# Panoramica su gestione dei rischi e conformità in AWS

*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

Questo documento fornisce informazioni per aiutare i clienti a integrare AWS nel framework di controllo esistente, con un approccio di base per la valutazione dei controlli AWS.

# Introduzione

AWS e i suoi clienti condividono il controllo sull'ambiente IT. La parte di AWS di tale responsabilità condivisa include l'erogazione di servizi su una piattaforma estremamente sicura e controllata e la fornitura di una vasta gamma di caratteristiche di sicurezza che i clienti possono utilizzare. I clienti sono responsabili della configurazione degli ambienti IT in una modalità sicura e controllata rispetto ai loro scopi. Mentre i clienti non comunicano modalità di utilizzo e configurazioni ad AWS, quest'ultima comunica ai clienti le informazioni relative al proprio ambiente di sicurezza e controllo che li riguardano. La procedura seguita a tale scopo da AWS è la seguente:

- Conseguimento delle certificazioni di settore e delle attestazioni di terze parti indipendenti descritte nel presente documento.
- Pubblicazione delle informazioni relative alle prassi di sicurezza e controllo di AWS in whitepaper e contenuti Web.
- Fornitura di certificati, rapporti e altri documenti direttamente ai clienti AWS ai sensi dell'accordo di riservatezza (come prescritto).

Per una descrizione più dettagliata della sicurezza di AWS, consultare il Centro di Sicurezza AWS.

Per una descrizione più dettagliata della conformità di AWS, consultare la pagina sulla conformità di AWS.

Il whitepaper AWS Overview of Security Processes (Panoramica sulle procedure di sicurezza AWS) illustra inoltre i controlli di sicurezza generali di AWS e le misure di sicurezza previste specificamente per i servizi.

## Shared Responsibility Environment

La transizione dell'infrastruttura IT ai servizi AWS crea un modello di Shared Responsibility tra il cliente e AWS. Tale modello condiviso può contribuire a ridurre l'onere operativo del cliente, dato che AWS rende operativi, gestisce e controlla tutti i componenti, dal sistema operativo host al layer di virtualizzazione fino alla 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), dell'altro software applicativo associato e della configurazione del security group firewall fornito da AWS. I clienti devono 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. Tale Shared Responsibility, inoltre, offre al cliente flessibilità e controllo, che a loro volta consentono la distribuzione di soluzioni in grado di soddisfare i requisiti di certificazione specifici del settore.

Questo modello di shared responsibility 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 condivisi anche la gestione, il funzionamento e la verifica dei controlli IT. AWS può aiutare il cliente a ridurre l'ammontare dei controlli operativi attraverso la gestione dei controlli dell'infrastruttura fisica di AWS, controlli che in precedenza erano completamente a carico del cliente. Poiché ogni cliente in AWS ha una diversa distribuzione, i clienti possono trarre vantaggio dal trasferimento della gestione di alcuni controlli IT ad AWS e ottenere un (nuovo) ambiente di controllo distribuito. I clienti possono quindi utilizzare la documentazione AWS su controllo e conformità a loro disposizione (descritta nella sezione Certificazioni AWS e attestazioni di terze parti) per eseguire le proprie procedure di valutazione e verifica dei controlli, come prescritto.

## Solida governance della conformità

I clienti AWS sono sempre tenuti a mantenere una governance adeguata sull'intero ambiente di controllo IT, indipendentemente dalla modalità di distribuzione di tale ambiente. Tra le principali prassi adottate si possono menzionare la comprensione degli obiettivi e dei requisiti in termini di conformità (utilizzando fonti pertinenti), la definizione di un ambiente di controllo che soddisfi tali obiettivi e requisiti, la comprensione della convalida richiesta in base alla tolleranza al rischio dell'organizzazione e la verifica dell'efficacia operativa dell'ambiente di controllo. La distribuzione nel cloud AWS offre alle imprese numerose opzioni per l'applicazione dei vari tipi di controlli e dei diversi metodi di verifica.

