Amazon Web Services:
Risiko dan Kepatuhan

Amazon Web Services: Risiko dan Kepatuhan

Daftar Isi

Amazon Web Services: Risiko dan Kepatuhan

Tanggal publikasi: **11 Maret 2021** (*Revisi Dokumen* (halaman 12))

Abstrak

AWS melayani berbagai pelanggan, termasuk yang berada di industri yang diatur. Melalui model tanggung jawab bersama kami, kami memungkinkan pelanggan untuk mengelola risiko secara efektif dan efisien di lingkungan TI, dan memberikan jaminan manajemen risiko yang efektif melalui kepatuhan kami terhadap kerangka kerja, dan program yang telah ditetapkan, diakui secara luas. Makalah ini menguraikan mekanisme yang AWS telah menerapkan untuk mengelola risiko di sisi AWS dari Model Tanggung Jawab Bersama, dan alat yang pelanggan dapat memanfaatkan untuk mendapatkan jaminan bahwa mekanisme ini sedang dilaksanakan secara efektif.

Pendahuluan

AWS dan pelanggannya berbagi kontrol atas lingkungan TI. Oleh karena itu, keamanan adalah tanggung jawab bersama. Ketika datang untuk mengelola keamanan dan kepatuhan dalam AWS Cloud, masing-masing pihak memiliki tanggung jawab yang berbeda. Tanggung jawab pelanggan tergantung pada layanan yang mereka gunakan. Namun, secara umum, pelanggan bertanggung jawab untuk membangun lingkungan TI mereka dengan cara yang sesuai dengan persyaratan keamanan dan kepatuhan khusus mereka.

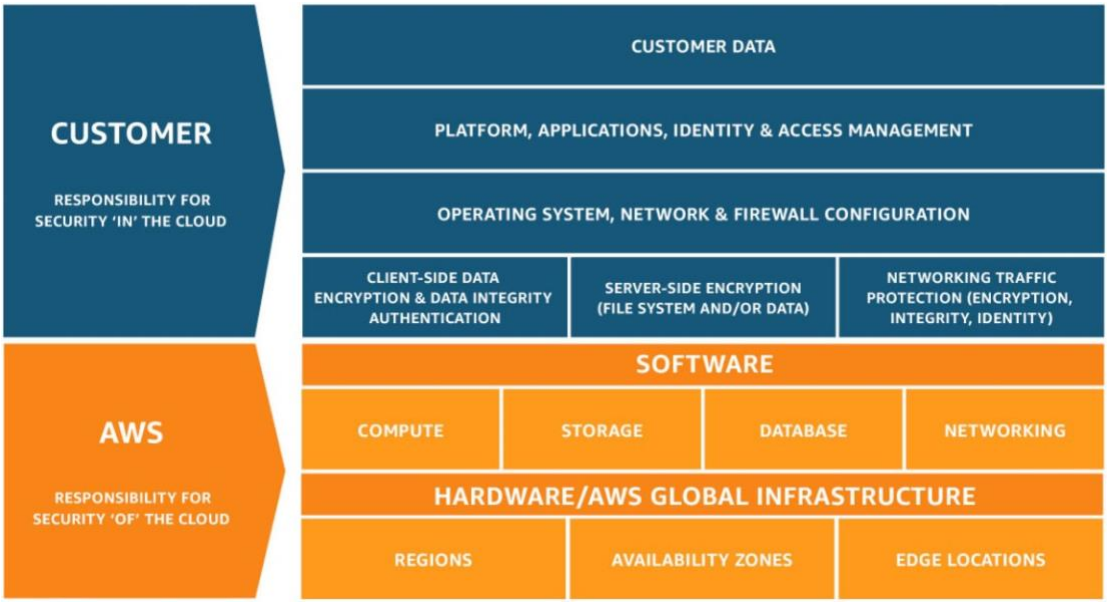
Makalah ini memberikan rincian lebih lanjut tentang tanggung jawab keamanan masing-masing pihak dan cara pelanggan dapat memberikan manfaat dari Program Risiko dan Kepatuhan AWS.

Model tanggung jawab bersama

Keamanan dan kepatuhan adalah tanggung jawab bersama antara AWS dan pelanggan. Tergantung pada layanan yang dikerahkan, model bersama ini dapat membantu meringankan beban operasional pelanggan. Hal ini karena AWS beroperasi, mengelola, dan mengontrol komponen dari sistem operasi host dan lapisan virtualisasi ke keamanan fisik fasilitas di mana layanan beroperasi. Pelanggan memikul tanggung jawab dan pengelolaan sistem operasi tamu (termasuk pembaruan dan *patch* keamanan) dan perangkat lunak aplikasi terkait lainnya, selain konfrontasi kelompok keamanan yang disediakan AWS-wall.

