentrale Verwaltung von AWS- und Anwendungsprotokollen	Alle Protokollinformationen aus der Anwendung und aus der AWS-Infrastruktur müssen in ein System konsolidiert werden.	Ja	Nein	
2.4 Zentrale Verwaltung von Überwachung und Alarmen für AWS und Anwendungen	Die Anwendung und die AWS-Infrastruktur müssen zentral und auf Basis von Alarmen überwacht werden, die an das zuständige Ablaufpersonal gesendet werden.	Ja	Nein	
2.5 Automatisierung der Bereitstellung und Verwaltung der Infrastruktur	Die Lösung muss ein automatisiertes Tool, wie z. B. AWS CloudFormation oder Terraform, für die Bereitstellung und Verwaltung der AWS-Infrastruktur verwenden. Die AWS-Konsole darf nicht für Routineänderungen an der AWS-Produktionsinfrastruktur verwendet werden.	Ja	Ja	

2.6 Regelmäßige Datensicherungen	Sie müssen regelmäßige Sicherungen auf einen dauerhaften Speicherservice durchführen. Mit Sicherungen können Sie sicherstellen, dass Sie die Möglichkeit haben, administrative, logische oder physische Fehlerszenarien zu beheben. Amazon S3 und Amazon Glacier sind die idealen Services für Sicherung und Archivierung. Bei beiden Lösungen handelt es sich um dauerhafte und kostengünstige Speicherplattformen. Beide Lösungen bieten außerdem unbegrenzte Kapazität, und es entfällt die Volume- oder Datenträgerverwaltung, während das zu sichernde Datenaufkommen wächst. Durch das nutzungsabhängige Gebührenmodell und die geringen Kosten pro GB pro Monat eignen sich diese Services hervorragend für Anwendungsfälle im Bereich des Datenschutzes.	Ja	Ja	
2.7 Regelmäßige Tests der Wiederherstellungsmechanismen auf Basis eines Terminplans und nach signifikanten Änderungen an der Architektur	Sie müssen Wiederherstellungsmechanismen und -verfahren regelmäßig und nach signifikanten Änderungen an Ihrer Cloud-Umgebung testen. AWS bietet substanzielle Ressourcen, um Sie bei der Sicherung und Wiederherstellung Ihrer Daten zu unterstützen.	Ja	Nein	
2.8 Lösung bietet Ausfallsicherheit bei Unterbrechungen in Availability Zones	Die Lösung muss weiter funktionieren, wenn alle Services innerhalb einer Availability Zone unterbrochen sind.	Ja	Ja	
2.9 Ausfallsicherheit der Lösung getestet	Die Ausfallsicherheit der Infrastruktur bei Unterbrechungen in einer einzelnen Availability Zone wurde innerhalb der vergangenen zwölf Monate in der Produktion getestet, z. B. im Rahmen einer Übung an einem Game Day.	Ja	Nein	
2.10 Notfallwiederherstellung (DR) definiert	Ein gut strukturierter Notfallwiederherstellungsplan enthält einen Wiederherstellungszeitpunkt (RPO) und eine Wiederherstellungsdauer (RTO). Sie müssen einen RPO und eine RTO für alle betroffenen Services definieren, und der RPO und die RTO müssen mit dem SLA übereinstimmen, den Sie Ihren Kunden anbieten.	Ja	Ja	
2.11 Wiederherstellungsdauer (RTO) weniger als 24 Stunden	Als Grundanforderung sollte die Wiederherstellungsdauer (RTO) für Kernservices weniger als 24 Stunden betragen.	Ja	Nein	
2.12 Notfallwiederherstellungsplan ausreichend getestet	Ihr Notfallwiederherstellungsplan muss regelmäßig und nach wichtigen Aktualisierungen in Bezug auf Ihren Wiederherstellungszeitpunkt (RPO) und Ihre Wiederherstellungsdauer (RTO) getestet werden. Es muss mindestens ein Test der Notfallwiederherstellung vor der Genehmigung Ihrer AWS APN-Anwendung auf der Stufe "Advanced" abgeschlossen werden.	Ja	Nein	
2.13 Notfallwiederherstellungsplan enthält Wiederherstellung auf eine andere Region	Ihr Notfallwiederherstellungsplan muss eine Strategie für die Wiederherstellung auf eine andere AWS-Region enthalten, und im Rahmen Ihrer regelmäßigen Wiederherstellungstests muss dieses Szenario getestet werden. Sie haben in den vergangenen zwölf Monaten mindestens einen vollständigen Test des Notfallwiederherstellungsplans abgeschlossen, einschließlich mindestens einer Wiederherstellung auf eine andere AWS-Region. Hinweis: Obwohl Prozesse zur Wiederherstellung von Daten in Testumgebungen oder das Exportieren von Daten für Benutzer sinnvolle Möglichkeiten zur Überprüfung von Sicherungen darstellen, erfüllen diese Prozesse nicht die Anforderungen zum Ausführen einer vollständigen Wiederherstellung auf eine andere AWS-Region.	Ja	Nein	

