



Strategie zur Modernisierung des Bankwesens für das
Kundenlebenszyklusmanagement in der AWS -Cloud

AWS Prescriptive Guidance



AWS Prescriptive Guidance: Strategie zur Modernisierung des Bankwesens für das Kundenlebenszyklusmanagement in der AWS - Cloud

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Einführung	1
Herausforderungen bei der Modernisierung	2
Veränderte Erwartungen und Neobanken	2
Geschäftliches Problem	2
Kundenlebenszyklusverwaltung	3
Onboarding von Kunden	4
Onboardingreise	6
Serverless-Onboarding	7
Onboarding-Lösung	7
Sicherheits und Compliance	9
Häufig gestellte Fragen	11
Wie kann ich sicher sein, dass AWS Dienste keine personenbezogenen Daten speichern?	11
Ist die Architektur DSGVO-konform?	11
Wie kann ich eine angemessene Datenvertraulichkeit sicherstellen?	11
Kann ich eine AWS-Lösung zur Modernisierung des Bankwesens in jedes bestehende Bankensystem integrieren?	11
Kann ich den Onboarding-Dialog anpassen?	11
Nächste Schritte	12
Ressourcen	13
Dokumentverlauf	14
.....	xv

Strategie zur Modernisierung des Bankwesens für das Kundenlebenszyklusmanagement in der AWS Cloud

Patrick Rotzetter und Florent Batard, Amazon Web Services (AWS)

Juni 2022 ([Dokumentverlauf](#))

Die Finanzdienstleistungsbranche (FS) steht vor großen Umwälzungen. Immer mehr Kunden erwarten und bevorzugen sogar die vollständig digitalen Self-Service-Bankdienstleistungen, die Finanztechnologieunternehmen (Fintechs) und Neobanken (d. h. rein digitale Banken ohne physische Filialen) im Rahmen des Onboarding-Prozesses für Privatkunden anbieten. Traditionelle Finanzinstitute können mit Fintechs und Neobanken nicht Schritt halten. Dies liegt daran, dass die Bankprozesse in den meisten traditionellen Finanzinstituten immer noch manuell oder halbautomatisch ablaufen.

Es gibt keinen Standardrahmen für die Implementierung traditioneller Bankprozesse, obwohl diese Prozesse allen Finanzinstituten gemeinsam sind. Das Fehlen eines solchen Standardrahmens behindert Innovationen. Traditionelle Finanzinstitute sind beispielsweise nicht in der Lage, von einem der neuesten Trends im Bankwesen zu profitieren: integriertes Finanzwesen. Das ist die Fähigkeit von Nichtbanken, bankähnliche Services anzubieten. Weitere Informationen finden Sie unter [Was Embedded-Finance und banking-as-a-service Trends für Finanzdienstleistungen von McKinsey & Company bedeuten](#). Damit traditionelle Finanzinstitute von integriertem Finanzwesen profitieren können, müssen sie ihre Geschäftsmöglichkeiten nahtlos anderen Unternehmen zugänglich machen.

Diese Strategie definiert einen Modernisierungsansatz für die Implementierung skalierbarer und sicherer Standardbankprozesse mithilfe einer API-orientierten, serverlosen Architektur, die auf Cloud-Diensten basiert. AWS Um die Herausforderungen und Chancen dieses Ansatzes zu veranschaulichen, konzentriert sich diese Strategie auf eine Fallstudie zur Kundenlebenszyklusverwaltung (CLM). Zu den Zielgruppen dieser Strategie gehören CEOs, CFOs CIOs, und Führungskräfte im Privatkundengeschäft und in der Vermögensverwaltungsbranche.

