CAIQ (Consensus Assessments Initiative Questionnaire) della CSA

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

Il questionario dell'iniziativa di valutazione del consenso CSA contiene una serie di domande frequenti che un consumatore di servizi cloud e/o un revisore cloud potrebbero voler chiedere a un fornitore di servizi cloud. Riporta una serie di domande relative alla sicurezza, ai controlli e ai processi che si prestano a una vasta gamma di utilizzi, compresa la scelta del fornitore di servizi cloud e la valutazione della sicurezza. AWS ha completato il questionario fornendo le seguenti risposte.

Introduzione

Cloud Security Alliance (CSA) è "un'organizzazione no profit che intende promuovere l'utilizzo delle best practice per offrire la garanzia della sicurezza nel cloud computing ed educare agli utilizzi del cloud computing, rafforzando allo stesso tempo la sicurezza di tutte le altre forme di elaborazione". Per ulteriori informazioni, consultare la pagina https://cloudsecurityalliance.org/about/.

Numerosi professionisti, aziende e associazioni che operano nel settore della sicurezza partecipano a questa organizzazione per perseguire tale scopo.

CAIQ (Consensus Assessments Initiative Questionnaire) della CSA

Gruppo di controllo	CID	Domande sulla valutazione del consenso	Risposta AWS
Sicurezza delle applicazioni e delle interfacce *Sicurezza delle applicazioni*	AIS-01.1	Vengono utilizzati standard industriali (benchmark BSIMM (Build Security in Maturity Model), Open Group ACS Trusted Technology Provider Framework, NIST e così via) per integrare la sicurezza per l'SDLC (Systems/Software Development Lifecycle)?	Il ciclo di vita dello sviluppo di sistema AWS (SDLC) integra best practice di settore tra cui revisioni formali da parte del team di sicurezza AWS, modellazione delle minacce e completamento di una valutazione del rischio. Per ulteriori dettagli, consultare il whitepaper AWS Overview of Security Processes (Panoramica sulle procedure di sicurezza AWS). AWS ha implementato procedure per gestire il nuovo sviluppo di risorse. Per ulteriori dettagli, fare riferimento allo standard ISO 27001, appendice A, dominio 14. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	AIS-01.2	Viene utilizzato uno strumento di analisi del codice sorgente automatizzato per rilevare i difetti di sicurezza del codice prima della produzione?	
	AIS-01.3	Viene utilizzata un'analisi manuale del codice sorgente per rilevare i difetti di sicurezza del codice prima della produzione?	

