# SHARED RESPONSIBILITY MODEL

| REDAZIONE | CONTROLLO | APPROVAZIONE |
|---|---|---|
| Qualità | IT Manager | Responsabile SGSI |

## Classificazione del documento

| Tipo | Descrizione | Flag |
|---|---|---|
| **Pubblico (Public)** | Un documento **pubblico** può essere modificato solamente da chi ha completato l'iter di redazione, controllo e approvazione, è primariamente destinato ai componenti la lista di distribuzione ma può essere visualizzato da tutti all'interno dell'organizzazione. Può essere divulgato al di fuori dell'organizzazione, ma solo previa autorizzazione dell'Approvatore. | **X** |
| **Interno (Confidential)** | Un documento **interno** può essere modificato solamente da chi ha completato l'iter di redazione, controllo e approvazione, è primariamente destinato ai componenti la lista di distribuzione ma può essere visualizzato da tutti all'interno dell'organizzazione. Non può essere divulgato al di fuori dell'organizzazione. | |
| **Riservato (Restricted)** | Un documento **riservato** può essere modificato solamente da chi ha completato l'iter di redazione, controllo e approvazione, ed è destinato unicamente ai componenti la lista di distribuzione. Non può essere divulgato al di fuori della lista di distribuzione. | |

**Stato del documento**

| Data | Edizione | Descrizione |
|---|---|---|
| 31/08/2023 | 1.0 | Prima emissione |
| 27/02/2024 | 1.1 | Revisione del Documento |
| | | |

# Indice

# 1. Introduzione

Il presente documento descrive e regolamenta la responsabilità condivisa tra il Cloud Service Provider, Amazon Web Services, ACCA software ed il Cliente finale.

Il concetto di "modello di responsabilità condivisa" nel cloud computing si riferisce alla divisione delle responsabilità tra il fornitore di servizi cloud e il cliente (o utente) per garantire la sicurezza e la gestione efficiente dei dati e delle risorse nel cloud. Questo modello è fondamentale per comprendere chi è responsabile di cosa e per garantire una collaborazione efficace tra entrambe le parti coinvolte.

In generale, il modello di responsabilità condivisa si applica a diversi aspetti della gestione del cloud, inclusi ma non limitati a:

1. Infrastruttura fisica;
2. Sicurezza della piattaforma;
3. Gestione dell'identità e degli accessi;
4. Dati;
5. Conformità normativa;

Il modello di responsabilità condivisa è progettato per garantire che entrambe le parti, il fornitore di servizi cloud e il cliente, contribuiscano alla sicurezza e alla gestione dei dati e delle risorse nel cloud. È importante che le responsabilità siano chiare per evitare ambiguità e garantire un ambiente cloud sicuro e conforme.

# 2. Campo di applicazione

Il modello di responsabilità condivisa si applica a tutti i servizi erogati secondo il paradigma cloud computing da ACCA software ai propri Clienti Finali.

Per l'erogazione dei servizi cloud, ACCA software si avvale del Cloud Service Provider Amazon Web Services (AWS), il quale offre una vasta gamma di servizi, tra cui calcolo, archiviazione, database, analisi, intelligenza artificiale, sicurezza, sviluppo di applicazioni e molti altri.

AWS è diventato uno dei principali fornitori di servizi cloud a livello globale, utilizzato da aziende di diverse dimensioni e settori. Alcuni dei servizi più noti offerti da AWS includono Amazon EC2 (Elastic Compute Cloud) per il calcolo su richiesta, Amazon S3 (Simple Storage Service) per l'archiviazione di dati, Amazon RDS (Relational Database Service) per la gestione di database relazionali, e Amazon Lambda per l'esecuzione di codice senza la necessità di gestire l'infrastruttura sottostante.

La scelta di questo CSP è dovuta anche all'adozione di un approccio completo alla sicurezza e alla conformità, cercando di soddisfare le esigenze e i requisiti di un'ampia varietà di clienti provenienti da settori diversi: in tal senso AWS ha ottenuto numerosi certificati di conformità e ha implementato misure di sicurezza per garantire la protezione dei dati dei clienti.

Alcuni degli standard e dei certificati di conformità più comuni associati ad AWS includono:

- ISO 27001: Certificazione per il sistema di gestione della sicurezza delle informazioni.
- SOC 1, SOC 2, e SOC 3: Report di controllo delle organizzazioni di servizi, sviluppati dall'AICPA (American Institute of Certified Public Accountants).




☒ Pubblico
☐ Interno
☐ Riservato

- PCI DSS: Standard di sicurezza dei dati per le organizzazioni che elaborano transazioni con carte di pagamento.
- HIPAA: Standard di sicurezza delle informazioni per la gestione dei dati sanitari negli Stati Uniti.

# 3. Modello di Responsabilità condivisa

La sicurezza e la conformità sono una responsabilità condivisa tra AWS, ACCA software ed il Cliente finale.

Tale modello condiviso può aiutare ad agevolare le incombenze operative del cliente in quanto AWS aziona, gestisce e controlla i componenti dal sistema operativo host e il livello di virtualizzazione fino alla sicurezza fisica delle strutture in cui il servizio opera, mentre ACCA software si assume la responsabilità e la gestione del sistema operativo guest (inclusi gli aggiornamenti e le patch di sicurezza), di altro software applicativo nonché della configurazione del firewall del gruppo di sicurezza fornito da AWS; infine, il Cliente finale è proprietario dei dati e ne è responsabile per il loro utilizzo.