Herausforderungen bei der Modernisierung des Bankwesens

Veränderte Kundenerwartungen und der Aufstieg der Neobanken

Die FS-Branche steht vor einem massiven Wandel. Kunden erwarten nicht nur eine vollständig digitale Reise, sondern auch ein personalisiertes Erlebnis. Um diese Kundenerwartungen zu erfüllen und mit Neobanken konkurrieren zu können, müssen sich traditionelle Finanzinstitute einer massiven Transformation unterziehen, die Geschwindigkeit, Agilität und Innovation erfordert. Diese Transformation erfordert, dass traditionelle Finanzinstitute die folgenden kurzfristigen Herausforderungen bewältigen:

1. Traditionelle Banken müssen mit den Neobanken Schritt halten, die aufgrund des Mangels an technischer und prozessualer Tiefe agiler sind.
2. Traditionelle Finanzinstitute müssen integrierte Bankdienstleistungen im Rahmen von Banking-as-a-Service (BaaS) entwickeln und anbieten.
3. Traditionelle Finanzinstitute müssen anpassbare und flexible Kundenerlebnisse entwickeln und ermöglichen, die Modelle des Machine Learnings schnell und kostengünstig integrieren.

Die wichtigsten strategischen Faktoren, die es in den nächsten Jahren zu berücksichtigen gilt, sind die Nutzung integrierter Cloud-Services und die Erzielung von Vorteilen bei der Markteinführung, die sich aus der Zusammenarbeit mit Serviceanbietern und der agilen Transformation ergeben.

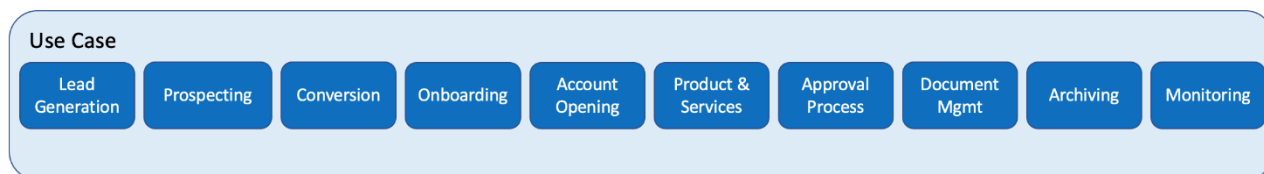
Geschäftliches Problem

Traditionelle Finanzinstitute arbeiten immer noch mit manuellen oder halbautomatischen Prozessen. Für reguläre Bankprozesse wird kein Industriestandard angewendet, obwohl diese Prozesse allen Finanzinstituten in ähnlichen Jurisdiktionen gemeinsam sind. Um diese Herausforderungen zu bewältigen, können traditionelle Finanzinstitute skalierbare und sichere Standardprozesse implementieren, indem sie einen serverlosen Ansatz verwenden, der auf AWS Cloud-Diensten basiert. Zum Beispiel [Amazon Lex](#) und [Amazon Rekognition](#) stellen trainierte Modelle für Machine Learning bereit, die Sie in verbesserte Kundenerlebnisse integrieren können. Bisher wurden solche Innovationen durch komplexe Integrations- und teure Entwicklungsprozesse behindert, aber jetzt sind diese Innovationen über API-Aufrufe direkt für Kundenanwendungen verfügbar.

AWS Cloud-Dienste bieten nicht nur zusätzliche Innovationen und eine schnelle Integration, sondern nutzen auch die neuesten Sicherheitsfunktionen, um die Vertraulichkeit und den Datenschutz von Daten zu gewährleisten. Wir möchten diesen Modernisierungsansatz für das Bankwesen für die CLM-Landschaft hervorheben. Der Kundenlebenszyklus steht im Mittelpunkt der Kundenbeziehung, weshalb er dringend modernisiert und sogar digitalisiert werden muss. [Wie in Was die Trends Embedded-Finance und Banking-as-a-Service für Finanzdienstleistungen von McKinsey & Company bedeuten](#), dargelegt, müssen Banken, die BaaS anbieten wollen, dafür sorgen, dass es funktioniert, und „damit es funktioniert, sind neue Technologien und Funktionen erforderlich, da BaaS in der Regel über APIs an Kunden verteilt wird und ein starkes Risiko- und Compliance-Management des eingebetteten Finanzpartners erfordert“. Im Abschnitt Serverless-Onboarding in dieser Strategie wird erklärt, wie Sie eine solche Strategie zum Laufen bringen können.

