Certificazioni AWS, programmi, rapporti e attestazioni di terze parti

Gennaio 2017

Note

Il presente documento è fornito a solo scopo informativo. In esso sono illustrate le attuali offerte di prodotti e le prassi di AWS alla data di pubblicazione del documento, offerte che sono soggette a modifica senza preavviso. È responsabilità dei clienti effettuare una propria valutazione indipendente delle informazioni contenute nel presente documento e dell'uso dei prodotti o dei servizi di AWS, ciascuno dei quali viene fornito "così com'è", senza garanzie di alcun tipo, né esplicite né implicite. Il presente documento non dà origine a garanzie, rappresentazioni, impegni contrattuali, condizioni o assicurazioni da parte di AWS, delle sue società affiliate, dei suoi fornitori o dei licenzianti. Le responsabilità di AWS nei confronti dei propri clienti sono definite dai contratti AWS e il presente documento non costituisce parte né modifica qualsivoglia contratto tra AWS e i suoi clienti.

Indice

Sintesi

AWS collabora con organismi di certificazione esterni e revisori indipendenti per fornire ai clienti numerose informazioni sulle policy, i processi e i controlli definiti e gestiti da AWS.

CJIS

AWS soddisfa lo standard CJIS (Criminal Justice Information Services) dell'FBI. AWS stipula con i clienti accordi di sicurezza basati sugli standard dei servizi informativi delle autorità giudiziarie penali statunitensi (Criminal Justice Information Services, CJIS); tali standard consentono anche l'esecuzione di controlli sul background dei dipendenti, in base a quanto previsto dalla CJIS Security Policy.

e autorità giudiziarie (e i partner che gestiscono i servizi CJI) ricorrono ad AWS per incrementare la sicurezza e la protezione dei dati CJI; AWS fornisce infatti caratteristiche e servizi di sicurezza avanzati, come la registrazione delle attività(AWS CloudTrail), la crittografia dei dati in movimento e inattivi (crittografia lato server S3 con la possibilità di portare la propria chiave), la gestione e la protezione complete delle chiavi (AWS Key Management Service e CloudHSM) e la gestione integrata delle autorizzazioni (gestione dell'identità federata IAM, autenticazione a più fattori).

AWS ha redatto una guida pratica sui servizi CJIS che fornisce un modello di piano di sicurezza che copre le aree della CJIS Security Policy. È stato inoltre sviluppato un whitepaper sui servizi CJIS per aiutare i clienti lungo il percorso di adozione del cloud.

Visitare la pagina relativa a CJIS all'indirizzo https://aws.amazon.com/compliance/cjis/.

CSA

Nel 2011, la Cloud Security Alliance (CSA) ha lanciato STAR (Security, Trust & Assurance Registry), un'iniziativa per incoraggiare la trasparenza delle prassi di sicurezza dei fornitori di servizi cloud. STAR è un registro pubblico gratuito che documenta i controlli di sicurezza forniti da varie soluzioni di cloud computing, per aiutare gli utenti a valutare la sicurezza dei fornitori di servizi cloud di cui si avvalgono o a cui stanno valutando di rivolgersi. AWS è presente nel registro STAR e ha completato il questionario CAIQ (Consensus Assessments Initiative Questionnaire) della CSA. Tale questionario pubblicato dalla CSA consente di documentare e descrivere quali sono i controlli di sicurezza presenti nelle offerte IaaS (Infrastructure-as-a-Service) di AWS. Il questionario CAIQ fornisce oltre 298 domande che un consumatore di servizi cloud e un cloud auditor potrebbero chiedere a un fornitore di servizi cloud.

Consultare il questionario CAIQ della CSA.

Cyber Essentials Plus

Cyber Essentials Plus è un programma di certificazione di settore sostenuto dal governo del Regno Unito introdotto nel paese per aiutare le organizzazioni a dimostrare di possedere una sicurezza operativa in grado di contrastare gli attacchi informatici.

Serve a documentare i controlli di base implementati da AWS per mitigare il rischio delle più comuni minacce provenienti da Internet, nel contesto dell'iniziativa del governo del Regno Unito "10 Steps to Cyber Security". È sostenuta dai rappresentanti di settore, compresa la Federation of Small Businesses, la Confederation of British Industry e numerose organizzazioni che operano in campo assicurativo e che offrono incentivi alle imprese che sono titolari di tale certificazione.

