Unable to locate subtitle

Amazon Web Services: Risiko dan Kepatuhan

Amazon Web Services: Risiko dan Kepatuhan: ***Unable to locate subtitle***

Table of Contents

Amazon Web Services: Risiko dan Kepatuhan

Tanggal publikasi: 11 Maret 2021 (Revisi Dokumen)

Abstrak

AWS melayani berbagai pelanggan, termasuk yang ada di industri yang diatur. Melalui model tanggung jawab bersama, 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 mapan dan diakui secara luas. Laporan resmi ini menguraikan mekanisme yang telah diterapkan AWS untuk mengelola risiko di sisi Model Tanggung Jawab Bersama AWS, dan alat yang dapat dimanfaatkan pelanggan untuk mendapatkan kepastian bahwa mekanisme ini diterapkan secara efektif.

Pendahuluan

AWS dan pelanggannya berbagi kontrol atas lingkungan TI. Oleh karena itu, keamanan adalah tanggung jawab bersama. Dalam hal mengelola keamanan dan kepatuhan di 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 IT mereka dengan cara yang sesuai dengan persyaratan keamanan dan kepatuhan khusus mereka.

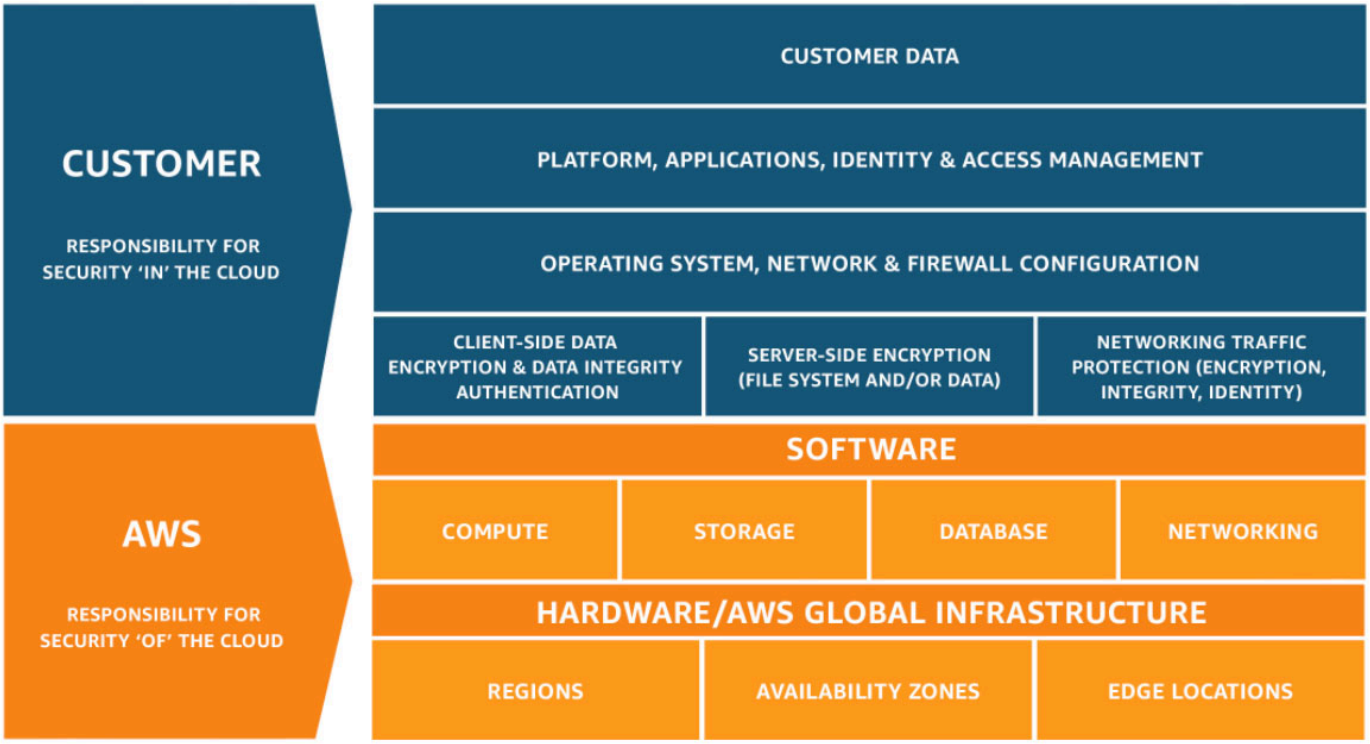
Laporan ini memberikan detail lebih lanjut tentang tanggung jawab keamanan masing-masing pihak dan cara pelanggan dapat memperoleh manfaat dari Program Risiko dan Kepatuhan AWS.