Kami menyarankan agar pelanggan mempertimbangkan dengan seksama layanan yang mereka pilih karena tanggung jawab mereka bervariasi tergantung pada layanan yang digunakan, integrasi layanan tersebut ke lingkungan TI mereka, serta hukum dan peraturan yang berlaku. Adalah mungkin bagi pelanggan untuk meningkatkan keamanan mereka dan/atau memenuhi persyaratan kepatuhan mereka yang lebih ketat dengan memanfaatkan teknologi seperti *firewalls* berbasis *host*, deteksi intrusi berbasis *host* dan pencegahan, enkripsi, dan manajemen kunci.

Sifat tanggung jawab bersama ini juga menyediakan fleksibilitas dan kontrol pelanggan yang memungkinkan pelanggan untuk menerapkan solusi yang memenuhi persyaratan sertifikasi khusus industri.



Model tanggung jawab bersama ini juga meluas ke kontrol TI. Sama seperti tanggung jawab untuk mengoperasikan lingkungan TI dibagi antara AWS dan pelanggannya, manajemen, operasi, dan verifikasi kontrol TI juga merupakan tanggung jawab bersama. AWS dapat membantu pelanggan dengan mengelola kontrol yang terkait dengan infrastruktur fisik dikerahkan di lingkungan AWS. Pelanggan kemudian dapat menggunakan kontrol AWS dan dokumentasi kepatuhan yang tersedia bagi mereka untuk melakukan evaluasi kontrol dan prosedur verifikasi mereka sesuai kebutuhan. Untuk contoh bagaimana tanggung jawab untuk kontrol tertentu dibagi antara AWS dan pelanggan, lihat AWS Bersama Tanggung Jawab Model.

Mengevaluasi dan mengintegrasikan kontrol AWS

AWS menyediakan berbagai informasi tentang lingkungan kontrol TI kepada pelanggan melalui makalah teknis, laporan, sertifikasi, dan pengesahan pihak ketiga lainnya. Dokumentasi ini membantu pelanggan untuk memahami kontrol di tempat, relevan dengan layanan AWS yang mereka gunakan, dan bagaimana kontrol tersebut telah divalidasi. Informasi ini juga membantu pelanggan memperhitungkan dan memvalidasi bahwa kontrol di lingkungan TI yang diperluas beroperasi secara efektif.

Secara tradisional, auditor internal dan/atau eksternal memvalidasi desain dan operasional eectiveness kontrol dengan proses walkthrough dan evaluasi bukti. Jenis pengamatan langsung dan verifikasi, oleh auditor eksternal pelanggan atau pelanggan, umumnya dilakukan untuk memvalidasi kontrol dalam penggunaan lokal tradisional.

Dalam kasus di mana penyedia layanan digunakan (seperti AWS), pelanggan dapat meminta dan mengevaluasi pengesahan pihak ketiga dan sertifikasi. Atestasi dan sertifikasi ini dapat membantu meyakinkan pelanggan tentang desain dan operasi eectiveness kontrol tujuan dan kontrol divalidasi oleh pihak ketiga yang memenuhi syarat, independen. Akibatnya, meskipun beberapa kontrol mungkin dikelola oleh AWS, lingkungan kontrol masih dapat menjadi kerangka kerja terpadu di mana pelanggan dapat memperhitungkan dan memverifikasi bahwa kontrol beroperasi secara eectively dan mempercepat proses peninjauan kepatuhan.

Pengesahan pihak ketiga dan sertifikasi AWS menyediakan pelanggan dengan visibilitas dan validasi independen dari lingkungan kontrol. Pengesahan dan sertifikasi tersebut dapat membantu meringankan pelanggan dari persyaratan untuk melakukan validasi tertentu bekerja sendiri untuk lingkungan TI mereka di AWS Cloud.

Program risiko dan kepatuhan AWS

AWS telah mengintegrasikan program risiko dan kepatuhan di seluruh organisasi. Program ini bertujuan untuk mengelola risiko dalam semua tahapan desain dan penyebaran layanan dan terus meningkatkan dan menilai kembali kegiatan terkait risiko organisasi. Komponen program risiko dan kepatuhan terintegrasi AWS dibahas secara lebih rinci pada bagian berikut.