Cyber Essentials definisce i controlli tecnici necessari e il relativo quadro di certificazione mostra il funzionamento del processo di certificazione indipendente per la certificazione Cyber Essentials Plus mediante una valutazione esterna annuale eseguita da un valutatore accreditato. A causa della natura regionale della certificazione, l'ambito della certificazione è limitato alla regione UE (Irlanda).

SRG DoD Livelli 2 e 4

La guida ai requisiti di sicurezza per il cloud del Dipartimento della Difesa statunitense fornisce una procedura formale di valutazione e di autorizzazione per i fornitori di servizi cloud; tale procedura consente a questi ultimi di ottenere un'autorizzazione provvisoria che può essere quindi utilizzata dai clienti del Dipartimento. L'autorizzazione provvisoria nel quadro del modello di sicurezza del cloud fornisce una certificazione riutilizzabile che attesta la conformità di Amazon agli standard DoD e riduce il tempo necessario affinché un mission owner DoD valuti e autorizzi uno dei sistemi per il funzionamento in AWS. AWS detiene attualmente le autorizzazioni provvisorie dei livelli 2 e 4 di SRG.

Per ulteriori informazioni sui controlli di base sulla sicurezza definiti per i livelli 2, 4, 5 e 6 consultare il sito: http://iase.disa.mil/cloud_security/Pages/index.aspx.

Visitare la pagina dedicata al Dipartimento della Difesa all'indirizzo https://aws.amazon.com/compliance/dod/.

FedRAMP SM

AWS è un fornitore di servizi cloud conforme al programma federale di gestione del rischio e delle autorizzazioni (FedRAMPsm, Federal Risk and Authorization Management Program). AWS ha superato i test eseguiti da un ente di valutazione indipendente accreditato da FedRAMPsm e ha ottenuto due autorizzazioni a operare (ATO) dal Dipartimento della salute e dei servizi umani degli Stati Uniti, essendo risultata conforme ai requisiti FedRAMPsm a livello di impatto moderato. Tutte le agenzie governative degli Stati Uniti possono utilizzare i pacchetti delle autorizzazioni ATO di AWS presenti nell'archivio FedRAMPsm per valutare AWS in relazione ai propri carichi di lavoro e applicazioni, fornire autorizzazioni per l'utilizzo di AWS e spostare i carichi di lavoro nell'ambiente AWS. Le due autorizzazioni ATO FedRAMPsm comprendono tutte le regioni degli Stati Uniti (la regione AWS GovCloud (US) e le regioni AWS degli Stati Uniti orientali/occidentali).

I seguenti servizi rientrano nell'ambito dell'accreditamento per le regioni indicate in precedenza:

- **Amazon Redshift**: Amazon Redshift è un servizio di data warehouse rapido e completamente gestito, con scalabilità di petabyte, che consente di analizzare in modo efficiente, semplice e conveniente tutti i dati utilizzando gli strumenti di business intelligence esistenti. Per ulteriori informazioni, fare clic qui.
- **Amazon Elastic Compute Cloud (Amazon EC2)**: Amazon EC2 mette a disposizione capacità di elaborazione nel cloud ridimensionabili a seconda delle esigenze. È un servizio progettato per semplificare l'elaborazione a livello Web per gli sviluppatori. Per ulteriori informazioni, fare clic qui.
- **Amazon Simple Storage Service (S3)**: Amazon S3 offre una semplice interfaccia di servizi Web che è possibile utilizzare per archiviare e recuperare qualunque quantità di dati, in qualsiasi momento, ovunque nel Web. Per ulteriori informazioni, fare clic qui.
- **Amazon Virtual Private Cloud (VPC)**: Amazon VPC consente di effettuare il provisioning di una sezione di AWS isolata a livello logico dove è possibile avviare le risorse AWS in una rete virtuale definita dall'utente. Per ulteriori informazioni, fare clic qui.
- **Amazon Elastic Block Store (EBS)**: Amazon EBS offre volumi di storage a disponibilità elevata ed estremamente affidabili e prevedibili che possono essere collegati a un'istanza di Amazon EC2 in esecuzione ed esposti come dispositivo all'interno dell'istanza. Per ulteriori informazioni, fare clic qui.
- **AWS Identity and Access Management (IAM)**: IAM consente di controllare in modo sicuro l'accesso ai servizi e alle risorse AWS per gli utenti. Grazie a IAM, è possibile creare e gestire utenti e gruppi AWS e utilizzare le autorizzazioni per consentire e negare l'accesso alle risorse AWS. Per ulteriori informazioni, fare clic qui.