3.0 Optimierung der Betriebsabläufe Die Säule zur Optimierung der Betriebsabläufe setzt den Fokus auf das Ausführen und Überwachen von Systemen für die Bereitstellung von geschäftlichem Nutzen und das kontinuierliche Verbessern von Prozessen und Abläufen. Die wichtigsten Themen umfassen die Verwaltung und Automatisierung von Änderungen, die Reaktion auf Ereignisse und das Definieren von Standards für die erfolgreiche Verwaltung von Routineabläufen.				
3.1 Bereitstellung von Code-Änderungen automatisiert	Die Lösung muss eine automatisierte Methode für die Bereitstellung von Code in die AWS-Infrastruktur verwenden. Interaktive Secure Shell (SSH)- oder Remote Desktop Protocol (RDP)-Sitzungen dürfen nicht für die Bereitstellung von Aktualisierungen in die AWS-Infrastruktur verwendet werden.	Ja	Nein	
3.2 Runbooks und Eskalationsprozess definiert	Runbooks müssen entwickelt werden, um die Standardverfahren für die Reaktion auf verschiedene Anwendungen und AWS-Ereignisse zu definieren. Ein Eskalationsprozess muss definiert werden, um durch das System generierte Warnungen und Alarme zu behandeln und auf von Kunden gemeldete Vorfälle zu reagieren. Der Eskalationsprozess muss, wenn zutreffend, außerdem die Eskalation auf den AWS-Support umfassen.	Ja	Nein	
3.3 AWS Business Support für das AWS-Konto aktiviert	Business Support muss aktiviert werden. Business Support (oder höher) ist eine AWS-Partnernetzwerkanforderung für Technologiepartner auf der Stufe "Advanced". Um sich für die Stufe "Advanced" zu qualifizieren, müssen Sie Business Support auf mindestens einem Ihrer AWS-Konten aktivieren.	Ja	Nein	
4.0 Leistungseffizienz Die Säule zur Leistungseffizienz setzt den Fokus auf die effiziente Nutzung von IT- und Computing-Ressourcen. Zu den wichtigsten Themen gehören die Auswahl der richtigen Ressourcentypen und der passenden Größen auf Basis von Workload-Anforderungen, Leistungsüberwachung und fundierten Entscheidungen zum Erhalt der Effizienz bei steigenden Geschäftsanforderungen.				
4.1 Leistungstest wird nach Bereitstellung aktiviert	Definieren messbarer Leistungsziele und Durchführen eines Leistungstests zur Überprüfung der Einhaltung dieser Leistungsziele vor dem Produktionsstart.	Ja	Ja	
4.2 Überwachung eingerichteter Schwellenwerte	Überwachung der Anwendungsleistung und vorhandene Mechanismen zum Auslösen von Alarmen, wenn Schwellenwerte unter- bzw. überschritten werden.	Ja	Ja	

AWS-Ressourcen:

Titel	Beschreibung
Erstellen einer Startseite zur Praxis	Bietet eine Anleitung zum Erstellen einer Praxis-/Lösungsseite, die die Voraussetzungen für das Programm erfüllt.
Verfassen eines öffentlichen Fallbeispiels	Bietet eine Anleitung zum Erstellen eines öffentlichen Fallbeispiels, das die Voraussetzungen für das Programm erfüllt.
Entwickeln eines Architekturdiagramms	Bietet eine Anleitung zum Erstellen eines Architekturdiagramms, das die Voraussetzungen für das Programm erfüllt.
Dokument zur Partnerbereitschaft	Bietet eine Anleitung und Beispiele für Best Practices zu den Voraussetzungen für das Programm.
AWS Well Architected Website	Behandelt bewährte Well Architected-Methoden