



Strategi modernisasi perbankan untuk manajemen siklus hidup klien di Cloud
AWS

AWS Panduan Preskriptif



AWS Panduan Preskriptif: Strategi modernisasi perbankan untuk manajemen siklus hidup klien di Cloud AWS

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

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Pengantar	1
Tantangan modernisasi	2
Mengubah harapan dan neobank	2
Masalah bisnis	2
Manajemen siklus hidup klien	3
Orientasi klien	4
Perjalanan orientasi	5
Orientasi tanpa server	6
Solusi orientasi	6
Keamanan dan kepatuhan	8
Pertanyaan yang Sering Diajukan	10
Bagaimana saya bisa yakin bahwa AWS layanan tidak akan menyimpan data pribadi apa pun?	10
Apakah arsitekturnya sesuai dengan GDPR?	10
Bagaimana saya bisa memastikan kerahasiaan data yang tepat?	10
Dapatkah saya mengintegrasikan solusi modernisasi perbankan AWS dengan sistem perbankan lama apa pun?	10
Bisakah saya menyesuaikan dialog orientasi?	10
Langkah selanjutnya	11
Sumber Daya	12
Riwayat dokumen	13
.....	xiv

Strategi modernisasi perbankan untuk manajemen siklus hidup klien di Cloud AWS

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

Juni 2022 ([riwayat dokumen](#))

Industri jasa keuangan (FS) menghadapi gangguan besar. Semakin banyak pelanggan mengharapkan dan bahkan lebih memilih layanan perbankan swalayan digital sepenuhnya yang diberikan oleh perusahaan teknologi keuangan (fintech) dan neobank (yaitu, bank khusus digital tanpa cabang fisik) sebagai bagian dari proses orientasi pelanggan ritel. Lembaga keuangan tradisional tidak dapat mengimbangi fintech dan neobank. Ini karena proses perbankan di sebagian besar lembaga keuangan tradisional masih manual atau semi-otomatis.

Tidak ada kerangka kerja standar yang digunakan untuk menerapkan proses perbankan tradisional, meskipun proses ini umum untuk semua lembaga keuangan. Kurangnya kerangka standar seperti itu menghambat inovasi. Misalnya, lembaga keuangan tradisional tidak dalam posisi untuk memanfaatkan salah satu tren terbaru dalam perbankan: keuangan tertanam. Artinya, kemampuan nonbank untuk menawarkan layanan seperti bank. Untuk informasi selengkapnya, lihat [Apa arti keuangan dan banking-as-a-service tren yang disematkan untuk layanan keuangan](#) dari McKinsey & Perusahaan. Agar lembaga keuangan tradisional dapat memanfaatkan keuangan tertanam, mereka harus secara mulus mengekspos kemampuan bisnis mereka ke bisnis lain.

Strategi ini mendefinisikan pendekatan modernisasi untuk menerapkan proses perbankan standar yang terukur dan aman dengan menggunakan arsitektur tanpa server berorientasi API yang dibangun di atas layanan Cloud. AWS Untuk menggambarkan tantangan dan peluang pendekatan ini, strategi ini berfokus pada studi kasus manajemen siklus hidup klien (CLM). Audiens yang dituju untuk strategi ini meliputi CEOs CFOs CIOs,,, dan manajer senior di perbankan ritel dan industri manajemen kekayaan.

Tantangan modernisasi perbankan

Mengubah harapan pelanggan dan munculnya neobank

Industri FS menghadapi perubahan besar. Pelanggan tidak hanya mengharapkan perjalanan digital sepenuhnya, tetapi juga pengalaman yang dipersonalisasi. Untuk memenuhi harapan pelanggan ini dan bersaing dengan neobank, lembaga keuangan tradisional harus menjalani transformasi besar-besaran yang membutuhkan kecepatan, kelincahan, dan inovasi. Transformasi itu akan membutuhkan lembaga keuangan tradisional untuk mengatasi tantangan jangka pendek berikut:

1. Bank tradisional harus mengimbangi neobank, yang sifatnya lebih gesit berkat kurangnya hutang teknis dan proses.
2. Lembaga keuangan tradisional harus mengembangkan dan menyediakan layanan perbankan tertanam melalui perbankan sebagai layanan (BaaS).
3. Lembaga keuangan tradisional harus mengembangkan dan memungkinkan pengalaman pelanggan yang dapat disesuaikan dan fleksibel yang mengintegrasikan model pembelajaran mesin dengan cepat dan hemat biaya.