Per ulteriori informazioni sulla conformità di AWS a FedRAMP^{sm}, consultare le domande frequenti su AWS e FedRAMP^{sm} all'indirizzo https://aws.amazon.com/compliance/fedramp/.

FERPA

La legge Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Parte 99) è una legge federale che tutela la privacy della documentazione degli studenti relativa agli studi effettuati. La legge si applica a tutti gli istituti scolastici che ricevono fondi da un programma apposito del Dipartimento dell'istruzione degli Stati Uniti. La legge FERPA concede ai genitori determinati diritti riguardo alla documentazione sugli studi dei loro figli. Tali diritti vengono trasferiti allo studente al compimento del 18° anno di età o quando inizia un corso di studi dopo le superiori. Gli studenti a cui sono stati trasferiti i diritti diventano "studenti idonei".

AWS consente agli enti interessati e ai loro soci d'affari soggetti alla legge FERPA di utilizzare l'ambiente sicuro AWS per elaborare, gestire e archiviare dati protetti relativi all'istruzione.

AWS offre inoltre un whitepaper incentrato sulle disposizioni FERPA per i clienti interessati a scoprire come utilizzare AWS per l'elaborazione e lo storage dei dati didattici.

Il whitepaper FERPA Compliance on AWS descrive in che modo le aziende possono utilizzare AWS per elaborare sistemi che facilitino la conformità a FERPA:

FIPS 140-2

Il Federal Information Processing Standard (FIPS) Publication 140-2 è uno standard di sicurezza del governo degli Stati Uniti che specifica i requisiti di sicurezza previsti per i moduli crittografici che proteggono le informazioni sensibili. Per supportare i clienti che devono soddisfare i requisiti FIPS 140-2, le terminazioni SSL in AWS GovCloud (US) utilizzano hardware con convalida FIPS 140-2. AWS collabora con i clienti AWS GovCloud (US) per fornire le informazioni necessarie a gestire la conformità nell'ambiente AWS GovCloud (US).

FISMA e DIACAP

AWS consente alle agenzie governative degli Stati Uniti di ottenere e mantenere la conformità al Federal Information Security Management Act (FISMA). L'infrastruttura AWS è stata valutata da soggetti indipendenti per una varietà di sistemi governativi nel quadro del processo di approvazione dei rispettivi proprietari dei sistemi. Numerose organizzazioni civili federali e del Dipartimento della difesa (DoD) hanno ottenuto le autorizzazioni di sicurezza per i sistemi ospitati in AWS ai sensi del processo Risk Management Framework (RMF) definito nello standard NIST 800-37 e del processo del DoD Information Assurance Certification and Accreditation Process (DIACAP).

GxP

L'acronimo GxP si riferisce alle normative e alle linee guida applicabili alle organizzazioni delle scienze della vita che producono alimenti e prodotti medicali come farmaci, dispositivi e applicazioni software medicali. La finalità complessiva dei requisiti GxP consiste nel garantire che gli alimenti e i prodotti medicali siano sicuri per i consumatori e nell'assicurare l'integrità dei dati utilizzati per prendere decisioni sulla sicurezza associate ai prodotti.

AWS offre un whitepaper su GxP, che illustra i dettagli di un approccio completo per l'utilizzo di AWS per sistemi GxP. Questo whitepaper fornisce indicazioni sull'utilizzo dei prodotti AWS nel contesto dei sistemi GxP, con contenuti che sono stati sviluppati in collaborazione con clienti AWS nel settore dei dispositivi farmaceutici e medici e partner software che attualmente utilizzano prodotti AWS nei loro sistemi GxP convalidati.

Per ulteriori informazioni su GxP in AWS, contattare l'ufficio commerciale e di sviluppo aziendale AWS.

Per ulteriori informazioni, consultare le domande frequenti sulla conformità a GxP all'indirizzo https://aws.amazon.com/compliance/gxp-part-11-annex-11/.

HIPAA

AWS consente agli enti interessati e ai loro soci d'affari soggetti all'Health Insurance Portability and Accountability Act (HIPAA) degli Stati Uniti di utilizzare l'ambiente sicuro AWS per elaborare, gestire e archiviare dati sanitari protetti. AWS firmerà accordi di associazione commerciale con tali clienti. AWS offre, inoltre, un whitepaper incentrato sulle disposizioni HIPAA ai clienti interessati a scoprire come utilizzare AWS per l'elaborazione e lo storage dei dati sanitari. Il whitepaper Architecting for HIPAA Security and Compliance on Amazon Web Services descrive in che modo le aziende possono utilizzare AWS per elaborare sistemi che facilitino la conformità a HIPAA e a HITECH (Health Information Technology for Economic and Clinical Health).