Manajemen risiko bisnis AWS

AWS memiliki program manajemen risiko bisnis (BRM) yang bermitra dengan unit bisnis AWS untuk memberikan AWS Dewan Direksi dan kepemimpinan senior AWS pandangan holistik risiko utama di seluruh AWS. Program BRM menunjukkan pengawasan risiko independen atas fungsi AWS. Secara khusus, program BRM melakukan hal berikut:

- Melakukan penilaian risiko dan pemantauan risiko dari area fungsional AWS utama
- Identifikasi dan mendorong perbaikan risiko
- Mempertahankan daftar risiko yang diketahui

Untuk mendorong perbaikan risiko, program BRM melaporkan hasil eort-nya, dan meningkat jika diperlukan, kepada direksi dan wakil presiden di seluruh bisnis untuk menginformasikan pengambilan keputusan bisnis.

Manajemen operasional dan bisnis

AWS menggunakan kombinasi pertemuan mingguan, bulanan, dan triwulanan dan laporan untuk, antara lain, memastikan komunikasi risiko di semua komponen dari proses manajemen risiko. Selain itu, AWS mengimplementasikan proses eskalasi untuk memberikan visibilitas manajemen menjadi risiko prioritas tinggi di seluruh organisasi. Usaha-usaha ini, diambil bersama-sama, membantu memastikan bahwa risiko dikelola secara konsisten dengan kompleksitas model bisnis AWS.

Selain itu, melalui struktur tanggung jawab berjenjang, wakil presiden (pemilik bisnis) bertanggung jawab atas pengawasan bisnis mereka. Untuk tujuan ini, AWS melakukan pertemuan mingguan untuk meninjau metrik operasional dan mengidentifikasi tren dan risiko utama sebelum mereka mempengaruhi bisnis.

Kepemimpinan eksekutif dan senior memainkan peran penting dalam membangun nada AWS dan nilai-nilai inti. Setiap karyawan diberikan Kode Etik Bisnis dan Etika perusahaan, dan karyawan menyelesaikan pelatihan berkala. Audit kepatuhan dilakukan sehingga karyawan memahami dan mengikuti kebijakan yang ditetapkan.

Struktur organisasi AWS menyediakan kerangka kerja untuk perencanaan, melaksanakan, dan mengendalikan operasi bisnis. Struktur organisasi meliputi peran dan tanggung jawab untuk menyediakan stang yang memadai, eciency operasi, dan pemisahan tugas. Manajemen juga telah menetapkan jalur pelaporan yang tepat untuk personil kunci. Proses verifikasi perekrutan perusahaan meliputi validasi pendidikan, pekerjaan sebelumnya, dan, dalam beberapa kasus, pemeriksaan latar belakang sebagaimana diizinkan oleh hukum dan peraturan bagi karyawan sepadan dengan posisi karyawan dan tingkat akses ke fasilitas AWS. Perusahaan mengikuti proses on-boarding terstruktur untuk membiasakan karyawan baru dengan alat Amazon, proses, sistem, kebijakan, dan prosedur.

Lingkungan kontrol dan otomatisasi

AWS mengimplementasikan kontrol keamanan sebagai elemen dasar untuk mengelola risiko di seluruh organisasi. Lingkungan kontrol AWS terdiri dari standar, proses, dan struktur yang menyediakan dasar untuk menerapkan satu set minimum persyaratan keamanan di AWS.

Sementara proses dan standar termasuk sebagai bagian dari lingkungan kontrol AWS berdiri sendiri, AWS juga memanfaatkan aspek lingkungan kontrol keseluruhan Amazon. Alat leverage meliputi:

- Alat yang digunakan di semua bisnis Amazon, seperti alat yang mengelola pemisahan tugas
- Beberapa fungsi bisnis di Amazon-wide, seperti hukum, sumber daya manusia, dan finansial

Dalam kasus di mana AWS memanfaatkan lingkungan kontrol keseluruhan Amazon, standar dan proses yang mengatur mekanisme ini disesuaikan secara khusus untuk bisnis AWS. Ini berarti bahwa harapan untuk penggunaan dan aplikasi mereka dalam lingkungan kontrol AWS mungkin berbeda dari harapan untuk penggunaan dan aplikasi mereka dalam lingkungan Amazon secara keseluruhan. Lingkungan kontrol AWS akhirnya bertindak sebagai dasar untuk pengiriman aman penawaran layanan AWS.

