Unable to locate subtitle

Amazon Web Services: rischio e conformità

Amazon Web Services: rischio e conformità: ***Unable to locate subtitle***

Table of Contents

Amazon Web Services: rischio e conformità

Data di pubblicazione: 11 marzo 2021 (Revisioni del documento)

Riassunto

AWS serve una varietà di clienti, compresi quelli dei settori regolamentati. Attraverso il nostro modello di responsabilità condivisa, consentiamo ai clienti di gestire il rischio in modo efficace ed efficiente nell'ambiente IT e forniamo la garanzia di una gestione efficace del rischio attraverso la nostra conformità a framework e programmi consolidati e ampiamente riconosciuti. Questo documento delinea i meccanismi che AWS ha implementato per gestire il rischio a suo carico secondo il modello di responsabilità condivisa e gli strumenti che i clienti possono sfruttare per avere la certezza che questi meccanismi siano implementati in modo efficace.

Introduzione

AWS e i suoi clienti condividono il controllo sull'ambiente IT. Pertanto, la sicurezza è una responsabilità condivisa. Quando si tratta di gestire la sicurezza e la conformità in AWS Cloud, ciascuna parte ha responsabilità distinte. La responsabilità di un cliente dipende dai servizi che sta utilizzando. Tuttavia, in generale, i clienti sono responsabili della creazione del proprio ambiente IT in modo che sia in linea con i loro specifici requisiti di sicurezza e conformità.

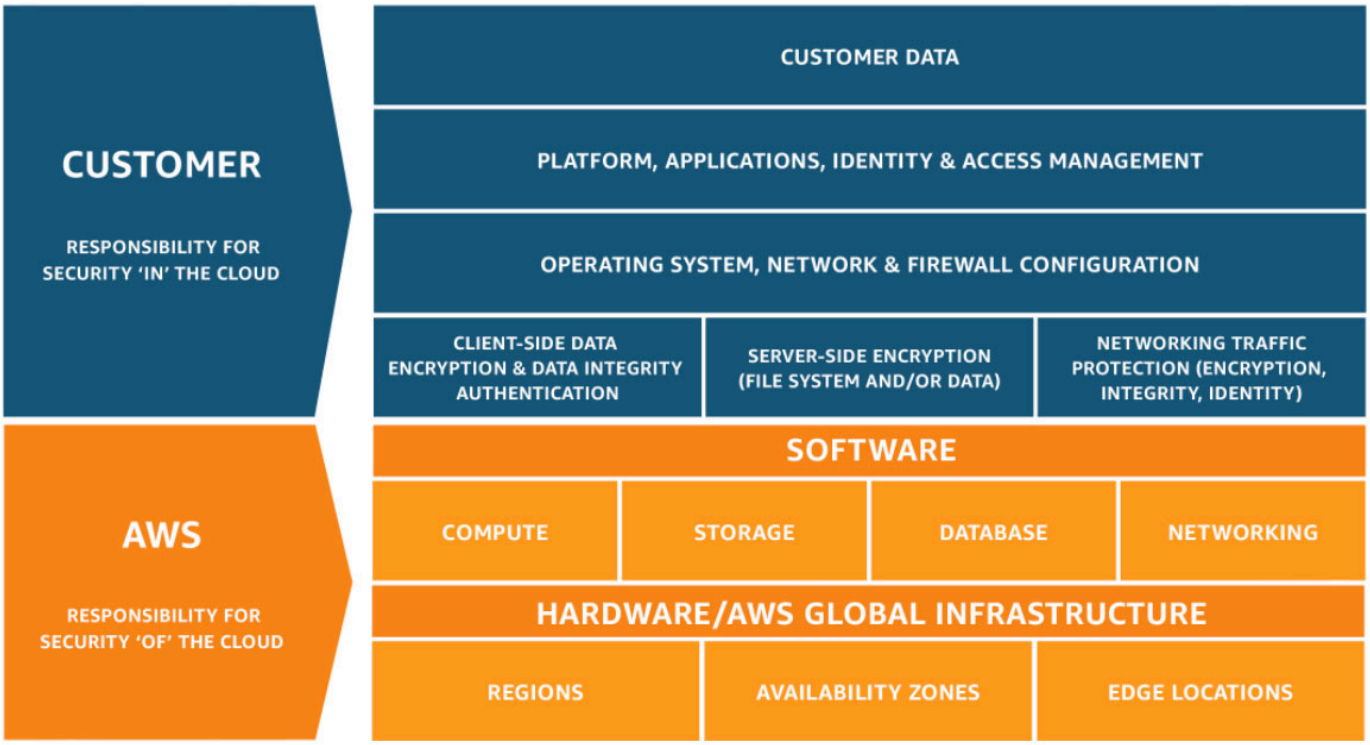
Questo documento fornisce ulteriori dettagli sulle responsabilità di sicurezza di ciascuna parte e sui modi in cui i clienti possono trarre vantaggio dal programma Rischio e conformità di AWS.