I clienti potranno impiegare tutti i servizi AWS all'interno dell'account designato per l'uso secondo la normativa HIPAA, ma potranno elaborare, immagazzinare e trasmettere informazioni sanitarie protette solamente nell'ambito dei servizi definiti nel BAA. Esistono attualmente nove servizi idonei ai fini HIPAA, ovvero:

- Amazon DynamoDB
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (Amazon RDS) con il solo utilizzo di motori MySQL e Oracle
- Amazon Simple Storage Service (S3)

AWS segue un programma di gestione del rischio basato su standard per garantire che i servizi idonei ai fini HIPAA supportino specificamente i processi di sicurezza, controllo e amministrazione prescritti ai sensi HIPAA. L'utilizzo di questi servizi per lo storage e l'elaborazione dei dati medici privati consente ai clienti e ad AWS di soddisfare i requisiti HIPAA applicabili al modello operativo basato su utilità. AWS aggiunge nuovi servizi idonei secondo una priorità basata sulla domanda dei clienti.

Per ulteriori informazioni, consultare le domande frequenti sulla conformità a HIPAA e il whitepaper Architecting for HIPAA Security and Compliance on Amazon Web Services.

IRAP

L'Information Security Registered Assessors Program (IRAP) consente ai clienti degli enti pubblici australiani di convalidare la presenza di controlli adeguati e di stabilire il modello di responsabilità più adatto a soddisfare le esigenze dell'Information Security Manual (ISM) dell'Australian Signals Directorate (ASD).

Amazon Web Services ha portato a termine una valutazione indipendente che ha accertato la presenza di tutti i controlli ISM applicabili nell'ambito dell'elaborazione, dello storage e della trasmissione di dati non classificati (DLM) per la regione AWS di Sydney.

Per ulteriori informazioni, consultare le domande frequenti sulla conformità a IRAP all'indirizzo https://aws.amazon.com/compliance/irap/ e le informazioni sulla conformità di AWS alle considerazioni in materia di sicurezza del cloud computing dell'Australian Signals Directorate (ASD).

ISO 9001

AWS ha conseguito la certificazione ISO 9001, che le consente di supportare direttamente i clienti che sviluppano, migrano e gestiscono i loro sistemi IT di qualità controllata nel cloud AWS. I clienti possono utilizzare i rapporti di conformità AWS come prove nei programmi ISO 9001 e nei programmi di qualità specifici del settore, come GxP nelle scienze biologiche, ISO 13485 nei dispositivi medici, AS9100 nel settore aerospaziale e ISO/TS 16949 nel settore automobilistico. I clienti AWS che non presentano requisiti per i sistemi di qualità trarranno comunque vantaggio dall'ulteriore garanzia e trasparenza offerte dalla certificazione ISO 9001.

La certificazione ISO 9001 comprende il sistema di gestione della qualità in un ambito specificato di servizi e di regioni di operazioni AWS (di seguito), tra cui:

- AWS CloudFormation
- AWS Cloud Hardware Security Model (HSM)
- Amazon CloudFront
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Amazon EC2 Container Service (ECS)
- Amazon Elastic File System (EFS)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)

- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- AWS Storage Gateway
- Amazon Simple Workflow Service (SWF)
- Amazon Virtual Private Cloud (VPC)
- AWS WAF - Web Application Firewall
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- L'infrastruttura fisica sottostante e l'ambiente di gestione AWS

L'accreditamento ISO 9001 comprende le regioni AWS, inclusi Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), AWS GovCloud (Stati Uniti), Sud America (San Paolo), UE (Irlanda), UE (Francoforte) e Asia Pacifico (Singapore), Asia Pacifico (Sydney) e Asia Pacifico (Tokyo).

ISO 9001:2008 è uno standard globale per la gestione della qualità di prodotti e servizi. Lo standard 9001 definisce un sistema di gestione della qualità basato su otto principi, definiti dal comitato tecnico per il Quality Management ed il Quality Assurance dell'International Organization for Standardization (ISO). Gli otto principi sono:

- Orientamento al cliente
- Leadership
- Coinvolgimento del personale
- Approccio per processi
- Approccio sistemico alla gestione
- Miglioramento continuo
- Approccio basato sui dati nel processo decisionale
- Rapporti con i fornitori reciprocamente vantaggiosi

La certificazione ISO 9001 di AWS può essere scaricata all'indirizzo https://d0.awsstatic.com/certifications/iso_9001_certification.pdf.