Otomatisasi kontrol adalah cara bagi AWS untuk mengurangi intervensi manusia dalam proses berulang tertentu yang terdiri dari lingkungan kontrol AWS. Ini adalah kunci untuk eective implementasi kontrol keamanan informasi dan manajemen terkait risiko. Otomatisasi kontrol berusaha untuk secara proaktif meminimalkan inkonsistensi potensial dalam pelaksanaan proses yang mungkin timbul karena sifat melanda manusia yang melakukan proses berulang. Melalui otomatisasi kontrol, penyimpangan proses potensial dieliminasi. Hal ini memberikan peningkatan tingkat jaminan bahwa kontrol akan diterapkan seperti yang dirancang.

Tim teknik di AWS di seluruh fungsi keamanan bertanggung jawab untuk rekayasa lingkungan kontrol AWS untuk mendukung peningkatan tingkat otomatisasi kontrol sedapat mungkin. Contoh kontrol otomatis di AWS meliputi:

- **Tata Kelola dan Pengawasan:** Versioning dan persetujuan kebijakan
- **Manajemen Personil:** Pengiriman pelatihan otomatis, penghentian karyawan yang cepat
- **Manajemen Pengembangan dan Konfigurasi:** Jaringan penyebaran kode, pemindaian kode, pencadangan kode, pengujian penyebaran terpadu
- **Manajemen Identitas dan Akses:** Pemisahan tugas secara otomatis, ulasan akses, manajemen izin
- **Pemantauan dan Logging:** Pengumpulan log otomatis dan korelasi, mengkhawatirkan
- **Keamanan Fisik:** Proses otomatis yang terkait dengan pusat data AWS, termasuk manajemen perangkat keras, pelatihan keamanan pusat data, akses yang mengkhawatirkan, dan manajemen akses fisik
- **Pemindaian dan Manajemen Patch:** Pemindaian kerentanan otomatis, manajemen *patch*, dan penyebaran

Mengontrol penilaian dan pemantauan berkelanjutan

AWS mengimplementasikan berbagai kegiatan sebelum dan sesudah penyebaran layanan untuk lebih mengurangi risiko dalam lingkungan AWS. Kegiatan ini mengintegrasikan persyaratan keamanan dan kepatuhan selama desain dan pengembangan setiap layanan AWS dan kemudian memvalidasi bahwa layanan beroperasi dengan aman setelah mereka dipindahkan ke produksi (diluncurkan).

Kegiatan manajemen risiko dan kepatuhan mencakup dua kegiatan pra-peluncuran dan dua kegiatan pasca peluncuran. Kegiatan pra-peluncuran adalah:

- AWS Application Security review manajemen risiko untuk memvalidasi bahwa risiko keamanan telah diidentifikasi dan dikurangi
- Peninjauan kesiapan arsitektur untuk membantu pelanggan memastikan keselarasan dengan rezim kepatuhan

Pada saat penyebaran, layanan akan melalui penilaian yang ketat terhadap persyaratan keamanan rinci untuk memenuhi standar AWS yang tinggi untuk keamanan. Kegiatan pasca-peluncuran adalah:

- AWS Aplikasi Keamanan yang sedang berlangsung review untuk membantu memastikan postur keamanan layanan dipertahankan
- Pemindaian manajemen kerentanan yang sedang berlangsung

Penilaian kontrol dan pemantauan berkelanjutan ini memungkinkan pelanggan yang diatur kemampuan untuk secara meyakinkan membangun solusi yang sesuai pada layanan AWS. Untuk daftar layanan dalam lingkup untuk berbagai program kepatuhan melihat Layanan AWS di halaman web Cakupan .

Sertifikasi AWS, program, laporan, dan pengesahan pihak ketiga

AWS secara teratur menjalani audit pengesahan pihak ketiga independen untuk memberikan jaminan bahwa kegiatan pengendalian beroperasi sebagaimana dimaksud. Lebih spesifik lagi, AWS diaudit terhadap berbagai kerangka keamanan global dan regional yang bergantung pada wilayah dan industri. AWS berpartisipasi dalam lebih dari 50 program audit yang berbeda.

Hasil audit ini didokumentasikan oleh badan penilaian dan dibuat tersedia untuk semua pelanggan AWS melalui AWS Artifact. AWS Artifact adalah portal tanpa biaya swalayan untuk akses on-demand untuk laporan kepatuhan AWS. Ketika laporan baru dirilis, mereka dibuat tersedia di AWS Artifact, memungkinkan pelanggan untuk terus memantau keamanan dan kepatuhan AWS dengan akses langsung ke laporan baru.