Modello di responsabilità condivisa

La sicurezza e la conformità sono una responsabilità condivisa tra AWS e il cliente. A seconda dei servizi implementati, questo modello condiviso può contribuire ad alleviare il carico operativo del cliente. Ciò accade perché AWS gestisce, amministra e controlla tutti i componenti, da sistema operativo host e livello di virtualizzazione, fino ai dispositivi per garantire la sicurezza fisica delle strutture in cui operano i servizi. Il cliente si assume la responsabilità della gestione del sistema operativo guest (con relativi aggiornamenti e patch di sicurezza), di altri software applicativi associati, oltre alla configurazione del firewall del gruppo di sicurezza fornito da AWS.

Consigliamo ai clienti di valutare con attenzione i servizi scelti, dato che le loro responsabilità variano in base ai servizi utilizzati, all'integrazione di tali servizi nel loro ambiente IT e alle leggi e ai regolamenti applicabili. I clienti hanno la possibilità di rafforzare la sicurezza e/o di soddisfare requisiti più rigorosi in materia di conformità utilizzando tecnologie come firewall basati su host, rilevamento/prevenzione di intrusioni basati su host, crittografia e gestione delle chiavi.

La natura della responsabilità condivisa, inoltre, offre al cliente flessibilità e controllo, che a loro volta consentono l'implementazione di soluzioni in grado di soddisfare i requisiti di certificazione specifici del settore.



Questo modello di responsabilità condivisa cliente/AWS si estende anche ai controlli IT. Proprio come avviene con la condivisione della responsabilità di gestione dell'ambiente IT tra AWS ed i suoi clienti, sono oggetto di responsabilità condivisa anche la gestione, il funzionamento e la verifica dei controlli IT. AWS può aiutare i clienti gestendo i controlli associati all'infrastruttura fisica implementata nell'ambiente AWS. I clienti possono quindi usare la documentazione sulla conformità e il controllo AWS di cui dispongono per eseguire le procedure di valutazione e verifica come richiesto. Per gli esempi di come la responsabilità di determinati controlli è condivisa tra AWS e i suoi clienti, consulta il Modello di responsabilità condivisa AWS.

Valutazione e integrazione dei controlli AWS

AWS fornisce ai clienti una vasta gamma di informazioni sull'ambiente di controllo IT tramite documenti tecnici, report, certificazioni e altre attestazioni di terze parti. Tale documentazione è utile ai clienti per capire quali sono i controlli esistenti e pertinenti ai fini dei servizi AWS utilizzati e come tali controlli sono stati convalidati. Queste informazioni, inoltre, permettono ai clienti di tenere conto e di verificare che i controlli nel loro ambiente IT esteso funzionino in modo efficace.

Generalmente, l'efficacia progettuale e operativa degli obiettivi di controllo è convalidata da revisori interni e/o esterni tramite valutazioni dettagliate del processo e dei riscontri. Questo tipo di osservazione/verifica diretta da parte del cliente o dei revisori esterni interpellati dal cliente rappresenta una procedura tipica per convalidare i controlli nelle classiche implementazioni On-Premise.

Nel caso in cui vengano utilizzati fornitori di servizi (come AWS), i clienti possono richiedere e valutare attestati e certificazioni di terze parti. Queste attestazioni e certificazioni possono aiutare a garantire al cliente la progettazione e l'efficacia operativa degli obiettivi di controllo e dei controlli convalidati da una terza parte qualificata e indipendente. Di conseguenza, sebbene alcuni controlli possano essere gestiti da AWS, l'ambiente di controllo può ancora essere un framework unificato di cui i clienti possono tenere conto e verificare che i controlli stiano funzionando in modo efficace, accelerando al contempo il processo di revisione della conformità.