Gruppo di	CID	Domande sulla	Risposta AWS
	AIS-01.4	Viene verificato se tutti i fornitori di software aderiscono agli standard di settore per la sicurezza SDLC (Systems/Software Development Lifecycle)?	
	AIS-01.5	(Solo SaaS) Viene effettuato il controllo delle applicazioni alla ricerca di vulnerabilità della sicurezza e vengono affrontati gli eventuali problemi prima della distribuzione per la produzione?	
Sicurezza delle applicazioni e delle interfacce *Requisiti di accesso dei clienti*	AIS-02.1	Tutti i requisiti normativi, contrattuali e di sicurezza identificati per l'accesso dei clienti sono stati presi in considerazione e corretti per contratto prima di concedere ai clienti l'accesso a dati, asset e sistemi informatici?	Spetta sempre ai clienti AWS la responsabilità di garantire che il proprio uso di AWS sia conforme alle leggi e alle norme vigenti. AWS comunica ai clienti informazioni sul proprio ambiente di sicurezza e controllo tramite certificazioni del settore e attestazioni di terze parti, whitepaper (disponibili all'indirizzo http://aws.amazon.com/compliance) e fornendo certificazioni, rapporti e altra documentazione pertinente direttamente ai clienti AWS.
	AIS-02.2	Tutti i requisiti e i livelli di attendibilità per l'accesso dei clienti sono stati definiti e documentati?	
Sicurezza delle applicazioni e delle interfacce *Integrità dei dati*	AIS-03.1	Le routine di integrità di ingresso e uscita dei dati (ovvero, controlli di modifiche e riconciliazione) sono state implementate per i database e le interfacce di applicazione in modo da impedire errori di elaborazione, manuali o sistematici o la corruzione dei dati?	I controlli dell'integrità dei dati AWS descritti nei rapporti AWS SOC illustrano i controlli sull'integrità dei dati mantenuti in tutte le fasi, comprese trasmissione, storage ed elaborazione. Per ulteriori informazioni, fare inoltre riferimento allo standard ISO 27001, appendice A, dominio 14. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza delle applicazioni e delle interfacce *Sicurezza/integrità dei dati*	AIS-04.1	L'architettura di sicurezza dei dati è progettata utilizzando uno standard industriale (ad esempio CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	L'architettura di sicurezza dei dati AWS è stata progettata per integrare pratiche all'avanguardia nel settore. Fare riferimento alle certificazioni, ai rapporti e ai whitepaper AWS per ulteriori dettagli sulle pratiche all'avanguardia adottate da AWS (disponibili all'indirizzo http://aws.amazon.com/compliance).
Affidabilità e conformità degli audit *Pianificazione dei controlli*	AAC-01.1	Vengono elaborate asserzioni di controllo utilizzando un formato strutturato e accettato nel settore (ad esempio CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, Cloud Computing Management Audit/Assurance Program di ISACA, ecc.)?	AWS ottiene determinate certificazioni di settore e attestazioni di terze parti indipendenti e fornisce determinate certificazioni, rapporti e altri documenti pertinenti direttamente ai clienti AWS.
Affidabilità e conformità degli audit *Controlli indipendenti*	AAC-02.1	Si consente ai tenant di visualizzare il rapporto SOC2/ISO 27001 o rapporti simili dei controlli o delle certificazioni di terze parti?	AWS fornisce direttamente ai clienti coperti dall'accordo di non divulgazione attestazioni di terze parti, certificazioni, rapporti SOC (Service Organization Controls) e altri rapporti rilevanti sulla conformità. La certificazione ISO 27001 di AWS può essere scaricata qui. Il rapporto AWS SOC 3 può essere scaricato qui. 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. Inoltre, l'ambiente di controllo AWS è soggetto a valutazioni del rischio e audit periodici, interni ed esterni. AWS collabora con organi di certificazione esterni e auditor indipendenti per verificare e testare l'ambiente di controllo AWS nel suo insieme.
	AAC-02.2	Vengono eseguiti periodicamente test di intrusione nella rete sul servizio cloud, come previsto dalle best practice e dalle linee guida di settore?	
	AAC-02.3	Vengono eseguiti periodicamente test di intrusione nelle applicazioni sull'infrastruttura cloud, come previsto dalle best practice e dalle linee guida di settore?	
	AAC-02.4	Vengono eseguiti periodicamente controlli interni, come prescritto dalle best practice e dalle linee guida di settore?	
	AAC-02.5	Vengono eseguiti periodicamente controlli esterni, come prescritto	

Gruppo di	CID	Domande sulla	Risposta AWS
		dalle best practice e dalle linee guida di settore?	
	AAC-02.6	I risultati dei test di intrusione sono messi a disposizione dei tenant su loro richiesta?	
	AAC-02.7	I risultati dei controlli interni ed esterni sono messi a disposizione dei tenant su loro richiesta?	
	AAC-02.8	Esiste un programma di controlli interni che consenta una verifica interfunzionale delle valutazioni?	
Affidabilità e conformità degli audit *Mappatura normativa del sistema informativo*	AAC-03.1	È possibile segmentare a livello logico o crittografare i dati dei clienti, per far sì che i dati possano essere prodotti solo per un unico tenant, senza accedere inavvertitamente ai dati di un altro tenant?	Tutti i dati archiviati da AWS per conto dei clienti dispongono di solide funzionalità di sicurezza e controllo dell'isolamento dei tenant. I clienti mantengono il controllo e la proprietà dei propri dati, pertanto è loro responsabilità scegliere se crittografare i dati. AWS consente ai clienti di utilizzare i propri meccanismi di crittografia per quasi tutti i servizi, inclusi S3, EBS, SimpleDB ed EC2. I tunnel da IPSec a VPC sono anch'essi crittografati. I clienti, inoltre, possono utilizzare AWS Key Management Systems (KMS) per creare e controllare le chiavi di crittografia (fare riferimento a https://aws.amazon.com/kms/). Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security AWS consente ai clienti di eseguire backup su nastro utilizzando il fornitore di servizi da loro scelto. Tuttavia, AWS non fornisce il servizio di backup su nastro. I servizi Amazon S3 e Glacier sono stati progettati per ridurre pressoché a zero il rischio di perdita di dati e la durabilità equivalente a copie multisito degli oggetti dati è ottenuta tramite la ridondanza dello storage dei dati. Per informazioni sulla durabilità dei dati e la ridondanza consultare il sito Web AWS.
	AAC-03.2	È possibile recuperare i dati per uno specifico cliente in caso di problemi o di perdita di dati?	