Anwendungsfall für die Kundenlebenszyklusverwaltung

Bei CLM handelt es sich um eine Reihe grob voneinander abhängiger und verbindlicher Prozesse, die die Geschäftsinteraktion eines Kunden mit seinem Finanzinstitut oder Versicherer definieren. Die folgende Abbildung bietet einen allgemeinen Überblick über die CLM-Phasen für die Banken- und Versicherungsbranche:



Beachten Sie, dass diese Prozesse je nach Kundensegment variieren. Beispielsweise unterscheidet sich das Onboarding von Geschäftskunden vom Onboarding von Privatkunden. Die Prozesse können auch von Branche zu Branche variieren. Das Onboarding eines Bankkunden unterscheidet sich vom Onboarding eines Versicherungskunden. Diese Strategie konzentriert sich auf die Erfahrung der Privatkunden im Bankgeschäft.

In der Abbildung oben stellt jedes Feld (Kundenakquise zum Beispiel) einen Kandidaten für eine Modernisierung dar. Sie können ein Diagramm wie dieses verwenden, um den Anwendungsfall in einzelne, unabhängige Anwendungsfälle zu unterteilen. Zum Beispiel kann der Kundenakquise-Anwendungsfall in einzelne Anwendungsfälle unterteilt werden. Anschließend können Sie jeden unabhängigen Anwendungsfall vorhandenen Funktionen zuordnen, entweder von Cloud-Serviceanbietern oder BaaS-Anbietern. Diese Kartierung kann zeigen, dass die Dokumentenarchivierung für Bankgeschäfte beispielsweise ein eigenständiger Service sein kann, der von einer externen Partei bereitgestellt wird. Die Aufteilung der Anwendungsfälle für die

Kundenlebenszyklusverwaltung in separate, unabhängige Anwendungsfälle ermöglicht es Ihnen, zielgerichtete Services zu entwerfen und zu entwickeln.

Diese Strategie konzentriert sich auf den beispielhaften Anwendungsfall der Eröffnung eines neuen Bankkontos. Für Kunden ist dies oft ein langwieriger, sehr manueller und fehleranfälliger Prozess, der zu Frustration und Unzufriedenheit führt. Heute erfolgt der Großteil des Onboardings immer noch manuell über Telefonanrufe oder physische Kontaktpunkte. Untersuchungen deuten jedoch darauf hin, dass Kunden ein digitales Erlebnis bevorzugen. Laut [Digitales Onboarding im Finanzwesen: ein neuartiges Modell und damit verbundene Cybersicherheitsrisiken](#) von Open Research Europe ziehen es 70 Prozent der Kunden vor, Produkte digital abzuschließen.

Möglichkeiten zum Onboarding von Kunden

In der Zeit nach der COVID-Krise müssen sich Bank- und Finanzkunden mit umständlichen und komplexen Prozessen auseinandersetzen. Tatsächlich können heute nur wenige Kunden den gesamten Prozess der Eröffnung eines Girokontos von einem mobilen Gerät aus abschließen. Die Mehrheit der Kunden muss zur Eröffnung eines Bankkontos einen manuellen Onboarding-Prozess befolgen, der dem folgenden ähnelt:

1. Der Kunde oder Endbenutzer muss einen Identitätsnachweis, einen gültigen Ausweis und verschiedene andere Datenpunkte einreichen. In vielen Fällen umfassen diese Datenpunkte Unterlagen für eine physische Adresse, einen Beschäftigungsnachweis und mehr. Oft muss der Kunde eine Filiale aufsuchen, um diese Informationen bereitzustellen, oder sie per Standardpost an die Bank senden.
2. Bevor Kunden ihre Bankkonten überhaupt nutzen können, erhalten sie mehrere Papierdokumente. Anschließend müssen die Kunden die Dokumente unterschreiben und an die Bank zurücksenden (d. h. Einzelverträge für jedes Bankprodukt, wie Privatkonten, Gemeinschaftskonten, Handelskonten, E-Banking, Kreditkarten oder Sicherheitscodes).
3. Die Bank digitalisiert alle unterschriebenen Dokumente und verknüpft sie mit dem „In Bearbeitung“ befindlichen Konto, um das Konto betriebsbereit zu machen.
4. Je nach Kundensegment oder Risikobewertung des Antragstellers muss die Bank diesen Vorgang regelmäßig teilweise oder vollständig wiederholen.
5. Wenn die Adresse, der Zivilstand oder andere Daten des Kunden, die als „Änderung der Umstände“ angesehen werden, aktualisiert werden, wird der Prozess erneut eingeleitet.