Tergantung pada persyaratan peraturan atau kontrak lokal negara atau industri, AWS juga dapat menjalani audit langsung dengan pelanggan atau auditor pemerintah. Audit ini memberikan pengawasan tambahan terhadap lingkungan kontrol AWS untuk memastikan bahwa pelanggan memiliki alat untuk membantu diri mereka beroperasi secara percaya, patuh, dan dengan cara berbasis risiko menggunakan layanan AWS.

Untuk informasi lebih rinci tentang program sertifikasi AWS, laporan, dan pengesahan pihak ketiga, kunjungi halaman web AWS Compliance Program . Anda juga dapat mengunjungi Layanan AWS di halaman web Cakupan untuk informasi layanan-spesifikasi.

Aliansi Keamanan Cloud

AWS berpartisipasi dalam Penilaian Self-Assessment Cloud Security Alliance (CSA) sukarela, Trust & Assurance Registry (STAR) untuk mendokumentasikan kepatuhannya dengan praktik terbaik yang diterbitkan CSA-diterbitkan. CSA adalah “organisasi terkemuka di dunia yang didedikasikan untuk membatalkan dan meningkatkan kesadaran akan praktik terbaik untuk membantu memastikan lingkungan komputasi awan yang aman”. CSA Consensus Assessments Initiative Questionnaire (CAIQ) menyediakan serangkaian pertanyaan yang diantisipasi oleh CSA kepada pelanggan cloud dan/atau auditor awan akan meminta penyedia awan. Ini menyediakan serangkaian pertanyaan keamanan, kontrol, dan proses, yang kemudian dapat digunakan untuk berbagai eorts, termasuk pilihan penyedia awan dan evaluasi keamanan.

Ada dua sumber daya yang tersedia untuk pelanggan yang mendokumentasikan keselarasan AWS ke CSA CAIQ. Yang pertama adalah CSA CAIQ Whitepaper, dan yang kedua adalah pemetaan kontrol yang lebih rinci ke kontrol SOC-2 kami yang tersedia untuk melalui AWS Artifact. Untuk informasi lebih lanjut tentang partisipasi AWS dalam CSA CAIQ, lihat situs AWS CSA.

Tata kelola kepatuhan cloud pelanggan

Pelanggan AWS bertanggung jawab untuk menjaga tata kelola yang memadai atas seluruh lingkungan kontrol TI mereka, terlepas dari bagaimana atau di mana TI dikerahkan. Praktik terkemuka meliputi:

- Memahami tujuan dan persyaratan kepatuhan yang diperlukan (dari sumber yang relevan)
- Membangun lingkungan kontrol yang memenuhi tujuan dan persyaratan
- Memahami validasi yang diperlukan berdasarkan toleransi risiko organisasi
- Memverifikasi efektivitas operasi lingkungan kontrol mereka

Penyebaran di AWS Cloud memberikan perusahaan pilihan yang berbeda untuk menerapkan berbagai jenis kontrol dan berbagai metode verifikasi.

Kepatuhan dan tata kelola pelanggan yang kuat dapat mencakup pendekatan dasar berikut:

1. Meninjau AWS Bersama Tanggung Jawab Model, Dokumentasi AWS Keamanan,laporankepatuhan AWS, dan informasi lain yang tersedia dari AWS, bersama-sama dengan pelanggan lainnya- dokumentasi spesifik. Cobalah untuk memahami sebanyak mungkin seluruh lingkungan TI, dan kemudian mendokumentasikan semua persyaratan kepatuhan ke dalam kerangka kontrol komputasi awan yang komprehensif.
2. Merancang dan menerapkan tujuan kontrol untuk memenuhi persyaratan kepatuhan perusahaan seperti yang diletakkan di AWS Bersama Tanggung Jawab Model.
3. Mengidentifikasi dan mendokumentasikan kontrol yang dimiliki oleh pihak luar.
4. Memverifikasi bahwa semua tujuan kontrol terpenuhi dan semua kontrol kunci dirancang dan beroperasi secara efektif.

Mendekati tata kelola kepatuhan dengan cara ini akan membantu pelanggan mendapatkan pemahaman yang lebih baik tentang lingkungan kontrol mereka dan akan membantu menggambarkan secara jelas kegiatan verifikasi yang akan dilakukan.