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

1. Esaminare le informazioni messe a disposizione da AWS insieme ad altre informazioni, per capire quanto più possibile dell'ambiente IT nel suo complesso e successivamente documentare tutti i requisiti di conformità.
2. Definire ed implementare gli obiettivi di controllo che soddisfino i requisiti aziendali in materia di conformità.
3. Identificare e documentare i controlli gestiti da 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 le aziende a comprendere meglio il proprio ambiente di controllo e a definire chiaramente le attività di verifica da eseguire.

# Valutazione e integrazione dei controlli AWS

AWS fornisce ai clienti una vasta gamma di informazioni sull'ambiente di controllo IT, tramite whitepaper, documenti, 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. Le informazioni, inoltre, aiutano i clienti a verificare e confermare che i controlli presenti nel loro ambiente IT esteso funzionino in modo efficace.

Generalmente, l'efficacia progettuale e operativa degli obiettivi di controllo e dei controlli è convalidata da revisori interni e/o esterni tramite valutazioni dettagliate del processo e dei riscontri. L'osservazione/verifica diretta da parte del cliente o dei revisori esterni interpellati dal cliente rappresenta una procedura tipica per convalidare i controlli. Nel caso in cui si avvalgano di fornitori di servizi, come AWS, le aziende richiedono e tengono in considerazione attestati e certificazioni rilasciati da terze parti per avere la garanzia dell'efficacia progettuale e operativa degli obiettivi di controllo e dei controlli. Di conseguenza, sebbene i principali controlli dei clienti potrebbero essere gestiti da AWS, l'ambiente di controllo può comunque rimanere un framework unificata in cui tutti i controlli sono gestiti e verificati in maniera efficace. Gli attestati e le certificazioni rilasciati da terze parti sui servizi di AWS non solo offrono un livello di convalida più alto dell'ambiente di controllo, ma possono liberare i clienti dall'onere di eseguire alcune procedure di convalida per il loro ambiente IT nel cloud AWS.

# Informazioni sui controlli IT AWS

AWS fornisce informazioni sui controlli IT ai clienti secondo queste modalità:

**Definizione del controllo specifico.** I clienti AWS possono identificare i principali controlli gestiti da AWS. I controlli principali sono essenziali per l'ambiente di controllo dei clienti e richiedono un'attestazione esterna sulla loro efficacia operativa in modo da soddisfare i requisiti di conformità, come ad esempio quelli del controllo finanziario annuale. A questo scopo, AWS pubblica un'ampia gamma di controlli IT specifici all'interno del rapporto Service Organization Controls 1 (SOC 1) di tipo II. Il rapporto SOC 1, ex Statement on Auditing Standards (SAS) No. 70, rapporto Service Organizations, è uno standard di auditing ampiamente riconosciuto sviluppato dall'American Institute of Certified Public Accountants (AICPA). Il SOC 1 è un tipo di controllo che verifica approfonditamente l'efficacia progettuale e operativa degli obiettivi di controllo definiti e delle attività di controllo di AWS (che includono gli obiettivi di controllo e le attività di controllo della parte dell'infrastruttura gestita da AWS). "Type II" fa riferimento al fatto che ciascun controllo descritto all'interno del rapporto non viene soltanto valutato ai fini dell'adeguatezza progettuale, ma anche testato dal punto di vista dell'efficacia operativa dal revisore esterno. Tenuto conto dell'indipendenza e della competenza del revisore esterno di AWS, i controlli identificati nel rapporto offrono ai clienti un alto livello di sicurezza riguardo all'ambiente di controllo di AWS. I controlli operati da AWS possono essere considerati efficaci dal punto di vista progettuale e operativo in riferimento a numerose necessità di conformità, tra cui la revisione dei bilanci secondo la Sarbanes-Oxley (SOX) Section 404. L'uso dei rapporti SOC 1 di tipo II viene di solito consentito da altri organi di certificazione esterna (ad esempio i revisori ISO 27001 possono richiedere un rapporto SOC 1 di tipo II per completare le valutazioni da presentare ai clienti).