Faktor strategis utama yang perlu dipertimbangkan untuk beberapa tahun ke depan adalah memanfaatkan layanan cloud bawaan dan untuk memungkinkan manfaat waktu-ke-pasar yang dihasilkan dari kolaborasi dengan penyedia layanan dan transformasi tangkas.

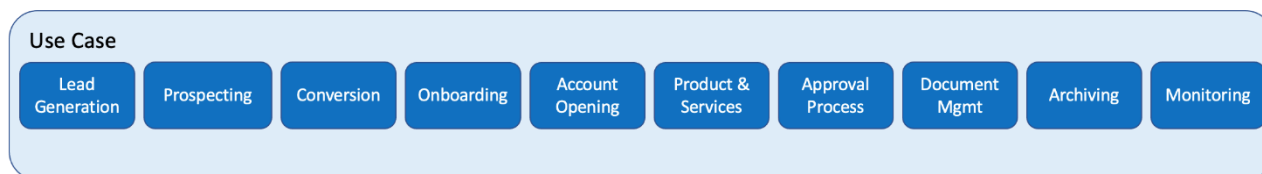
Masalah bisnis

Lembaga keuangan tradisional masih bekerja dengan proses manual atau semi-otomatis. Tidak ada standar industri yang diterapkan untuk proses perbankan reguler, meskipun proses ini umum untuk semua lembaga keuangan di yurisdiksi yang sama. Untuk mengatasi tantangan ini, lembaga keuangan tradisional dapat menerapkan proses standar yang terukur dan aman dengan menggunakan pendekatan tanpa server yang dibangun di atas AWS layanan Cloud. Misalnya, [Amazon Lex](#) dan [Amazon Rekognition](#) menyediakan model pembelajaran mesin terlatih yang dapat Anda integrasikan ke dalam perjalanan pelanggan yang disempurnakan. Sebelumnya, inovasi semacam itu terhambat oleh integrasi yang kompleks dan proses pengembangan yang mahal, tetapi sekarang inovasi ini tersedia langsung untuk aplikasi pelanggan melalui panggilan API.

AWS Layanan cloud tidak hanya memberikan inovasi tambahan dan kecepatan integrasi, tetapi juga memanfaatkan kemampuan keamanan terbaru untuk memastikan kerahasiaan dan privasi data. Kami ingin menyoroti pendekatan modernisasi perbankan untuk lanskap CLM ini. Siklus hidup klien adalah inti dari hubungan klien, itulah sebabnya ia harus segera dimodernisasi dan bahkan didigitalkan. Seperti yang ditunjukkan dalam [Apa arti tren keuangan tertanam dan perbankan sebagai layanan untuk layanan keuangan](#) dari McKinsey & Perusahaan, bank yang ingin menawarkan BaaS harus membuatnya bekerja, dan “Membuatnya bekerja akan membutuhkan teknologi dan kemampuan baru karena BaaS biasanya didistribusikan ke klien melalui API dan membutuhkan risiko yang kuat dan manajemen kepatuhan dari mitra keuangan tertanam.” Bagian orientasi tanpa server dalam strategi ini menjelaskan bagaimana Anda dapat membuat strategi seperti itu bekerja.

Kasus penggunaan manajemen siklus hidup klien

CLM adalah serangkaian proses yang saling bergantung dan wajib yang mendefinisikan interaksi bisnis klien dengan lembaga keuangan atau perusahaan asuransinya. Gambar berikut memberikan gambaran umum tahapan CLM untuk industri perbankan dan asuransi:



Mempertimbangkan bahwa proses ini bervariasi menurut segmen klien. Misalnya, orientasi klien komersial berbeda dari orientasi klien ritel. Prosesnya juga dapat bervariasi dari industri ke industri. Orientasi klien perbankan berbeda dengan orientasi klien asuransi. Strategi ini berfokus pada pengalaman klien ritel perbankan.