Kesimpulan

Menyediakan infrastruktur dan layanan yang sangat aman dan tangguh kepada pelanggan kami merupakan prioritas utama bagi AWS. Komitmen kami kepada pelanggan kami difokuskan untuk bekerja untuk terus mendapatkan kepercayaan pelanggan dan memastikan pelanggan mempertahankan kepercayaan dalam mengoperasikan beban kerja mereka dengan aman di AWS. Untuk mencapai hal ini, AWS memiliki mekanisme risiko dan kepatuhan terintegrasi yang meliputi:

- Implementasi berbagai macam kontrol keamanan dan alat otomatis
- Pemantauan dan penilaian kontrol keamanan secara berkelanjutan untuk membantu memastikan operasi AWS eectiveness dan kepatuhan yang ketat terhadap rezim kepatuhan
- Penilaian risiko independen oleh program AWS Business Risk Management
- Mekanisme operasional dan manajemen bisnis

Selain itu, AWS secara teratur menjalani audit pihak ketiga independen untuk memberikan jaminan bahwa kegiatan kontrol beroperasi sebagaimana dimaksud. Audit ini, bersama dengan banyak sertifikasi AWS telah diperoleh, memberikan tingkat tambahan validasi lingkungan kontrol AWS yang memberi manfaat kepada pelanggan.

Bersama dengan kontrol keamanan yang dikelola pelanggan, usaha-usaha ini memungkinkan AWS untuk berinovasi dengan aman atas nama pelanggan dan membantu pelanggan memperbaiki postur keamanan mereka saat membangun AWS.

Kontributor

Kontributor dokumen ini meliputi:

- Marta Taggart, Manajer Program Senior, Keamanan AWS
- Bradley Roach, Manajer Risiko, AWS Manajemen Risiko Bisnis
- Patrick Woods, Spesialis Keamanan Senior, AWS Keamanan

Pembacaan lebih lanjut

AWS menyediakan pelanggan dengan informasi mengenai keamanan dan lingkungan kontrol dengan:

- Memperoleh dan memelihara sertifikasi industri dan pengesahan pihak ketiga independen seperti yang tercantum di Halaman Program Kepatuhan AWS.
- Secara konsisten menerbitkan informasi tentang praktik keamanan dan kontrol AWS dalam whitepapers dan konten web, seperti AWS Security Blog.
- Menyediakan deskripsi mendalam tentang bagaimana AWS memanfaatkan otomatisasi dalam skala untuk mengelola infrastruktur layanan kami di The AWS Builders Library.
- Meningkatkan transparansi dengan memberikan sertifikasi kepatuhan, laporan, dan dokumentasi lainnya langsung ke pelanggan AWS melalui portal swalayan yang dikenal sebagai AWS Artifact.
- Menyediakan AWS Compliance Resources dan secara konsisten mendokumentasikan dan menerbitkan jawaban atas pertanyaan pada halaman web AWS Compliance FAQ .
- Pelanggan dapat mengikuti prinsip-prinsip desain dalam AWS Well-Architected Framework untuk bimbingan bagaimana mendekati di atas garis confrontasi beban kerja mereka membangun AWS.

Revisi Dokumen

Untuk diberitahu tentang pembaruan untuk whitepaper ini, berlangganan RSS feed.

memperbarui-sejarah-	update-history-description Ditinjau	update-history-date 10
perubahan Pembaruan kecil	untuk akurasi teknis	Maret 2021
(hal 12)	Versi ini mencakup perubahan substansial yang mencakup menghapus informasi referensi tentang program kepatuhan dan skema karena informasi ini tersedia pada Program Kepatuhan AWS dan AWS Layanan di Cakupan olehhalaman webProgram Kepatuhan . Selain itu, kami menghapus bagian yang mencakup pertanyaan kepatuhan umum karena informasi yang sekarang tersedia di halaman web AWS Compliance FAQ .	1 November 2020
Publikasi awal (hal 12)	Amazon Web Services: whitepaper Risiko dan Kepatuhan diterbitkan	1 Mei 2011

Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya untuk tujuan informasi, (b) mewakili penawaran dan praktik produk AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak menciptakan komitmen atau jaminan dari AWS dan afiliates, pemasok atau pemberi lisensi. AWS produk atau layanan disediakan “sebagaimana adanya” tanpa jaminan, representasi, atau kondisi apapun, baik tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggan dikendalikan oleh perjanjian AWS, dan dokumen ini bukan bagian dari, juga tidak memodifikasi, perjanjian antara AWS dan pelanggannya.