Der Abschluss dieses Prozesses kann mehrere Tage oder sogar Wochen dauern und erfordert häufig das Eingreifen und die Genehmigung durch mehrere Bankangestellte aus verschiedenen Abteilungen.

Die Onboarding-Kundenreise

Eine modernisierte Kundenerfahrung bei der Kontoeröffnung sollte die folgenden Features und Fähigkeiten beinhalten:

- Der Kunde kann über eine Internet-Website, einen virtuellen Assistenten oder ein Call Center auf den Onboarding-Service zugreifen. Der virtuelle Assistent kann ein text- oder sprachorientierter Chatbot sein, der in eine Webseite oder in eine Messaging-Anwendung wie Messenger oder Telegram integriert werden kann.
- Virtuelle Assistenten können mit Kunden interagieren, indem sie vordefinierte Absichten verwenden, um die Bedürfnisse und den Hintergrund des Kunden zu verstehen. Der virtuelle Assistent kann Kunden beispielsweise bitten, ihre Interessen mitzuteilen, persönliche Daten mitzuteilen, um ein Konto zu eröffnen, ihren Ausweis zu scannen und ein Selfie zu machen oder zu bestätigen, dass sie mit der Kontoeröffnung fortfahren möchten.
- Der Chatbot wird mehrsprachig sein.
- Kunden können mit dem Chatbot per Sprache oder Text interagieren.
- Nachdem Sie alle erforderlichen Informationen vom Kunden gesammelt haben, können Sie die Informationen an die Bank senden, um den Kontoeröffnungsprozess einzuleiten. Der Kunde erhält eine E-Mail-Benachrichtigung, in der bestätigt wird, dass der Vorgang gestartet wurde.
- Sie können den Dialog schließen, nachdem das Konto eröffnet wurde.
- Vermeiden Sie es, Kundeninformationen in der Cloud zu speichern. Diese Informationen müssen vorübergehend sein und nur während der Kundenbindung existieren. Nach Abschluss der Kontoeröffnung müssen Sie die Daten löschen und, wenn möglich, Belege für die Löschung vorlegen. Auch wenn der Dialog unterbrochen wird, müssen Sie bestätigen, dass alle persönlichen Daten gelöscht wurden (kein Zwischenspeichern).
- Vermeiden Sie es, Protokolle mit persönlich identifizierbaren Informationen (PII) zu speichern.
- Kunden können sich darauf verlassen, dass keine PII-Daten gespeichert werden. Wenn die verwendeten Services Serverless sind, verbleiben keine Daten oder Protokolle mit personenbezogenen Daten.

Serverless-Onboarding

Dieser Abschnitt konzentriert sich auf den Anwendungsfall Kunden-Onboarding. Er dient als Beispiel dafür, wie Serverless-Muster wiederverwendet werden können, um eine wichtige Kundenreise zu modernisieren.