Model Tanggung Jawab Bersama

Keamanan dan Kepatuhan merupakan tanggung jawab bersama antara AWS dan pelanggan. Tergantung pada layanan yang di-deploy, model bersama ini dapat membantu meringankan beban operasional pelanggan. Hal ini karena AWS mengoperasikan, mengelola, dan mengontrol komponen infrastruktur, dari sistem operasi host dan lapisan virtualisasi, hingga keamanan fisik fasilitas tempat layanan beroperasi. Pelanggan memikul tanggung jawab dan pengelolaan sistem operasi tamu (termasuk pembaruan dan patch keamanan), perangkat lunak aplikasi terkait lainnya serta konfigurasi firewall grup keamanan yang disediakan AWS.

Kami merekomendasikan pelanggan untuk mempertimbangkan dengan hati-hati layanan yang mereka pilih karena tanggung jawab mereka akan bervariasi tergantung pada layanan yang digunakan, integrasi layanan tersebut ke dalam lingkungan IT mereka, serta undang-undang 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 firewall berbasis host, deteksi dan pencegahan intrusi berbasis host, enkripsi, dan manajemen kunci.

Sifat tanggung jawab bersama ini juga memberikan fleksibilitas dan kontrol pelanggan yang memungkinkan pelanggan untuk men-deploy solusi yang memenuhi persyaratan sertifikasi khusus industri.



Model tanggung jawab bersama pelanggan/AWS ini juga diperluas ke kontrol IT. AWS dan pelanggannya sama-sama bertanggung jawab untuk mengoperasikan lingkungan IT, begitu juga manajemen, operasi, dan verifikasi kontrol IT. AWS dapat membantu pelanggan dengan mengelola kontrol yang terkait dengan infrastruktur fisik yang di-deploy di lingkungan AWS. Pelanggan kemudian dapat menggunakan dokumentasi kontrol dan kepatuhan AWS yang tersedia bagi mereka untuk melakukan prosedur evaluasi dan verifikasi kontrol mereka sebagaimana diperlukan. Sebagai contoh bagaimana tanggung jawab atas kontrol tertentu dibagi antara AWS dan pelanggannya, lihat Model Tanggung Jawab Bersama AWS.

Mengevaluasi dan mengintegrasikan kontrol AWS

AWS menyediakan berbagai informasi mengenai lingkungan kontrol TI kepada pelanggan melalui laporan teknis laporan, sertifikasi, dan pengesahan pihak ketiga lainnya. Dokumentasi ini membantu pelanggan memahami kontrol yang ada, 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 IT diperluas mereka beroperasi secara efektif.

Secara tradisional, auditor internal dan/atau eksternal memvalidasi desain dan efektivitas operasional kontrol dengan panduan proses dan evaluasi bukti. Jenis pengamatan dan verifikasi langsung ini, oleh auditor eksternal pelanggan atau pelanggan, umumnya dilakukan untuk memvalidasi kontrol dalam deployment on-premise tradisional.

Dalam kasus di mana penyedia layanan digunakan (seperti AWS), pelanggan dapat meminta dan mengevaluasi pengesahan dan sertifikasi pihak ketiga. Pengesahan dan sertifikasi ini dapat membantu meyakinkan pelanggan tentang desain dan efektivitas operasi objektif dan kontrol yang divalidasi oleh pihak ketiga yang memenuhi syarat dan 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 efektif dan mempercepat proses peninjauan kepatuhan.

Pengesahan dan sertifikasi pihak ketiga AWS memberikan visibilitas dan validasi independen terhadap lingkungan kontrol kepada pelanggan. Pengesahan dan sertifikasi tersebut dapat membantu meringankan pelanggan dari persyaratan untuk melakukan validasi tertentu untuk lingkungan IT 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 deployment layanan dan terus meningkatkan dan menilai kembali kegiatan terkait risiko organisasi. Komponen program risiko dan kepatuhan terintegrasi AWS dibahas secara lebih rinci di bagian berikut.

Manajemen risiko bisnis AWS

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

- Melakukan penilaian risiko dan pemantauan risiko pada area fungsional AWS utama
- Mengidentifikasi dan mendorong remediasi risiko
- Mempertahankan daftar risiko yang diketahui

Untuk mendorong perbaikan risiko, program BRM melaporkan hasil upayanya, 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 dan laporan mingguan, bulanan, dan triwulanan untuk, antara lain, memastikan komunikasi risiko di semua komponen proses manajemen risiko. Selain itu, AWS menerapkan proses eskalasi untuk memberikan visibilitas manajemen ke dalam risiko prioritas tinggi di seluruh organisasi. Upaya ini, yang dilakukan bersama, membantu memastikan bahwa risiko dikelola secara konsisten dengan kompleksitas model bisnis AWS.