AWS ha pubblicato ulteriori informazioni e le domande frequenti riguardo alla certificazione ISO 9001 all'indirizzo: https://aws.amazon.com/compliance/iso-9001-faqs/.

ISO 27001

AWS ha conseguito la certificazione ISO 27001 per il sistema ISMS (Information Security Management System) che copre l'infrastruttura, i data center e i servizi AWS, compresi:

- AWS CloudFormation
- Amazon CloudFront
- AWS Cloudtrail
- AWS Directory Service
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Amazon EC2 Container Service (ECS)
- AWS Direct Connect
- Amazon EC2 VM Import/Export
- AWS Cloud Hardware Security Model (HSM)
- Elastic Load Balancing (ELB)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)

- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- AWS WAF - Web Application Firewall
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- L'Infrastruttura fisica sottostante (compreso GovCloud) e l'ambiente di gestione AWS

ISO 27001/27002 è uno standard di sicurezza ampiamente adottato a livello globale che stabilisce i requisiti e le best practice per un approccio sistematico alla gestione delle informazioni aziendali e dei clienti basato su valutazioni periodiche del rischio idonee a scenari di rischio in continua evoluzione. Per ottenere la certificazione, un'azienda deve dimostrare di avere adottato un approccio sistematico e continuativo per la gestione dei rischi di sicurezza delle informazioni che minacciano la riservatezza, l'integrità e la disponibilità delle informazioni aziendali e dei clienti. La certificazione costituisce un'ulteriore dimostrazione dell'impegno di Amazon teso a fornire informazioni significative circa i suoi controlli e le sue prassi di sicurezza.

L'accreditamento ISO 27001 comprende le regioni AWS, inclusi Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), AWS GovCloud (Stati Uniti), Sud America (San Paolo), UE (Irlanda), UE (Francoforte), Asia Pacifico (Singapore), Asia Pacifico (Sydney) e Asia Pacifico (Tokyo).

La certificazione ISO 27001 di AWS può essere scaricata all'indirizzo https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf.

AWS ha pubblicato ulteriori informazioni e le domande frequenti riguardo alla certificazione ISO 27001 all'indirizzo: https://aws.amazon.com/compliance/iso-27001-faqs/.

ISO 27017

ISO 27017 è il codice più recente sulle best practice pubblicato all'International Organization for Standardization (ISO). Fornisce indicazioni sull'implementazione dei controlli per la sicurezza delle informazioni che riguardano specificamente i servizi cloud.

AWS ha conseguito la certificazione ISO 27017 per il sistema ISMS (Information Security Management System) che copre l'infrastruttura, i data center e i servizi AWS, compresi:

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift

- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway
- AWS WAF (Web Application Firewall)
- Elastic Load Balancing
- VM Import/Export

La certificazione ISO 27017 di AWS può essere scaricata all'indirizzo https://d0.awsstatic.com/certifications/iso_27017_certification.pdf.

Per ulteriori informazioni e domande frequenti sulla certificazione ISO 27017 di AWS, visitare il sito all'indirizzo https://aws.amazon.com/compliance/iso-27017-faqs/.

ISO 27018

ISO 27018 è il primo codice internazionale delle best practice incentrato sulla protezione dei dati personali nel cloud. Si basa sullo standard ISO 27002 relativo alla sicurezza delle informazioni e fornisce indicazioni per l'implementazione dei controlli ISO 27002 che si applicano alle informazioni di carattere personale nel cloud pubblico. Prevede, inoltre, una serie di controlli aggiuntivi e di indicazioni associate finalizzati al soddisfacimento dei requisiti relativi alle informazioni di carattere personale nel cloud pubblico non previsti dal gruppo di controlli dello standard ISO 27002 esistente.

AWS ha conseguito la certificazione ISO 27018 per il sistema ISMS (Information Security Management System) che copre l'infrastruttura, i data center e i servizi AWS, compresi:

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)

- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway
- AWS WAF (Web Application Firewall)
- Elastic Load Balancing
- VM Import/Export

La certificazione ISO 27018 di AWS può essere scaricata all'indirizzo https://d0.awsstatic.com/certifications/iso_27018_certification.pdf.