Eine Onboarding-Lösung

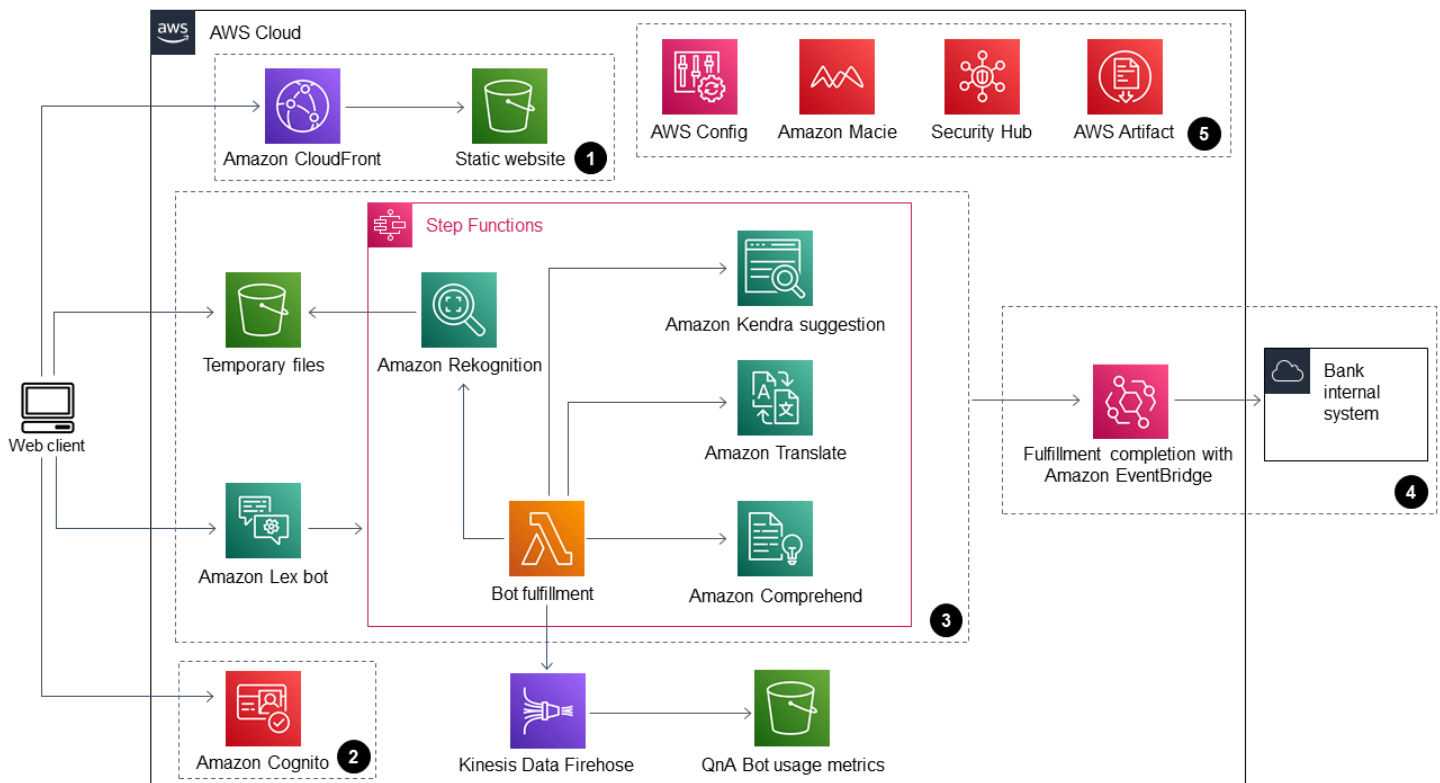
Eine Onboarding-Lösung wird normalerweise nicht isoliert angeboten, sondern ist Teil einer größeren Landschaft. Zu den für die Integration erforderlichen Komponenten und Services gehören:

1. Lead-Generierung (CRM-Systeme)
2. Sorgfaltspflicht (AML, Risiko und Compliance)
3. Zentrale Kundendatendatei (Kernbankensysteme)
4. Verwaltung digitaler Signaturen (mit einem Drittanbieter-Tool wie DocuSign)
5. Biometrische Überprüfung
6. Lebenszyklus des digitalen Vertragsmanagements
7. Automatisierung von Prozessen und Betriebsmodellen

Hinweis

Die Integration dieser Komponenten in externe Anwendungen würde den Rahmen dieser Strategie sprengen.