Dalam diagram di atas, setiap kotak (Prospecting, misalnya) mewakili kandidat untuk modernisasi. Anda dapat menggunakan diagram seperti ini untuk memecah kasus penggunaan menjadi kasus penggunaan independen yang terpisah. Misalnya, kasus penggunaan Prospecting dapat dipecah menjadi kasus penggunaan konstituen. Kemudian, Anda dapat memetakan setiap kasus penggunaan independen ke kemampuan yang ada, baik dari penyedia layanan cloud atau penyedia BaaS. Latihan pemetaan ini dapat mengungkapkan bahwa pengarsipan dokumen untuk perbankan, misalnya, bisa menjadi layanan dengan sendirinya yang disediakan oleh pihak eksternal. Memecah kasus penggunaan manajemen siklus hidup klien menjadi kasus penggunaan terpisah dan independen memungkinkan Anda merancang dan mengembangkan layanan terfokus.

Strategi ini berfokus pada contoh kasus penggunaan pembukaan rekening bank baru. Bagi pelanggan, ini sering kali merupakan proses yang panjang, sangat manual, dan rawan kesalahan, yang mengakibatkan frustrasi dan ketidakpuasan. Saat ini sebagian besar orientasi masih terjadi secara manual melalui panggilan telepon atau titik sentuh fisik. Namun, penelitian menunjukkan bahwa pelanggan lebih menyukai pengalaman digital. Menurut [Digital onboarding in finance: model baru dan risiko keamanan siber terkait](#) dari Open Research Europe, 70 persen pelanggan lebih suka mengontrak produk secara digital.

Peluang orientasi klien

Di era pasca-krisis COVID, perbankan dan pelanggan FS harus menghadapi proses yang rumit dan kompleks. Bahkan, beberapa pelanggan saat ini dapat menyelesaikan seluruh proses pembukaan rekening giro dari perangkat seluler. Mayoritas nasabah harus mengikuti proses orientasi manual untuk membuka rekening bank yang mirip dengan yang berikut ini:

1. Pelanggan, atau pengguna akhir, harus menyerahkan bukti identitas, ID resmi, dan berbagai titik data lainnya. Dalam banyak kasus, titik data ini mencakup dokumentasi untuk alamat fisik, bukti pekerjaan, dan banyak lagi. Seringkali, pelanggan harus mengunjungi kantor cabang untuk memberikan informasi ini, atau mengirimkannya ke bank melalui surat standar.
2. Sebelum pelanggan bahkan dapat menggunakan rekening perbankan mereka, mereka akan menerima beberapa dokumen paper. Kemudian, pelanggan harus menandatangani dan mengembalikan dokumen ke bank (yaitu, kontrak tunggal untuk setiap produk perbankan, seperti akun pribadi, rekening bersama, akun perdagangan, e-banking, kartu kredit, atau kode keamanan).
3. Bank mendigitalkan semua dokumen yang ditandatangani dan menautkannya ke akun “sedang dalam proses” untuk membuat akun beroperasi.
4. Bergantung pada segmen klien atau penilaian risiko pemohon, bank harus secara teratur mengulangi proses ini sebagian atau seluruhnya.
5. Jika alamat pelanggan, status sipil, atau data lain yang dianggap sebagai “perubahan keadaan” diperbarui, proses dimulai lagi.

Penyelesaian proses ini dapat memakan waktu hingga beberapa hari atau bahkan berminggu-minggu, dan seringkali memerlukan intervensi dari dan persetujuan oleh beberapa karyawan bank dari berbagai departemen.

Perjalanan pelanggan orientasi

Perjalanan pelanggan yang dimodernisasi untuk membuka akun harus mencakup fitur dan kemampuan berikut:

- Pelanggan dapat mengakses layanan orientasi melalui situs web internet, asisten virtual, atau call center. Asisten virtual dapat berupa chatbot berorientasi teks atau berorientasi ucapan, yang dapat diintegrasikan ke dalam halaman web atau ke dalam aplikasi perpesanan seperti Messenger atau Telegram.
- Asisten virtual dapat berinteraksi dengan pelanggan dengan menggunakan maksud yang telah ditentukan untuk memahami kebutuhan dan latar belakang pelanggan. Misalnya, asisten virtual dapat meminta klien untuk berbagi minat mereka, berbagi detail pribadi untuk membuka akun, memindai ID mereka dan mengambil selfie, atau mengonfirmasi bahwa mereka ingin melanjutkan dengan membuka akun.
- Chatbot akan multi-bahasa.
- Pelanggan dapat berinteraksi dengan chatbot menggunakan suara atau teks.
- Setelah Anda mengumpulkan semua informasi yang diperlukan dari pelanggan, maka Anda dapat mengirim informasi ke bank untuk memulai proses pembukaan rekening. Pelanggan akan menerima pemberitahuan email yang mengonfirmasi bahwa proses dimulai.
- Anda dapat menutup dialog setelah akun dibuka.
- Hindari menyimpan informasi pelanggan di cloud. Informasi ini harus bersifat sementara dan hanya ada selama keterlibatan pelanggan. Setelah proses pembukaan akun selesai, Anda harus menghapus data dan, jika mungkin, memberikan beberapa bukti penghapusan. Bahkan jika dialog terputus, Anda harus mengonfirmasi bahwa semua data pribadi dihapus (tidak ada caching).
- Hindari menyimpan log dengan informasi identitas pribadi (PII).
- Pelanggan dapat yakin bahwa tidak ada data PII yang disimpan. Jika layanan yang digunakan tanpa server, maka tidak ada data atau log dengan data pribadi yang tersisa.

Orientasi tanpa server

Bagian ini berfokus pada kasus penggunaan orientasi klien. Ini berfungsi sebagai contoh bagaimana menggunakan kembali pola tanpa server untuk memodernisasi perjalanan pelanggan utama.

Solusi orientasi

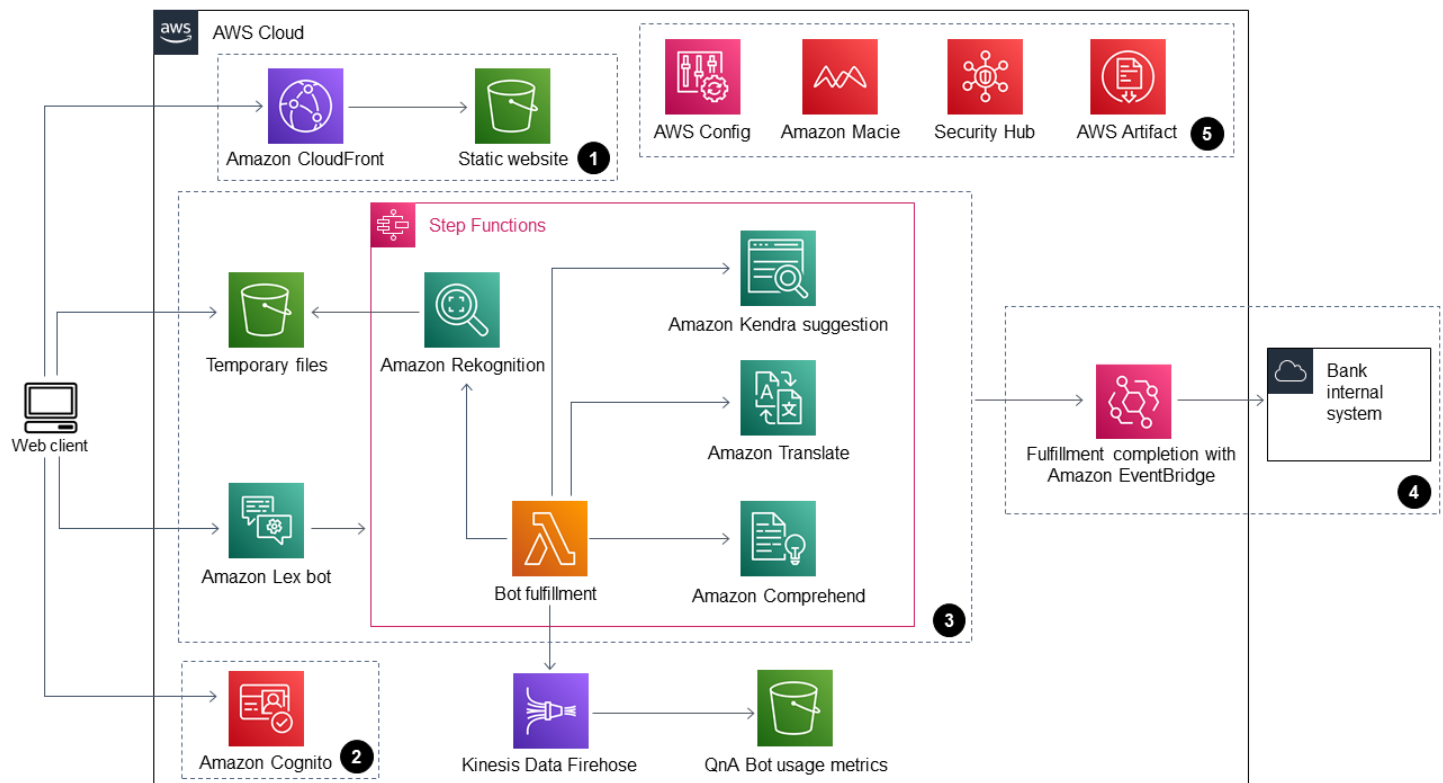
Solusi orientasi biasanya tidak datang secara terpisah, tetapi merupakan bagian dari lanskap yang lebih besar. Komponen dan layanan yang diperlukan untuk integrasi meliputi:

1. Generasi pemimpin (sistem CRM)
2. Uji tuntas (AML, risiko dan kepatuhan)
3. File data klien pusat (sistem perbankan inti)
4. Manajemen tanda tangan digital (menggunakan alat pihak ketiga seperti DocuSign)
5. Verifikasi biometrik
6. Siklus hidup manajemen kontrak digital
7. Otomatisasi model proses dan operasi

Catatan

Integrasi komponen-komponen ini dengan aplikasi eksternal berada di luar cakupan strategi ini.

Diagram berikut menggambarkan arsitektur tanpa server untuk berinteraksi dengan pelanggan melalui chatbots di Cloud: AWS



❗ Catatan

Arsitektur ini didasarkan pada AWS solusi QnA Bot dan pembaruan untuk Amazon Rekognition. Untuk informasi selengkapnya, lihat [QnA Bot AWS di Perpustakaan AWS Solusi](#) dan [Amazon Rekognition mengumumkan pembaruan untuk kemampuan deteksi wajah, analisis, dan pengenalannya](#) di Blog Machine Learning. AWS

Diagram menunjukkan alur kerja berikut:

1. Pelanggan mengakses komponen front-end untuk berinteraksi dengan bot. Dalam hal ini, pustaka front-end dapat dimasukkan dalam aset yang ada dengan berbagai cara. Misalnya, Anda dapat mengintegrasikan komponen ini ke situs web perusahaan atau menautkannya ke aplikasi obrolan utama. Komponen ini dikirimkan JavaScript dan dilayani melalui manajemen aset statis dengan menggunakan Amazon Simple Storage Service (Amazon S3) dan Amazon CloudFront
2. Komponen front-end menyematkan koneksi ke komponen back-end untuk memvalidasi kredensi melalui Amazon Cognito. Setelah diotorisasi, layanan klien dapat berkomunikasi dengan layanan solusi orientasi.

3. Pelanggan berinteraksi dengan layanan dengan menggunakan bot Amazon Lex. Skenario yang telah ditentukan untuk orientasi dijalankan dengan menggunakan AWS Step Functions untuk memanggil layanan yang diperlukan untuk menyelesaikan proses. Anda dapat menyesuaikan skenario ini agar sesuai dengan kebutuhan sistem perbankan (misalnya, untuk memenuhi persyaratan fotografi, terjemahan dalam berbagai bahasa, dan pemrosesan bahasa alami agar sesuai dengan maksud pelanggan). Anda dapat menggunakan AWS Lambda fungsi untuk memenuhi tindakan bot Amazon Lex dengan pelanggan dan layanan panggilan tergantung pada tahap orientasi.
4. Output Step Functions dikirim dalam batch ke sistem internal bank melalui Amazon EventBridge, yang menggunakan metode pilihan Anda untuk terhubung ke Sistem Internal Bank. Anda dapat menangani komunikasi ini baik dengan mengintip ke AWS akun lain atau jaringan mengintip melalui jaringan pribadi virtual (VPN) ke sistem perbankan.
5. Seluruh arsitektur dirancang untuk keamanan dan kepatuhan dengan menggunakan AWS Config, Amazon Macie AWS Artifact, dan. AWS Security Hub CSPM