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

Kepemimpinan eksekutif dan senior memainkan peran penting dalam menetapkan sikap dan nilai-nilai inti AWS. Setiap karyawan diberikan Kode Perilaku dan Etika Bisnis perusahaan, dan

karyawan menyelesaikan pelatihan berkala. Audit kepatuhan dilakukan agar karyawan memahami dan mengikuti kebijakan yang ditetapkan.

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

Kontrol lingkungan dan otomatisasi

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

Sementara proses dan standar yang disertakan sebagai bagian dari lingkungan kontrol AWS berdiri sendiri, AWS juga memanfaatkan aspek lingkungan kontrol Amazon secara keseluruhan. Alat yang dimanfaatkan meliputi:

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

Dalam kasus di mana AWS memanfaatkan lingkungan kontrol Amazon secara keseluruhan, standar dan proses yang mengatur mekanisme ini disesuaikan khusus untuk bisnis AWS. Ini berarti bahwa harapan untuk penggunaan dan aplikasinya dalam lingkungan kontrol AWS mungkin berbeda dari harapan untuk penggunaan dan aplikasinya dalam lingkungan Amazon secara keseluruhan. Lingkungan kontrol AWS pada 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 implementasi kontrol keamanan informasi yang efektif dan manajemen risiko terkait. Otomatisasi kontrol berusaha untuk secara proaktif meminimalkan potensi inkonsistensi dalam pelaksanaan proses yang mungkin timbul karena sifat cacat 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 merekayasa lingkungan kontrol AWS untuk mendukung peningkatan tingkat otomatisasi kontrol sedapat mungkin. Contoh kontrol otomatis di AWS meliputi:

- Tata Kelola dan Pengawasan: Versi kebijakan dan persetujuan
- Manajemen Personalia: Pengiriman pelatihan otomatis, penghentian karyawan yang cepat
- Manajemen Pengembangan dan Konfigurasi: Saluran pipa deployment kode, pemindaian kode, pencadangan kode, pengujian deployment terpadu
- Manajemen Identitas dan Akses: Pemisahan tugas otomatis, ulasan akses, manajemen izin
- Monitoring dan Logging: Koleksi log otomatis dan korelasi, mengkhawatirkan
- Keamanan Fisik: Proses otomatis yang terkait dengan pusat data AWS, termasuk manajemen perangkat keras, pelatihan keamanan pusat data, mengkhawatirkan akses, dan manajemen akses fisik
- Manajemen Pemindaian dan Patch: Pemindaian kerentanan otomatis, manajemen patch, dan deployment

Mengontrol penilaian dan pemantauan berkelanjutan

AWS menerapkan berbagai aktivitas sebelum dan sesudah deployment layanan untuk mengurangi risiko lebih lanjut dalam lingkungan AWS. Aktivitas ini mengintegrasikan persyaratan keamanan dan kepatuhan selama desain dan pengembangan setiap layanan AWS dan kemudian memvalidasi bahwa layanan beroperasi dengan aman setelah dipindahkan ke produksi (diluncurkan).

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

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

Pada saat deployment, layanan akan melalui penilaian yang ketat terhadap persyaratan keamanan terperinci untuk memenuhi bilah tinggi AWS untuk keamanan. Kegiatan pasca-peluncuran adalah:

- Tinjauan berkelanjutan AWS Application Security untuk membantu memastikan postur keamanan layanan dipertahankan
- Pemindaian manajemen kerentanan berkelanjutan

Penilaian kontrol dan pemantauan berkelanjutan ini memungkinkan pelanggan yang diatur kemampuan untuk membangun solusi yang sesuai dengan percaya diri pada layanan AWS. Untuk daftar layanan dalam lingkup berbagai program kepatuhan, lihat halaman web AWS Services in Scope .

AWS Certification, Program, Laporan, dan Atestasi Pihak Ketiga

AWS secara teratur menjalani audit pengesahan pihak ketiga independen untuk memberikan jaminan bahwa aktivitas kontrol beroperasi sebagaimana dimaksud. Lebih khusus lagi, AWS diaudit terhadap berbagai kerangka kerja 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 tersedia untuk semua pelanggan AWS melalui AWS Artifact. AWS Artifact adalah portal layanan mandiri gratis untuk akses sesuai permintaan ke laporan kepatuhan AWS Ketika laporan baru dirilis, laporan tersebut tersedia di AWS Artifact, yang memungkinkan pelanggan untuk terus memantau keamanan dan kepatuhan AWS dengan akses langsung ke laporan baru.

Bergantung pada persyaratan peraturan atau kontrak lokal negara atau industri, AWS juga dapat menjalani audit secara 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 sendiri beroperasi dengan percaya diri, 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 halaman web AWS Services in Scope untuk informasi khusus layanan.