Le attestazioni e le certificazioni di AWS di terze parti forniscono ai clienti visibilità e convalida indipendente dell'ambiente di controllo. Tali attestazioni e certificazioni possono aiutare a sollevare i clienti dall'obbligo di eseguire autonomamente determinati lavori di convalida per il loro ambiente IT in AWS Cloud.

Programma Rischio e conformità AWS

AWS ha integrato un programma di rischio e conformità in tutta l'organizzazione, che mira a gestire il rischio in tutte le fasi di progettazione e implementazione del servizio, oltre a migliorare e rivalutare continuamente le attività legate al rischio dell'organizzazione. I componenti del programma integrato di rischio e conformità AWS sono trattati in maggior dettaglio nelle sezioni seguenti.

Gestione del rischio aziendale AWS

AWS ha predisposto un programma di gestione del rischio aziendale (BRM) destinato ai reparti aziendali di AWS per fornire al consiglio di amministrazione e ai senior leader di AWS una visione olistica dei principali rischi in AWS. Il programma BRM dimostra una supervisione indipendente del rischio sulle funzioni AWS. In particolare, il programma BRM si occupa di quanto segue:

- Esegue valutazioni e monitoraggio del rischio delle principali aree funzionali di AWS
- Identifica e promuove la correzione dei rischi
- Mantiene un registro dei rischi noti

Per guidare la correzione dei rischi, il programma BRM riporta i risultati dei suoi sforzi e, se necessario, segnala i problemi ai direttori e ai vicepresidenti di tutta l'azienda per informare il processo decisionale aziendale.

Gestione operativa e aziendale

AWS utilizza una combinazione di riunioni e report settimanali, mensili e trimestrali per garantire, tra l'altro, la comunicazione del rischio tra tutti i componenti del processo di gestione del rischio. Inoltre, AWS implementa un processo di escalation per fornire visibilità alla gestione dei rischi ad alta priorità in tutta l'organizzazione. Questi sforzi, tutti insieme, contribuiscono a garantire che il rischio sia gestito in modo coerente con la complessità del modello di business di AWS.

Inoltre, attraverso una struttura di responsabilità a cascata, i vicepresidenti (i proprietari dell'azienda) sono responsabili della supervisione della loro attività. A tal fine, AWS organizza riunioni settimanali per esaminare i parametri operativi e identificare tendenze e rischi chiave prima che abbiano un impatto sull'azienda.

Le leadership esecutiva e di livello senior giocano ruoli importanti nello stabilire i toni di AWS e i suoi valori fondamentali. Ogni dipendente riceve il Codice di condotta aziendale ed etica e i dipendenti

completano una formazione periodica. Le verifiche di conformità sono eseguite in modo che i dipendenti comprendano e seguano le policy stabilite.

La struttura organizzativa di AWS offre un framework per la pianificazione, l'esecuzione e il controllo delle operazioni aziendali. La struttura organizzativa comprende ruoli e responsabilità in modo tale da disporre di personale adeguato, favorire l'efficienza delle operazioni e ottenere la segregazione dei compiti. La direzione, inoltre, ha definito le linee opportune per il personale più importante. Le verifiche condotte dall'azienda durante la procedura di assunzione prevedono la convalida dell'istruzione, degli impieghi precedenti e, in alcuni casi, dei precedenti penali, nei limiti di quanto ammesso dalle leggi e dai regolamenti in materia e in modo commisurato alla posizione del dipendente e al suo livello di accesso alle strutture AWS. L'azienda segue una procedura di formazione iniziale strutturata che consente ai nuovi dipendenti di acquisire familiarità con strumenti, processi, sistemi, policy e procedure Amazon.

Ambiente di controllo e automazione

AWS implementa i controlli di sicurezza come elemento fondamentale per gestire il rischio in tutta l'organizzazione. L'ambiente di controllo AWS è composto da standard, processi e strutture che forniscono la base per l'implementazione di una serie minima di requisiti di sicurezza in AWS.