Pertimbangan keamanan dan kepatuhan

Menjaga keamanan dan menangani informasi sensitif adalah inti dari pendekatan orientasi tanpa server. Orientasi tanpa server dirancang agar tidak memiliki kewarganegaraan dan tidak menyimpan PII atau data bisnis penting apa pun. Untuk memastikan keamanan dan kepatuhan yang berkelanjutan, Anda harus menempatkan layanan berikut dan mengkonfigurasinya dengan benar:

- AWS AppConfig memastikan integritas dan kerahasiaan layanan melalui aturan yang disesuaikan untuk kepatuhan. Kontrol yang ada akan memvalidasi kepatuhan secara keseluruhan dan mencegah penyimpangan dalam konfigurasi.
- Macie mendeteksi dan menandai PII apa pun selama proses berlangsung.
- Security Hub CSPM memastikan bahwa semua layanan didefinisikan dan digunakan dalam lingkup keamanan.
- AWS Artifact memberikan bukti audit untuk kepatuhan AWS layanan.

Bukti transaksi dan non-penolakan dapat disimpan dan dienkripsi dengan menggunakan kunci yang dikelola pelanggan atau modul keamanan perangkat keras khusus (HSM) yang disegel untuk tujuan audit. Anda juga dapat menyegel data dengan biaya rendah sambil memastikan integritas dan keamanan dengan menggunakan Amazon Glacier.

 Note

Amazon Glacier (layanan berbasis brankas mandiri asli) tidak akan lagi menerima pelanggan baru mulai 15 Desember 2025, tanpa berdampak pada pelanggan yang sudah ada.

Amazon Glacier adalah layanan mandiri dengan API sendiri yang menyimpan data di brankas dan berbeda dari Amazon S3 dan kelas penyimpanan Amazon S3 Glacier. Data Anda yang ada akan tetap aman dan dapat diakses di Amazon Glacier tanpa batas waktu. Tidak diperlukan migrasi. Untuk penyimpanan arsip jangka panjang berbiaya rendah, AWS merekomendasikan kelas [penyimpanan Amazon S3 Glacier](#), yang memberikan pengalaman pelanggan yang unggul dengan API berbasis ember S3, ketersediaan penuh, biaya lebih rendah, dan integrasi. Wilayah AWS Layanan AWS Jika Anda ingin meningkatkan kemampuan, pertimbangkan untuk bermigrasi ke kelas penyimpanan Amazon S3 Glacier dengan menggunakan [Panduan Solusi AWS kami untuk mentransfer data dari kubah Amazon Glacier ke kelas penyimpanan Amazon S3 Glacier](#).

Hanya tim operasional yang diizinkan untuk mengakses lingkungan. Setiap kegiatan pengembangan harus disederhanakan melalui pengiriman berkelanjutan otomatis untuk mencegah akses manusia ke lingkungan produksi. Untuk tujuan audit, peran tambahan harus disediakan untuk mengakses artefak dan laporan kepatuhan di platform.

AWS dapat membantu memastikan bahwa Anda memenuhi standar peraturan dan kepatuhan. Untuk informasi lebih lanjut, lihat Laporan FINMA ISAE 3000 Tipe 2 dalam dokumentasi. AWS Anda juga dapat mengunduh artefak perbankan yang relevan langsung dari AWS Artifact, termasuk FINMA Circular, FINMA ISAE 3000 Type 2 2008/21, FINMA Circular 2018/03, dan Global Financial Services Regulatory Principles.

Pertanyaan yang Sering Diajukan

Bagaimana saya bisa yakin bahwa AWS layanan tidak akan menyimpan data pribadi apa pun?

Anda dapat menggunakan AWS Config untuk memeriksa kepatuhan komponen arsitektur yang dikombinasikan dengan Macie untuk mendeteksi dan memulihkan data pribadi apa pun yang ditemukan.

Apakah arsitekturnya sesuai dengan GDPR?

Ya, sesuai GDPR Bab 2, [Pasal 5](#), arsitektur dirancang untuk tidak menyimpan data apa pun yang terkait dengan pengguna dalam jangka panjang tetapi hanya untuk memproses PII. Ini dipastikan melalui mekanisme kepatuhan berkelanjutan. Selain itu, Macie memastikan penandaan dan klasifikasi data PII apa pun yang dapat membahayakan kepatuhan GDPR.