Gruppo di	CID	Domande sulla	Risposta AWS
	AAC-03.3	È possibile limitare lo storage dei dati dei clienti a specifici paesi o aree geografiche?	I clienti AWS indicano in quale regione fisica saranno ubicati i propri contenuti. AWS non sposterà i contenuti dei clienti dalle regioni selezionate senza avvisare il cliente, a meno che ciò non sia necessario in osservanza della legge o di richieste da parte di enti governativi. Per un elenco completo delle regioni disponibili, consultare la pagina Infrastruttura globale di AWS.
	AAC-03.4	È stato implementato un programma che abbia la capacità di monitorare le modifiche ai requisiti di legge nelle giurisdizioni pertinenti, adeguare il programma di sicurezza a tali modifiche e assicurare la conformità ai requisiti normativi pertinenti?	AWS esegue il monitoraggio dei requisiti di legge e normativi pertinenti. Per ulteriori dettagli, fare riferimento allo standard ISO 27001, appendice 18. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
Gestione della continuità operativa e resilienza operativa *Pianificazione della continuità aziendale*	BCR-01.1	Ai tenant vengono fornite opzioni di hosting resilienti dal punto di vista geografico?	I data center sono costruiti in cluster in diverse regioni globali. AWS offre ai clienti la flessibilità necessaria per avviare istanze e memorizzare dati all'interno di più regioni geografiche e in più zone di disponibilità all'interno di ogni regione. I clienti dovrebbero pianificare l'utilizzo di AWS in modo da sfruttare le diverse regioni e zone di disponibilità. Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security.
	BCR-01.2	Ai tenant viene fornita la funzionalità di failover per i servizi infrastrutturali ad altri fornitori?	
Gestione della continuità operativa e resilienza operativa *Test della continuità aziendale*	BCR-02.1	I piani di continuità operativa sono sottoposti a test a intervalli pianificati o in caso di modifiche ambientali o organizzative significative per garantire una costante efficacia?	I piani e le policy di continuità operativa AWS sono stati sviluppati e testati in linea con gli standard ISO 27001. Per ulteriori dettagli su AWS e sulla continuità operativa, fare riferimento allo standard ISO 27001, appendice A, domino 17.