Sebbene i processi e gli standard inclusi nell'ambiente di controllo AWS siano autonomi, AWS sfrutta anche aspetti dell'ambiente di controllo di Amazon in generale. Gli strumenti impiegati comprendono:

- Strumenti utilizzati in tutte le attività Amazon, ad esempio quello che gestisce la separazione delle attività
- Alcune funzioni aziendali a livello di Amazon, come quelle legali, delle risorse umane e finanziarie

Nelle istanze in cui AWS sfrutta l'ambiente di controllo generale di Amazon, gli standard e i processi che governano questi meccanismi sono personalizzati specificamente per il business AWS. Ciò significa che le aspettative per il loro uso e applicazione all'interno dell'ambiente di controllo AWS possono differire dalle aspettative per il loro uso e applicazione all'interno dell'ambiente Amazon in generale. L'ambiente di controllo AWS funge da base per fornire in modo sicuro le offerte dei servizi AWS.

L'automazione del controllo è un modo per AWS di ridurre l'intervento umano in alcuni processi ricorrenti che comprendono l'ambiente di controllo AWS. È fondamentale per un'efficace implementazione del controllo della sicurezza delle informazioni e per la gestione dei rischi associata. L'automazione del controllo cerca di ridurre in modo proattivo le potenziali incongruenze

nell'esecuzione del processo che potrebbero insorgere a causa della natura imperfetta degli esseri umani che conducono un processo ripetitivo. Attraverso l'automazione del controllo, le potenziali deviazioni dal processo vengono eliminate. Ciò fornisce maggiori livelli di garanzia che il controllo verrà applicato come previsto.

I team di progettazione di AWS in tutte le funzioni di sicurezza sono responsabili della progettazione dell'ambiente di controllo AWS per supportare maggiori livelli di automazione del controllo, ove possibile. Esempi di controlli automatici in AWS includono:

- Governance e supervisione: controllo delle versioni e approvazione delle policy
- Gestione del personale: erogazione automatizzata della formazione, licenziamento rapido dei dipendenti
- Gestione dello sviluppo e della configurazione: pipeline di implementazione del codice, scansione del codice, backup del codice, test di implementazione integrati
- Gestione di identità e accesso: segregazione automatizzata dei compiti, revisioni degli accessi, gestione delle autorizzazioni
- Monitoraggio e registrazione: raccolta e correlazione dei registri automatizzate, allarmi
- Sicurezza fisica: processi automatizzati relativi ai data center AWS, tra cui gestione dell'hardware, formazione sulla sicurezza dei data center, allarmi di accesso e gestione degli accessi fisici
- Scansione e gestione delle patch: scansione automatizzata delle vulnerabilità, gestione e implementazione delle patch

Valutazione dei controlli e monitoraggio continuo

AWS implementa una serie di attività prima e dopo l'implementazione del servizio per ridurre ulteriormente il rischio all'interno dell'ambiente AWS. Queste attività integrano i requisiti di sicurezza e conformità durante la progettazione e lo sviluppo di ciascun servizio AWS e quindi convalidano che i servizi funzionino in modo sicuro dopo che sono stati trasferiti in produzione (avviati).

Le attività di gestione del rischio e della conformità comprendono due attività precedenti all'avvio e due attività successive all'avvio. Le attività precedenti all'avvio sono:

- Revisione della gestione del rischio di sicurezza dell'applicazione AWS per verificare che i rischi per la sicurezza siano stati identificati e attenuati
- Revisione della fattibilità dell'architettura per aiutare i clienti a garantire l'allineamento con i regimi di conformità

Al momento della sua implementazione, un servizio sarà stato sottoposto a rigorose valutazioni secondo requisiti di sicurezza dettagliati per soddisfare l'elevato livello di sicurezza di AWS. Le attività successive all'avvio sono:

- Revisione continua della sicurezza delle applicazioni AWS per garantire il mantenimento della posizione di sicurezza del servizio
- Analisi continua della gestione delle vulnerabilità

Queste valutazioni di controllo e il monitoraggio continuo permettono ai clienti regolamentati di creare con sicurezza soluzioni conformi sui servizi AWS. Per un elenco di servizi nell'ambito dei vari programmi di conformità, consulta la pagina Web Servizi AWS coperti dal programma di compliance.

Certificazioni AWS, programmi, rapporti e attestazioni di terze parti

AWS viene regolarmente sottoposto a verifiche di attestazione indipendenti di terze parti per garantire che le attività di controllo funzionino come previsto. Più specificamente, AWS è sottoposto a una verifica in base a una varietà di framework di sicurezza globali e regionali che dipendono dalla regione e dal settore. AWS partecipa a oltre 50 diversi programmi di verifica.