Bagaimana saya bisa memastikan kerahasiaan data yang tepat?

Kerahasiaan dipastikan melalui kepatuhan berkelanjutan dan pola keamanan dengan menggunakan Security Hub CSPM, dan Macie. AWS Config Pelanggaran kerahasiaan segera terdeteksi, diperbaiki, dan ditingkatkan. Kami juga menyarankan Anda menambahkan pagar pembatas pada fase penerapan. Pagar pembatas membantu memastikan bahwa tidak ada perubahan kritis yang dapat membahayakan kerahasiaan didorong ke arsitektur.

Dapatkan saya mengintegrasikan solusi modernisasi perbankan AWS dengan sistem perbankan lama apa pun?

Solusi ini dirancang agar dapat beradaptasi dan dapat diintegrasikan dengan sistem perbankan lama apa pun yang dapat menerima panggilan API standar.

Bisakah saya menyesuaikan dialog orientasi?

Ya, Anda dapat menyesuaikan dialog chatbot agar sesuai dengan kasus penggunaan dan urutan dialog yang ditargetkan. Untuk informasi selengkapnya, lihat [QnA Bot AWS aktif di](#) Perpustakaan AWS Solusi.

Langkah selanjutnya

Ada kasus penggunaan CLM lain di luar orientasi klien, dan kasus penggunaan ini dapat dimodernisasi dengan layanan bawaan. AWS Cloud Skenario berikut mengeksplorasi beberapa kasus penggunaan modernisasi potensial:

1. Integrasikan rekomendasi produk ke dalam produk dan layanan kue dengan menggunakan [Amazon Personalize](#) atau rekomendasi lain yang dibuat khusus. Meskipun produk FS berbeda dari produk ritel, masih ada tingkat personalisasi yang tinggi yang diprediksi pada tahun 2025 menurut [Pemimpin Industri Memprediksi Perubahan Besar dalam Perbankan pada tahun 2025](#) dari The Financial Brand. Pelanggan mungkin bersedia membayar lebih untuk layanan yang sangat personal dan kontekstual. Ini hanya dapat diimplementasikan dengan solusi yang lebih cerdas berdasarkan pembelajaran mesin.
2. Anda dapat menggunakan [Amazon Fraud Detector](#), detektor penipuan online berdasarkan pembelajaran mesin, untuk pemantauan akun. Anda juga dapat menyesuaikan algoritma bawaan lainnya untuk menyediakan layanan pemantauan akun standar (misalnya, dengan menggunakan deteksi anomali).

Note

Amazon Fraud Detector tidak lagi terbuka untuk pelanggan baru per 7 November 2025. Untuk kemampuan yang mirip dengan Amazon Fraud Detector, jelajahi Amazon SageMaker AutoGluon, dan AWS WAF. Untuk informasi selengkapnya, lihat [perubahan ketersediaan Amazon Fraud Detector](#).

3. Anda dapat memiliki asisten cerdas yang terlibat langsung dengan pelanggan dengan menggunakan Amazon Lex dan chatbots berdasarkan model bahasa alami terbaru.

Tidak ada batasan untuk solusi kreatif, tetapi Anda harus mengintegrasikan dan menerapkan solusi tersebut dalam skala dan kecepatan.

Sumber Daya

- [Apa arti keuangan dan banking-as-a-service tren yang disematkan untuk layanan keuangan](#) (McKinsey & Perusahaan)
- [Orientasi digital di bidang keuangan: model baru dan risiko keamanan siber terkait](#) (Open Research Europe)
- [Pemimpin Industri Memprediksi Perubahan Besar dalam Perbankan pada 2025](#) (The Financial Brand)
- [AWS Panduan Pengguna untuk Peraturan dan Pedoman Layanan Keuangan di Swiss dan publikasi buku kerja FINMA \(BlogAWS Keamanan\)](#)
- [Sorotan Layanan FSI: Menampilkan AWS Lambda](#) (AWS posting blog)
- [Amazon Rekognition mengumumkan pembaruan untuk deteksi wajah, analisis, dan kemampuan pengenalannya](#) (Machine AWS Learning Blog)
- [QnA Bot on AWS](#) (Perpustakaan AWS Solusi)

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan masa depan, Anda dapat berlangganan umpan [RSS](#).

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	Juni 8, 2022

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.