Das folgende Diagramm zeigt eine serverlose Architektur für die Interaktion mit Kunden über Chatbots in der AWS Cloud:



i Hinweis

Die Architektur basiert auf der QnA Bot AWS on-Lösung und den Updates für Amazon Rekognition. Weitere Informationen finden Sie unter [QnA Bot on AWS](#) in der AWS Solutions Library und [Amazon Rekognition kündigt Aktualisierungen seiner Funktionen zur Gesichtserkennung, -analyse und -erkennung im AWS Machine Learning Learning-Blog](#) an.

Das Diagramm zeigt den folgenden Workflow:

1. Kunden greifen auf die Frontend-Komponenten zu, um mit dem Bot zu interagieren. In diesem Fall kann die Frontend-Bibliothek auf verschiedene Weise in bestehende Komponenten aufgenommen werden. Sie können diese Komponenten beispielsweise in die Unternehmenswebsite integrieren oder sie mit einer wichtigen Chat-Anwendung verknüpfen. Diese Komponenten werden über Static Asset Management mithilfe von Amazon Simple Storage Service (Amazon S3) und Amazon bereitgestellt und bereitgestellt CloudFront. JavaScript

2. Die Front-End-Komponenten betten Verbindungen zu den Back-End-Komponenten ein, um die Anmeldeinformationen durch Amazon Cognito zu validieren. Nach der Autorisierung kann der Kundenservice mit dem Service der Onboarding-Lösung kommunizieren.
3. Kunden interagieren mit dem Service, indem sie einen Amazon-Lex-Bot verwenden. Ein vordefiniertes Onboarding-Szenario wird ausgeführt AWS Step Functions , indem die zum Abschluss des Vorgangs erforderlichen Dienste aufgerufen werden. Sie können dieses Szenario an die Bedürfnisse des Bankensystems anpassen (z. B. um die Anforderungen an die Fotografie, die Übersetzung in mehrere Sprachen und die Verarbeitung natürlicher Sprache entsprechend den Kundenwünschen zu erfüllen). Sie können AWS Lambda Funktionen verwenden, um die Aktionen des Amazon Lex Lex-Bot mit dem Kunden auszuführen und je nach Onboarding-Phase den Service anrufen.
4. Die Ausgabe von Step Functions wird stapelweise über Amazon an das bankinterne System gesendet EventBridge, das Ihre bevorzugte Methode verwendet, um eine Verbindung zum bankinternen System herzustellen. Sie können diese Kommunikation entweder per Peering mit einem anderen AWS Konto oder per Netzwerk-Peering über ein virtuelles privates Netzwerk (VPN) mit dem Bankensystem abwickeln.
5. Die gesamte Architektur ist auf Sicherheit und Compliance ausgelegt und verwendet AWS Config Amazon Macie AWS Artifact, und AWS Security Hub CSPM.

Überlegungen zu Sicherheit und Compliance

Die Aufrechterhaltung der Sicherheit und der Umgang mit vertraulichen Informationen stehen im Mittelpunkt des Serverless-Onboarding-Ansatzes. Das Serverless-Onboarding ist so konzipiert, dass es zustandslos ist und keine personenbezogenen Daten oder kritische Geschäftsdaten speichert. Um kontinuierliche Sicherheit und Compliance zu gewährleisten, müssen Sie die folgenden Services einrichten und korrekt konfigurieren:

- AWS AppConfig gewährleistet die Integrität und Vertraulichkeit der Dienste durch Regeln, die auf die Einhaltung von Vorschriften zugeschnitten sind. Durch die vorhandenen Kontrollen wird die allgemeine Einhaltung der Vorschriften überprüft und Abweichungen bei der Konfiguration verhindert.
- Macie erkennt und markiert alle personenbezogenen Daten während des gesamten Prozesses.
- Security Hub CSPM stellt sicher, dass alle Dienste innerhalb des Sicherheitsbereichs definiert und verwendet werden.
- AWS Artifact liefert Prüfungsnachweise für die Konformität der Dienste. AWS

Transaktionen und unbestreitbare Beweise können gespeichert und verschlüsselt werden, indem vom Kunden verwaltete Schlüssel oder ein spezielles Hardware-Sicherheitsmodul (HSM) verwendet werden, das für Prüfzwecke versiegelt ist. Mit Amazon Glacier können Sie Daten auch kostengünstig versiegeln und gleichzeitig Integrität und Sicherheit gewährleisten.