I risultati di queste verifiche sono documentati dall'ente di valutazione e resi disponibili per tutti i clienti AWS tramite AWS Artifact. AWS Artifact è un portale self-service gratuito per l'accesso on demand ai report di conformità di AWS. Quando vengono rilasciati nuovi report, questi vengono resi disponibili in AWS Artifact, permettendo ai clienti di monitorare continuamente la sicurezza e la conformità di AWS con accesso immediato a nuovi report.

A seconda dei requisiti normativi o contrattuali locali di un paese o settore, AWS può anche sottoporsi a verifiche direttamente con clienti o revisori governativi. Queste verifiche forniscono una supervisione aggiuntiva dell'ambiente di controllo AWS per garantire che i clienti dispongano degli strumenti necessari per operare in modo sicuro, conforme e basato sul rischio utilizzando i servizi AWS.

Per informazioni più dettagliate sui programmi di certificazione AWS, i report e gli attestati di terze parti, visita la pagina web del Programmi per la conformità di AWS. Puoi anche visitare la pagina Web di Servizi AWS coperti dal programma di compliance per informazioni specifiche sui servizi.

Cloud Security Alliance

AWS partecipa all'autovalutazione volontaria Cloud Security Alliance (CSA), Trust & Assurance Registry (STAR) per documentare la conformità alle best practice pubblicate da CSA. CSA è "l'organizzazione leader a livello mondiale dedicata alla definizione e alla sensibilizzazione delle best practice per contribuire a garantire un ambiente di cloud computing sicuro". Il Questionario dell'Iniziativa di valutazione del consenso di Cloud Security Alliance (CSA) (CAIQ) fornisce una serie di domande che CSA prevede che un cliente cloud e/o un revisore cloud chiedano a un fornitore di servizi cloud. Riporta una serie di domande relative a sicurezza, controlli e processi che si prestano a una vasta gamma di utilizzi, compresa la scelta del fornitore di servizi cloud e la valutazione della sicurezza.

Sono disponibili due risorse per i clienti che documentano l'allineamento di AWS al CSA CAIQ. Il primo è il whitepaper CSA CAIQ, mentre il secondo è una mappatura più dettagliata dei controlli SOC-2, disponibile tramite AWS Artifact. Per ulteriori informazioni sulla partecipazione di AWS a CSA CAIQ, consulta il sito AWS CSA.

Governance della conformità cloud del cliente

I clienti AWS hanno la responsabilità di mantenere una governance adeguata sull'intero ambiente di controllo IT, indipendentemente da come e dove viene implementato l'IT. Le pratiche principali includono:

- Comprendere i requisiti e gli obiettivi di conformità richiesti (da fonti pertinenti)
- Stabilire un ambiente di controllo che soddisfi questi obiettivi e requisiti
- Comprendere le convalide richieste, in base alla tolleranza del rischio dell'organizzazione
- Verifica dell'efficacia operativa del loro ambiente di controllo

L'implementazione in AWS Cloud offre alle aziende numerose opzioni per l'applicazione di vari tipi di controlli e diversi metodi di verifica.

Una solida governance e conformità da parte del cliente potrebbe includere il seguente approccio di base:

1. Revisione del Modello di responsabilità condivisa AWS, della documentazione della sicurezza di AWS, dei report di conformità AWS e di altre informazioni disponibili su AWS, insieme ad altra documentazione specifica per il cliente. Prova a comprendere quanto più possibile dell'ambiente IT nel suo complesso e successivamente a documentare tutti i requisiti di conformità in un framework completo per il controllo del cloud.
2. Progettazione e implementazione di obiettivi di controllo per soddisfare i requisiti di conformità aziendale come stabilito nel Modello di responsabilità condivisa AWS.
3. Identificare e documentare i controlli di proprietà di soggetti esterni.
4. Verificare che tutti gli obiettivi di controllo siano soddisfatti e che tutti i controlli principali siano stati definiti e funzionino in modo efficace.

L'adozione di tale approccio alla governance della conformità aiuta i clienti a comprendere meglio il proprio ambiente di controllo e a definire chiaramente le attività di verifica da eseguire.