Per ulteriori informazioni e domande frequenti sulla certificazione ISO 27018 di AWS, visitare il sito all'indirizzo https://aws.amazon.com/compliance/iso-27018-faqs/.

ITAR

La regione AWS GovCloud (US) supporta la conformità alle normative International Traffic in Arms Regulations (ITAR) degli Stati Uniti. Nel quadro della gestione di un programma completo di conformità ITAR, le aziende soggette alla disciplina ITAR sulle esportazioni devono controllare le esportazioni non volute limitando l'accesso ai dati protetti ai soggetti statunitensi e l'ubicazione fisica di tali dati agli Stati Uniti. AWS GovCloud (Stati Uniti) offre un ambiente ubicato fisicamente negli Stati Uniti, il cui accesso da parte del personale AWS è limitato a soggetti statunitensi, consentendo in tal modo ad aziende qualificate di trasmettere, elaborare e archiviare articoli e dati protetti soggetti alle limitazioni ITAR. L'ambiente AWS GovCloud (Stati Uniti) è stato sottoposto al controllo di una terza parte indipendente per convalidare l'esistenza di controlli adeguati a sostegno dei programmi di conformità delle esportazioni dei clienti finalizzati a questo requisito.

MPAA

La Motion Picture Association of America (MPAA) ha definito una serie di best practice per archiviare, elaborare e fornire in modo sicuro supporti e contenuti protetti (http://www.fightfilmtheft.org/facility-security-program.html). Le aziende del settore dei media utilizzano queste best practice per valutare il rischio e la sicurezza dei loro contenuti e delle loro infrastrutture. AWS ha dimostrato di rispettare le best practice MPAA e che l'infrastruttura AWS è conforme a tutti i controlli infrastrutturali MPAA applicabili. Sebbene la MPAA non fornisca una "certificazione", i clienti del settore dei media possono utilizzare la documentazione MPAA AWS per migliorare la propria valutazione del rischio e la valutazione dei contenuti di tipo MPAA in AWS.

Per ulteriori dettagli, consultare la pagina sulla conformità di AWS alle best practice di MPAA all'indirizzo https://aws.amazon.com/compliance/mpaa/.

Certificazione MTCS livello 3

La certificazione Multi-Tier Cloud Security (MTCS) è uno standard di gestione della sicurezza in uso a Singapore (SPRING SS 584:2013) basato sugli standard ISMS (Information Security Management System) ISO 27001/02. La valutazione della certificazione prevede che AWS esegua le seguenti operazioni:

- Valutare sistematicamente i rischi di sicurezza relativi alle informazioni, prendendo in esame l'impatto di minacce aziendali e vulnerabilità.
- Progettare e implementare una suite completa di controlli di sicurezza delle informazioni e altre forme di gestione del rischio per far fronte ai rischi di sicurezza aziendali e architetturali.
- Adottare una procedura di gestione completa che accerti la conformità dei controlli di sicurezza delle informazioni alle esigenze in fatto di protezione delle informazioni in modo regolare.

Visitare la pagina su MTCS all'indirizzo https://aws.amazon.com/compliance/aws-multitiered-cloud-security-standard-certification/.

NIST

Nel giugno 2015, il National Institute of Standards and Technology (NIST) ha pubblicato le linee guida 800-171, "Final Guidelines for Protecting Sensitive Government Information Held by Contractors". Tali linee guida si applicano alla protezione di informazioni controllate non classificate (Controlled Unclassified Information - CUI) su sistemi non federali.

AWS è già conforme a tali linee guida e i clienti dispongono immediatamente della conformità a NIST 800-171. Le linee guida NIST 800-171 definiscono un sottoinsieme dei requisiti NIST 800-53, ovvero linee guida in base alle quali AWS è già stata sottoposta ad audit nel quadro del programma FedRAMP. La baseline del controllo di sicurezza FedRAMP Moderate è più rigorosa dei requisiti raccomandati dal Capo 3 di 800-171 e comprende un numero significativo di controlli di sicurezza più stringenti rispetto a quelli prescritti dai sistemi FISMA Moderate che proteggono i dati CUI. Una mappatura dettagliata è disponibile in NIST Special Publication 800-171, a partire dalla pagina D2 (ovvero la pagina 37 del file PDF).