 Note

Amazon Glacier (ursprünglicher eigenständiger, vault-basierter Service) akzeptiert ab dem 15. Dezember 2025 keine Neukunden mehr, ohne dass dies Auswirkungen auf Bestandskunden hat.

Amazon Glacier ist ein eigenständiger Service mit eigenen APIs, der Daten in Tresoren speichert und sich von den Speicherklassen Amazon S3 und Amazon S3 Glacier unterscheidet. Ihre vorhandenen Daten bleiben in Amazon Glacier auf unbestimmte Zeit sicher und zugänglich. Es ist keine Migration erforderlich. Für kostengünstige, langfristige Archivierungsspeicherung AWS empfiehlt sich die [Amazon S3 Glacier-Speicherklassen](#), die mit S3-Bucket-basierten APIs, voller AWS-Region Verfügbarkeit, niedrigeren Kosten und Integration ein hervorragendes Kundenerlebnis bieten. AWS-Service Wenn Sie erweiterte Funktionen wünschen, sollten Sie eine Migration zu Amazon S3 Glacier-Speicherklassen in Betracht ziehen, indem Sie unseren [AWS Lösungsleitfaden für die Übertragung von Daten aus Amazon Glacier-Tresoren in Amazon S3 Glacier-Speicherklassen](#) verwenden.

Nur das Betriebsteam sollte Zugriff auf die Umgebung haben. Alle Entwicklungsaktivitäten sollten durch automatische kontinuierliche Bereitstellung optimiert werden, um jeglichen menschlichen Zugriff auf die Produktionsumgebung zu verhindern. Zu Prüfungszwecken sollte eine zusätzliche Rolle für den Zugriff auf Artefakte und Compliance-Berichte auf der Plattform bereitgestellt werden.

AWS kann Ihnen dabei helfen, sicherzustellen, dass Sie die gesetzlichen Vorschriften und Compliance-Standards einhalten. Weitere Informationen finden Sie in der Dokumentation im FINMA ISAE 3000 Type 2-Bericht. AWS Sie können relevante Bankinformationen auch direkt unter FINMA-Rundschreiben AWS Artifact, FINMA ISAE 3000 Type 2 2008/21, FINMA-Rundschreiben und Global Financial Services Regulatory 2018/03 Principles herunterladen.

Häufig gestellte Fragen

Wie kann ich sicher sein, dass AWS Dienste keine personenbezogenen Daten speichern?

Sie können AWS Config es verwenden, um die Konformität der Architekturkomponenten in Kombination mit Macie zu überprüfen, um alle entdeckten personenbezogenen Daten zu erkennen und zu korrigieren.

Ist die Architektur DSGVO-konform?

Ja, gemäß Kapitel 2 der DSGVO, [Artikel 5](#), ist die Architektur so konzipiert, dass keine Daten, die sich auf den Nutzer beziehen, langfristig gespeichert werden, sondern nur personenbezogene Daten verarbeitet werden. Dies wird durch kontinuierliche Compliance-Mechanismen gewährleistet. Darüber hinaus sorgt Macie für die Kennzeichnung und Klassifizierung aller personenbezogenen Daten, die die Einhaltung der DSGVO gefährden könnten.

Wie kann ich eine angemessene Datenvertraulichkeit sicherstellen?

Die Vertraulichkeit wird durch kontinuierliche Compliance- und Sicherheitsmuster unter Verwendung von Security Hub CSPM AWS Config, und Macie gewährleistet. Verstöße gegen die Vertraulichkeit werden sofort erkannt, behoben und eskaliert. Wir empfehlen außerdem, dass Sie in der Bereitstellungsphase Integritätsschutz hinzufügen. Integritätsschutz stellt sicher, dass keine kritischen Änderungen, die die Vertraulichkeit gefährden könnten, in die Architektur übertragen werden.