Conclusione

Fornire infrastrutture e servizi altamente sicuri e resilienti ai nostri clienti è una priorità assoluta per AWS. Il nostro impegno nei confronti dei nostri clienti si concentra sul lavoro per guadagnare continuamente la loro fiducia e garantire che la mantengano nel gestire i loro carichi di lavoro in sicurezza su AWS. Per raggiungere questo obiettivo, AWS ha integrato meccanismi di rischio e conformità che includono:

- L'implementazione di una vasta gamma di controlli di sicurezza e strumenti automatizzati
- Il monitoraggio e la valutazione continui dei controlli di sicurezza per garantire l'efficacia operativa di AWS e il rispetto rigoroso dei regimi di conformità
- La valutazione indipendente del rischio da parte del programma di gestione del rischio aziendale di AWS
- Meccanismi operativi e di gestione aziendale

Inoltre, AWS viene regolarmente sottoposto a verifiche indipendenti di terze parti per garantire che le attività di controllo funzionino come previsto. Queste verifiche, insieme alle numerose certificazioni ottenute da AWS, forniscono un ulteriore livello di convalida dell'ambiente di controllo AWS a vantaggio dei clienti.

Insieme ai controlli di sicurezza gestiti dai clienti, questi sforzi permettono ad AWS di innovare in modo sicuro per conto dei clienti e aiutarli a migliorare la posizione di sicurezza durante la costruzione su AWS.

Collaboratori

I collaboratori di questo documento includono:

- Marta Taggart, Senior Program Manager, AWS Security
- Bradley Roach, Risk Manager, AWS Business Risk Management
- Patrick Woods, Senior Security Specialist, AWS Security

Approfondimenti

AWS fornisce ai clienti informazioni relative al suo ambiente di sicurezza e controllo secondo queste modalità:

- Ottenere e mantenere le certificazioni di settore e le attestazioni di terze parti indipendenti elencate nella pagina del Programma per la conformità di AWS.
- Pubblicazione continuativa delle informazioni relative alle prassi di sicurezza e controllo di AWS in whitepaper e contenuti Web, come il Blog di AWS sulla sicurezza.
- Fornire descrizioni approfondite su come AWS utilizza l'automazione su vasta scala per gestire la nostra infrastruttura di servizi nella AWS Builders Library.
- Migliorare la trasparenza fornendo certificati di conformità, report e altra documentazione direttamente ai clienti AWS tramite il portale self-service noto come AWS Artifact.
- Fornire risorse per la conformità di AWS e documentare e pubblicare costantemente le risposte alle domande sulla pagina Web delle Domande frequenti sulla conformità di AWS.
- I clienti possono seguire i principi di progettazione in AWS Well-Architected Framework per una guida su come affrontare la configurazione di tutti i carichi di lavoro basati su AWS.

Revisioni del documento

Per ricevere una notifica sugli aggiornamenti di questo whitepaper, iscriviti al feed RSS.

update-history-change	update-history-description	update-history-date
Aggiornamenti minori	Rivisto per l'accuratezza tecnica	10 marzo 2021
Whitepaper aggiornato	Questa versione include modifiche sostanziali che includono la rimozione delle informazioni di riferimento sui programmi e sugli schemi di conformità, poiché queste informazioni sono disponibili nelle pagine Web dei Programmi per la conformità di AWS e dei Servizi AWS coperti dal programma di conformità. Inoltre, abbiamo rimosso la sezione relativa alle domande di conformità più comuni perché tali informazioni sono ora disponibili nella pagina Web delle Domande frequenti sulla conformità di AWS.	1 novembre 2020
Pubblicazione iniziale	Pubblicato il whitepaper Amazon Web Services: rischio e conformità	1 maggio 2011

Avvisi

I clienti sono responsabili della propria valutazione autonoma delle informazioni contenute in questo documento. Questo documento: (a) è solo a scopo informativo, (b) mostra le offerte e le pratiche attuali dei prodotti AWS soggette a modifiche senza preavviso, e (c) non crea alcun impegno o garanzia da parte di AWS e dei suoi affiliati, fornitori o licenziatari. I prodotti o servizi AWS sono forniti "così come sono" senza garanzie, dichiarazioni o condizioni di alcun tipo, sia esplicite che implicite. Le responsabilità e gli obblighi di AWS verso i propri clienti sono disciplinati dagli accordi AWS e il presente documento non fa parte né modifica alcun accordo tra AWS e i suoi clienti.