Cloud Security Alliance (CSA)

AWS berpartisipasi dalam Penilaian Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR) sukarela untuk mendokumentasikan kepatuhan kami dengan praktik terbaik yang diterbitkan CSA. CSA adalah “organisasi terkemuka di dunia yang didedikasikan untuk

mendefinisikan dan meningkatkan kesadaran akan praktik terbaik untuk membantu memastikan lingkungan komputasi cloud yang aman". The CSA Consensus Assessments Initiative Questionnaire (CAIQ) memberikan serangkaian pertanyaan CSA mengantisipasi pelanggan cloud dan/atau auditor cloud akan meminta penyedia cloud. Dokumen ini menyediakan serangkaian pertanyaan keamanan, kontrol, dan proses yang kemudian dapat digunakan untuk berbagai penggunaan, termasuk seleksi penyedia cloud dan evaluasi keamanan.

Ada dua sumber daya yang tersedia untuk pelanggan yang mendokumentasikan keselarasan AWS ke CSA CAIQ. Yang pertama adalah Laporan resmi CSA CAIQ, dan yang kedua adalah pemetaan kontrol yang lebih rinci untuk kontrol SOC-2 kami yang tersedia 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 di-deploy. Praktik terkemuka meliputi:

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

Deployment di AWS Cloud memberikan opsi berbeda kepada perusahaan untuk menerapkan berbagai jenis kontrol dan berbagai metode verifikasi.

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

1. Meninjau Model Tanggung Jawab BersamaAWS, Dokumentasi KeamananAWS, laporan kepatuhan AWS, dan informasi lain yang tersedia dari AWS, bersama dengan dokumentasi khusus pelanggan lainnya. Cobalah untuk memahami sebanyak mungkin seluruh lingkungan TI, dan kemudian mendokumentasikan semua persyaratan kepatuhan ke dalam kerangka kerja kontrol cloud yang komprehensif.
2. Merancang dan menerapkan tujuan kontrol untuk memenuhi persyaratan kepatuhan perusahaan sebagaimana tercantum dalam Model Tanggung Jawab Bersama AWS.
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 dengan jelas menggambarkan kegiatan verifikasi yang akan dilakukan.

Kesimpulan

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

- Implementasi berbagai kontrol keamanan dan alat otomatis
- Pemantauan dan penilaian berkelanjutan terhadap kontrol keamanan untuk membantu memastikan efektivitas operasional AWS dan kepatuhan yang ketat terhadap rezim kepatuhan
- Penilaian risiko independen oleh program Manajemen Risiko Bisnis AWS
- Mekanisme operasional dan manajemen bisnis

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

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

Kontributor

Kontributor dokumen ini meliputi:

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

Bacaan lebih lanjut

AWS memberi pelanggan informasi mengenai lingkungan keamanan dan kontrolnya 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 di laporan resmi dan konten web, seperti Blog Keamanan AWS.
- Menyediakan deskripsi mendalam tentang bagaimana AWS memanfaatkan otomatisasi sesuai skala untuk mengelola infrastruktur layanan kami di AWS Builders Library.
- Meningkatkan transparansi dengan menyediakan sertifikat kepatuhan, laporan, dan dokumentasi lainnya secara langsung kepada pelanggan AWS melalui portal layanan mandiri yang dikenal sebagai AWS Artifact.
- Menyediakan Sumber Daya Kepatuhan AWS dan secara konsisten mendokumentasikan dan menerbitkan jawaban atas kueri di halaman web FAQ Kepatuhan AWS .
- Pelanggan dapat mengikuti prinsip-prinsip desain dalam AWS Well-Architected Framework untuk panduan bagaimana mendekati konfigurasi garis di atas beban kerja mereka yang dibangun di AWS.

Revisi Dokumen

Untuk menerima pemberitahuan tentang pembaruan laporan resmi ini, berlangganan umpan RSS.

perubahan-riwayat-pembaruan	pembaruan-riwayat-pembaruan	pembaruan-riwayat-tanggal
Pembaruan kecil	Ditinjau untuk akurasi teknis	10 Maret 2021
Laporan resmi diperbarui	Versi ini mencakup perubahan substansial yang mencakup penghapusan informasi referensi tentang program kepatuhan dan skema karena informasi ini tersedia di halaman web Program Kepatuhan AWS dan AWS Services in Scope by Compliance Program . Selain itu, kami menghapus bagian yang mencakup pertanyaa n kepatuhan umum karena informasi tersebut sekarang tersedia di halaman web FAQ Kepatuhan AWS .	1 November 2020
Publikasi awal	Amazon Web Services: Laporan Resmi Risiko dan Kepatuhan dipublikasikan	1 Mei 2011

Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya disediakan sebagai informasi, (b) berisi penawaran produk dan praktik AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak menjadi komitmen atau jaminan apa pun dari AWS dan afiliasi, pemasok, atau pemberi lisensinya. Produk atau layanan AWS disediakan “sebagaimana adanya” tanpa jaminan, representasi, atau ketentuan apa pun, baik tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggannya dikendalikan oleh perjanjian AWS, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.