Altri controlli specifici sono quelli relativi alla conformità di AWS con la Payment Card Industry (PCI) e con il Federal Information Security Management Act (FISMA). AWS è conforme agli standard FISMA Moderate e allo standard PCI Data Security. Gli standard PCI e FISMA sono molto prescrittivi e richiedono una convalida indipendente che attesti l'aderenza di AWS allo standard pubblicato.

**Conformità allo standard di controllo generale.** Nel caso in cui un cliente AWS richieda che venga soddisfatta un'ampia gamma di obiettivi di controllo, si potrebbe procedere a una valutazione delle certificazioni di settore di AWS. Grazie alla certificazione AWS ISO 27001, AWS soddisfa uno standard di sicurezza ampio e completo e segue le best practice per il mantenimento di un ambiente sicuro. Con lo standard PCI Data Security (PCI DSS), AWS soddisfa una serie di controlli importanti per le aziende che gestiscono informazioni sulle carte di credito. Con gli standard FISMA, AWS soddisfa un'ampia gamma di controlli specifici richiesti dalle agenzie governative degli Stati Uniti. La conformità a questi standard generali offre ai clienti informazioni approfondite sulla completezza dei controlli e dei processi di sicurezza adottati e può essere tenuta in considerazione durante la gestione della conformità.

## AWS Global Regions

I data center sono costruiti in cluster in diverse regioni globali, tra cui: Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), AWS GovCloud (US) (Oregon), UE (Francoforte), UE (Irlanda), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Tokyo), Asia Pacifico (Sydney), Cina (Pechino) e Sud America (San Paolo).

Per un elenco completo delle regioni, consultare la pagina Infrastruttura globale di AWS.

# Programma Risk and Compliance di AWS

AWS fornisce informazioni sul suo programma di gestione del rischio e di conformità in modo da consentire ai clienti di integrare i controlli AWS nel loro framework di governance. Queste informazioni possono aiutare i clienti a documentare un framework di controllo e governance completo in cui AWS ricopre un ruolo importante.

# Gestione del rischio

La direzione di AWS ha sviluppato un piano aziendale strategico che include l'identificazione del rischio e l'implementazione di controlli che limitano o gestiscono i rischi. La direzione di AWS rivaluta il piano aziendale strategico almeno ogni due anni. Questo processo richiede che la direzione identifichi i rischi che rientrano nelle sue aree di responsabilità e che implementi le misure adeguate progettate per affrontare tali rischi.

Inoltre, l'ambiente di controllo AWS è soggetto a diverse valutazioni del rischio sia interne sia esterne. I team AWS che si occupano di conformità e sicurezza hanno stabilito un framework e policy di sicurezza delle informazioni basati sul modello COBIT (Control Objectives for Information and related Technology) e hanno integrato in modo efficace il framework certificabile ISO 27001 sulla base dei controlli ISO 27002, dei criteri Trust Services Principles dell'AICPA (American Institute of Certified Public Accountants), del PCI DSS v3.1 e della pubblicazione 800-53 Rev 3 del NIST (National Institute of Standards and Technology), Recommended Security Controls for Federal Information Systems. AWS gestisce la policy di sicurezza, si occupa della formazione dei dipendenti in materia di sicurezza ed effettua verifiche sulla sicurezza dell'applicazione. Tali verifiche valutano la riservatezza, l'integrità e la disponibilità dei dati, oltre alla conformità alla policy di sicurezza delle informazioni.