La natura di questa responsabilità condivisa offre anche la flessibilità e il controllo cliente che rendono possibile la distribuzione. Come illustrato graficamente in Figura 1, questa differenziazione della responsabilità viene comunemente detta sicurezza "*del*" cloud rispetto a sicurezza "*nel*" cloud, oltre alla responsabilità finale del Cliente per quanto riguarda l'utilizzo dei propri dati.

- **Responsabilità di AWS "Sicurezza del cloud":** AWS si occupa di proteggere l'infrastruttura globale su cui vengono eseguiti tutti i servizi offerti nel cloud AWS. L'infrastruttura è formata dai componenti hardware e software, le reti e le strutture che eseguono i servizi Cloud AWS.
- **Responsabilità di ACCA software "Sicurezza nel cloud":** la responsabilità di ACCA software viene applicata ai servizi Cloud AWS di cui ACCA ne fa uso per erogare servizi SaaS agli utenti finali. Ad esempio, Amazon Elastic Compute Cloud (Amazon EC2), è classificato come Infrastructure as a Service (IaaS) e, in quanto tale, richiede che ACCA esegua tutte le necessarie attività di configurazione e gestione della sicurezza; in tal senso ACCA è responsabile della gestione del sistema operativo guest (inclusi aggiornamenti e patch di sicurezza), di qualsiasi software applicativo o utilità installata dal cliente sulle istanze e della configurazione del firewall fornito da AWS (chiamato gruppo di sicurezza) in ogni istanza.
- **Responsabilità del Cliente Finale:** il Cliente si impegna a utilizzare i servizi SaaS erogati da ACCA software nel rispetto delle vigenti disposizioni di legge, rimane unico ed esclusivo responsabile dei contenuti immessi o diffusi tramite i servizi oggetti di contratto, sui quali ACCA garantisce disponibilità, integrità e riservatezza senza effettuare alcuna verifica o controllo nei contenuti di tali dati.

Questo modello di responsabilità condivisa da Cliente Finale/ACCA software/AWS si estende anche ai controlli IT. Oltre alla responsabilità di esecuzione dell'ambiente IT, anche la gestione, l'esecuzione e la verifica dei controlli IT sono condivise tra AWS ed ACCA.

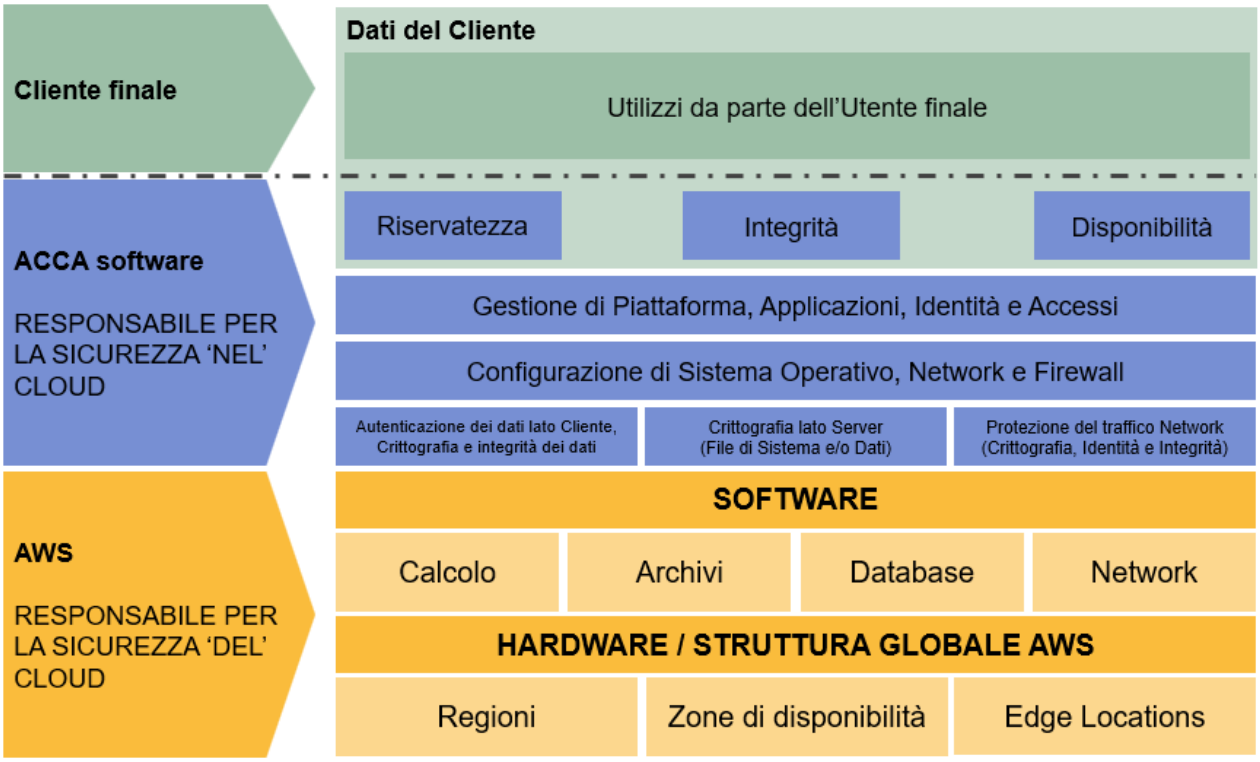


*Figura 1. Modello di responsabilità condivisa.*