Kann ich eine AWS-Lösung zur Modernisierung des Bankwesens in jedes bestehende Bankensystem integrieren?

Die Lösung ist so konzipiert, dass sie anpassungsfähig ist und sich in jedes bestehende Bankensystem integrieren lässt, das Standard-API-Aufrufe akzeptiert.

Kann ich den Onboarding-Dialog anpassen?

Ja, Sie können den Chatbot-Dialog an Ihren Anwendungsfall und die gewünschte Dialogsequenz anpassen. Weitere Informationen finden Sie unter [QnA Bot on AWS in der Solutions Library](#). AWS

Nächste Schritte

Neben dem Kunden-Onboarding gibt es noch andere CLM-Anwendungsfälle, und diese Anwendungsfälle können mit integrierten Diensten modernisiert werden. AWS Cloud In den folgenden Szenarien werden einige potenzielle Anwendungsfälle für die Modernisierung untersucht:

1. Integrieren Sie Produktempfehlungen in Produktgestaltung und -service, indem Sie [Amazon Personalize](#) oder andere maßgeschneiderte Empfehlungen verwenden. FS-Produkte unterscheiden sich zwar von Einzelhandelsprodukten, es wird jedoch laut Prognosen bis 2025 immer noch ein hoher Grad an Personalisierung prognostiziert laut [Branchenführer prognostizieren massive Veränderungen im Bankwesen bis 2025](#) von The Financial Brand. Kunden sind möglicherweise bereit, für hochgradig personalisierte und kontextbezogene Services mehr zu zahlen. Dies kann nur mit intelligenteren Lösungen umgesetzt werden, die auf Machine Learning basieren.
2. Sie können [Amazon Fraud Detector](#) verwenden, ein auf Machine Learning basierender Online-Betrugsdetektor zur Kontoüberwachung. Sie können auch andere integrierte Algorithmen anpassen, um standardisierte Kontoüberwachungsservices bereitzustellen (z. B. mithilfe von Anomalien-Erkennung).

Note

Amazon Fraud Detector ist seit dem 7. November 2025 nicht mehr für Neukunden geöffnet. Funktionen, die Amazon Fraud Detector ähneln, finden Sie SageMaker unter Amazon AutoGluon, und AWS WAF. Weitere Informationen finden Sie unter [Änderung der Verfügbarkeit von Amazon Fraud Detector](#).

3. Sie können intelligente Assistenten einsetzen, die mithilfe von Amazon Lex und Chatbots, die auf den neuesten Modellen natürlicher Sprache basieren, direkt mit Kunden in Kontakt treten.

Kreativen Lösungen sind keine Grenzen gesetzt, aber Sie müssen solche Lösungen in großem Umfang und Geschwindigkeit integrieren und bereitstellen.

Ressourcen

- [Was Embedded-Finance und banking-as-a-service Trends für Finanzdienstleistungen \(McKinsey und Unternehmen\) bedeuten](#)
- [Digitales Onboarding im Finanzwesen: ein neuartiges Modell und damit verbundene Cybersicherheitsrisiken](#) (Open Research Europe)
- [Branchenführer prognostizieren massive Veränderungen im Bankwesen bis 2025](#) (The Financial Brand)
- [AWS Benutzerleitfaden zu den Vorschriften und Richtlinien für Finanzdienstleistungen in der Schweiz und Veröffentlichungen der FINMA-Arbeitsmappen](#) (AWS Security Blog)
- [FSI Services im Rampenlicht: Mit dabei AWS Lambda](#)(Blogbeitrag)AWS
- [Amazon Rekognition kündigt Updates seiner Funktionen zur Gesichtserkennung, -analyse und -erkennung](#) an (AWS Machine Learning Blog)
- [QnA Bot aktiviert AWS](#)(Lösungsbibliothek)AWS

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen [RSS-Feed](#) abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	8. Juni 2022

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.