AWS Security esegue scansioni regolari di tutti gli indirizzi IP dell'endpoint del servizio connessi a Internet per individuare le vulnerabilità (tali scansioni non includono le istanze dei clienti). AWS Security notifica alle parti interessate le eventuali vulnerabilità identificate a cui è necessario porre rimedio. Vengono inoltre eseguite valutazioni di vulnerabilità alle minacce esterne da parte di società indipendenti operanti nel settore della sicurezza. I risultati di tali valutazioni e le relative raccomandazioni sono categorizzati e forniti alla direzione di AWS. Le scansioni sono effettuate in modo da valutare l'integrità e l'adeguatezza dell'infrastruttura AWS sottostante e non hanno lo scopo di sostituire le scansioni di vulnerabilità che il cliente deve eseguire per soddisfare gli specifici obblighi di conformità che gli competono. I clienti possono chiedere l'autorizzazione a eseguire scansioni della propria infrastruttura cloud, purché i controlli siano limitati alle istanze del cliente e non violino l'Acceptable Use Policy (policy di utilizzo accettabile) di AWS. Per ottenere la preventiva autorizzazione per questo tipo di scansioni, è necessario inviare una richiesta utilizzando il modulo di richiesta per il test di vulnerabilità/intrusione di AWS.

# Ambiente di controllo

AWS gestisce un ambiente di controllo completo che include policy, processi e attività di controllo che si avvalgono di vari elementi dell'ambiente di controllo globale di Amazon. Questo ambiente di controllo esiste per garantire l'erogazione sicura dei servizi offerti da AWS. L'ambiente di controllo collettivo comprende le persone, i processi e la tecnologia necessari a definire e gestire un ambiente che supporti l'efficacia operativa del framework di controllo di AWS. AWS ha integrato nel proprio framework di controllo i controlli specifici applicabili al cloud computing identificati dai più importanti organismi di settore. AWS continua a monitorare tali gruppi di settore per comprendere quali prassi principali si possano adottare per aiutare al meglio i clienti a gestire l'ambiente di controllo.

In Amazon l'ambiente di controllo inizia al più alto livello dell'azienda. I dirigenti e l'alta dirigenza svolgono un ruolo importante nella definizione dei principi e dei valori seguiti dall'azienda. Ogni dipendente riceve il Codice di condotta aziendale ed etica e completa una formazione periodica. Vengono effettuati controlli in materia di conformità affinché i dipendenti comprendano e seguano le policy definite.

La struttura organizzativa di AWS offre un framework per la pianificazione, l'esecuzione e il controllo delle operazioni aziendali. La struttura organizzativa assegna ruoli e responsabilità in modo tale da disporre di personale adeguato, favorire l'efficienza delle operazioni e ottenere la separazione dei compiti. La direzione, inoltre, ha definito i livelli di autorità e le linee gerarchiche opportune per il personale più importante. Le verifiche condotte dall'azienda durante la procedura di assunzione prevedono controlli sull'istruzione, sui posti di lavoro precedenti e, in alcuni casi, sui 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 gli strumenti, i processi, i sistemi, le policy e le procedure Amazon.

## Sicurezza delle informazioni

AWS ha implementato un programma formale per la sicurezza delle informazioni pensato per proteggere la riservatezza, l'integrità e la disponibilità dei sistemi e dei dati dei clienti. AWS pubblica un whitepaper sulla sicurezza, disponibile nel sito Web pubblico, che illustra come AWS può aiutare i clienti a rendere sicuri i propri dati.

# Contatto AWS

I clienti possono richiedere i rapporti e le certificazioni elaborati dagli auditor di terze parti oppure maggiori informazioni circa la conformità di AWS contattando l'ufficio commerciale e di sviluppo aziendale AWS. Il rappresentante indirizzerà i clienti verso il team competente, in base alla natura della richiesta di informazioni. Per ulteriori informazioni sulla conformità di AWS, consultare il sito dedicato alla conformità di AWS o inviare le domande direttamente a mailto:awscompliance@amazon.com.

# Approfondimenti

Per ulteriori informazioni, consultare le seguenti fonti:

- CAIQ (Consensus Assessments Initiative Questionnaire) della CSA
- Certificazioni AWS, programmi, rapporti e attestazioni di terze parti
- Risposte di AWS alle principali domande sulla conformità

# Revisioni del documento

| Data | Descrizione |
|---|---|
| **Gennaio 2017** | Eseguire la migrazione a un nuovo modello |
| **Gennaio 2016** | Prima pubblicazione |