PCI DSS livello 1

AWS è conforme al livello 1 ai fini dello standard PCI Data Security (DSS). I clienti possono eseguire applicazioni nell'infrastruttura tecnologica conforme a PCI per archiviare, elaborare e trasmettere informazioni sulle carte di credito nel cloud. Nel febbraio 2013, il PCI Security Standards Council ha pubblicato il documento PCI DSS Cloud Computing Guidelines. Tali linee guida offrono ai clienti che gestiscono un ambiente per i dati dei titolari di carte di credito indicazioni su come mantenere i controlli PCI DSS nel cloud. AWS ha inserito le linee guida PCI DSS Cloud Computing nel pacchetto AWS PCI conformità per i clienti. Il pacchetto AWS PCI Compliance include l'attestazione di conformità (AoC) di AWS a PCI, che dimostra che AWS è stata ritenuta conforme agli standard applicabili a un fornitore di servizi di livello 1 ai sensi di PCI DSS versione 3.1 e il riepilogo delle responsabilità di AWS in relazione allo standard PCI, che spiega in che modo vengono condivise le responsabilità in materia di conformità tra AWS e i clienti nel cloud.

I seguenti servizi rientrano nell'ambito di applicazione di PCI DSS livello 1:

- Auto Scaling
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Key Management Service (KMS)

- AWS Identity and Access Management (IAM)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Storage Service (S3)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Workflow Service SWF
- Amazon Virtual Private Cloud (VPC)
- L'infrastruttura fisica sottostante (compreso GovCloud) e l'ambiente di gestione AWS

L'ultimo aggiornamento sui servizi e sulle regioni per la certificazione AWS PCI DSS di livello 1 è disponibile all'indirizzo https://aws.amazon.com/compliance/pci-dss-level-1-faqs/.

SOC 1/ISAE 3402

Amazon Web Services pubblica un rapporto Service Organization Controls 1 (SOC 1) di tipo II. Il controllo per questo rapporto viene effettuato ai sensi degli standard American Institute of Certified Public Accountants (AICPA): AT 801 (ex SSAE 16) e International Standards for Assurance Engagements No. 3402 (ISAE 3402). Questo rapporto, che riguarda due standard, ha lo scopo di soddisfare una vasta gamma di requisiti di controllo finanziario per gli organismi di revisione statunitensi e internazionali. Il rapporto SOC 1 attesta che gli obiettivi di controllo di AWS sono stati definiti idoneamente e che i singoli controlli definiti per tutelare i dati dei clienti sono efficaci. Questo rapporto sostituisce il rapporto di controllo Statement on Auditing Standards No. 70 (SAS 70) di tipo II.

Gli obiettivi di controllo di AWS SOC 1 sono specificati di seguito. Lo stesso rapporto indica le attività di controllo che supportano ciascuno degli obiettivi e gli esiti delle procedure di prova di ogni controllo effettuate dal revisore indipendente.

Area dell'obiettivo	Descrizione dell'obiettivo
Organizzazione della sicurezza	I controlli forniscono una ragionevole garanzia del fatto che le policy di sicurezza siano state implementate e comunicate nell'intera organizzazione.
Accesso utente dei dipendenti	I controlli forniscono una ragionevole garanzia del fatto che siano state definite procedure che consentano di aggiungere, modificare e cancellare gli account utente dei dipendenti Amazon in modo tempestivo e di controllarli periodicamente.
Sicurezza logica	I controlli forniscono una ragionevole garanzia del fatto che esistano policy e meccanismi capaci di limitare adeguatamente gli accessi interni ed esterni non autorizzati ai dati e di consentire l'opportuna separazione dei dati dei diversi clienti.
Gestione sicura dei dati	I controlli forniscono una ragionevole garanzia del fatto che la gestione dei dati tra il punto iniziale presso il cliente e la posizione di storage AWS avvenga in modo sicuro e sia mappata con precisione.
Sicurezza fisica e protezione ambientale	I controlli forniscono una ragionevole garanzia del fatto che l'accesso fisico ai data center sia limitato al personale autorizzato e che esistano meccanismi capaci di ridurre al minimo gli effetti di un malfunzionamento o di un'emergenza fisica per le strutture dei data center.
Gestione delle modifiche	I controlli forniscono una ragionevole garanzia del fatto che le modifiche (comprese quelle di emergenza/non di routine e relative alla configurazione) alle risorse IT esistenti siano registrate, autorizzate, testate, approvate e documentate.
Integrità, disponibilità e ridondanza dei dati	I controlli forniscono una ragionevole garanzia del fatto che l'integrità dei dati sia preservata in tutte le fasi, compresa la trasmissione, lo storage e l'elaborazione.
Gestione degli eventi imprevisti	I controlli forniscono una ragionevole garanzia del fatto che gli eventi imprevisti relativi ai sistemi siano registrati, analizzati e risolti.

I rapporti SOC 1 sono pensati per focalizzare l'attenzione sui controlli a livello di organizzazione di servizi che potrebbero essere pertinenti ai fini della revisione dei bilanci di un'entità utente. Dato che AWS ha un'ampia base clienti e che l'utilizzo dei servizi AWS è altrettanto diffuso, l'applicabilità dei controlli ai bilanci dei clienti varia in base al cliente. Il rapporto AWS SOC 1, pertanto, è pensato per includere controlli principali specifici che potrebbero essere richiesti durante un controllo finanziario, oltre a comprendere una vasta gamma di controlli IT generali che tengono conto di una vasta gamma di scenari di utilizzo e di controllo. In questo modo i clienti hanno la possibilità di utilizzare l'infrastruttura AWS per archiviare ed elaborare dati critici, compresi quelli che costituiscono parte integrante del processo di rendicontazione finanziaria. AWS esegue periodicamente nuove valutazioni sull'insieme di tali controlli per tenere conto del feedback e dell'utilizzo da parte dei clienti di questo importante rapporto di controllo.

AWS si impegna costantemente per migliorare il rapporto SOC 1 e continuerà il processo di revisione periodica. L'ambito di applicazione del rapporto SOC 1 include:

- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- Amazon Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Identity and Access Management (IAM)

- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow (SWF)
- Amazon Simple Queue Service (SQS)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkSpaces

SOC 2

Oltre al rapporto SOC 1, AWS pubblica un rapporto Service Organization Controls 2 (SOC 2) di tipo II. Simile al rapporto SOC 1 nella valutazione dei controlli, il rapporto SOC 2 è un'attestazione che estende la valutazione dei controlli ai criteri stabiliti dai Trust Services Principles dell'American Institute of Certified Public Accountants (AICPA). Tali principi definiscono i controlli principali relativi a sicurezza, disponibilità, integrità di elaborazione, riservatezza e privacy applicabili alle organizzazioni di servizi come AWS. Il rapporto AWS SOC 2 è una valutazione dell'efficacia progettuale e operativa dei controlli che soddisfano i criteri dei principi di sicurezza e disponibilità definiti dai Trust Services Principles dell'AICPA. Questo rapporto offre una trasparenza ancora maggiore sulla sicurezza e sulla disponibilità di AWS in base a uno standard di settore predefinito di prassi principali e costituisce un'ulteriore dimostrazione dell'impegno di AWS nella tutela dei dati dei clienti. Il rapporto SOC 2 comprende gli stessi servizi inclusi nel rapporto SOC 1. Consultare la descrizione di SOC 1 sopra per informazioni sui servizi compresi nell'ambito di applicazione.

SOC 3

AWS pubblica un rapporto Service Organization Controls 3 (SOC 3). Il rapporto SOC 3 è una sintesi disponibile al pubblico del rapporto AWS SOC 2. Il rapporto comprende il parere dell'auditor esterno in merito al funzionamento dei controlli (sulla base dei Security Trust Principe AICPA inclusi nel rapporto SOC 2), la dichiarazione della direzione AWS circa l'efficacia dei controlli e una panoramica dell'infrastruttura e dei servizi AWS. Il rapporto AWS SOC 3 comprende tutti i data center AWS a livello mondiale che supportano i servizi compresi nell'ambito di applicazione. Si tratta di un'ottima risorsa per consentire ai clienti di confermare l'avvenuto conseguimento da parte di AWS della garanzia del revisore esterno, senza dover eseguire la procedura di richiesta di un rapporto SOC 2. Il rapporto SOC 3 comprende gli stessi servizi inclusi nel rapporto SOC 1. Consultare la descrizione di SOC 1 sopra per informazioni sui servizi compresi nell'ambito di applicazione. Vedere il rapporto AWS SOC 3 qui.

Approfondimenti

Per ulteriori informazioni, consultare le seguenti fonti:

- Panoramica su gestione dei rischi e conformità in AWS
- Risposte di AWS alle principali domande sulla conformità
- CAIQ (Consensus Assessments Initiative Questionnaire) della CSA

Revisioni del documento

Data	Descrizione
Gennaio 2017	Migrazione a un nuovo modello
Gennaio 2016	Prima pubblicazione