Gruppo di	CID	Domande sulla	Risposta AWS
Gestione della continuità operativa e resilienza operativa *Alimentazione/ telecomuni-cazioni*	BCR-03.1	Ai tenant viene fornita la documentazione in cui è descritto il percorso di trasporto dei propri dati tra un sistema e l'altro?	I clienti AWS indicano in quale regione fisica saranno ubicati i propri dati e server. AWS non sposterà i contenuti dei clienti dalle regioni selezionate senza avvisare il cliente, a meno che ciò non sia necessario in osservanza della legge o di richieste da parte di enti governativi. Nei rapporti AWS SOC sono forniti ulteriori dettagli. I clienti possono anche scegliere il loro percorso di rete alle strutture AWS, tra cui reti private dedicate in cui il cliente controlla l'instradamento del traffico.
	BCR-03.2	I tenant possono definire in che modo i propri dati vengono trasportati e attraverso quali giurisdizioni legali?	
Gestione della continuità operativa e resilienza operativa Documenta-zione	BCR-04.1	I documenti relativi al sistema informatico (ad esempio guide per gli utenti e gli amministratori, schemi dell'architettura e così via) sono messi a disposizione del personale autorizzato per garantire la corretta configurazione, installazione e utilizzo del sistema informatico?	La documentazione sul sistema informativo è resa disponibile internamente al personale AWS tramite il sito Intranet di Amazon. Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security/. Fare riferimento allo standard ISO 27001, appendice A, dominio 12.
Gestione della continuità operativa e resilienza operativa *Rischi ambientali*	BCR-05.1	La protezione fisica contro danni (ad esempio da calamità, eventi naturali, attacchi deliberati) è prevista e progettata e sono applicate contromisure?	I data center AWS si avvalgono di protezioni fisiche contro i rischi ambientali. La protezione fisica adottata da AWS contro i rischi ambientali è stata convalidata da un revisore indipendente e ne è stata certificata la conformità con le best practice ISO 27002. Fare riferimento allo standard ISO 27001, appendice A, dominio 11.
Gestione della continuità operativa e resilienza operativa *Ubicazione dell'apparecchiatura*	BCR-06.1	Esistono data center della società situati in luoghi caratterizzati da alta probabilità/frequenza di rischi ambientali a impatto elevato (inondazioni, tornado, terremoti, uragani e così via)?	I data center AWS si avvalgono di protezioni fisiche contro i rischi ambientali. La protezione fisica adottata da AWS contro i rischi ambientali è stata convalidata da un revisore indipendente e ne è stata certificata la conformità con le best practice ISO 27002. Fare riferimento allo standard ISO 27001, appendice A, dominio 11.

Gruppo di	CID	Domande sulla	Risposta AWS
Gestione della continuità operativa e resilienza operativa *Manutenzione delle apparecchiature*	BCR-07.1	Se si utilizza l'infrastruttura virtuale, la soluzione cloud include funzionalità di ripristino e recupero indipendenti dall'hardware?	La funzionalità EBS Snapshot consente ai clienti di acquisire e ripristinare le immagini della macchina virtuale in qualsiasi momento. I clienti possono esportare le proprie AMI e utilizzarle localmente o presso un altro fornitore (soggetto alle limitazioni di licenza del software). Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security.
	BCR-07.2	Se si utilizza l'infrastruttura virtuale, ai tenant viene consentito di ripristinare una macchina virtuale a uno stato precedente nel tempo?	
	BCR-07.3	Se si utilizza l'infrastruttura virtuale, sono consentiti il download e il trasferimento delle immagini della macchina virtuale a un nuovo fornitore di servizi cloud?	
	BCR-07.4	Se si utilizza l'infrastruttura virtuale, le immagini delle macchine sono messe a disposizione del cliente in modo tale da permettergli di replicare tali immagini nella propria posizione di storage fuori sede?	
	BCR-07.5	La soluzione cloud include funzionalità di ripristino e recupero indipendenti dal software/provider?	
Gestione della continuità operativa e resilienza operativa *Interruzione di corrente alle apparecchiature*	BCR-08.1	Sono stati implementati meccanismi di sicurezza e ridondanza per proteggere le apparecchiature da interruzioni dei servizi di utilità (ad esempio interruzioni di corrente, interruzioni di rete e così via)?	L'apparecchiatura AWS è protetta dalle interruzioni dei servizi di utilità in conformità allo standard ISO 27001. AWS è stato convalidato e certificato da un auditor indipendente per confermare la conformità allo standard di certificazione ISO 27001. Nei rapporti AWS SOC vengono fornite informazioni aggiuntive sui controlli applicati per ridurre al minimo gli effetti di un malfunzionamento o di un problema fisico del computer o nelle strutture dei data center. Fare inoltre riferimento al whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security.

Gruppo di	CID	Domande sulla	Risposta AWS
Gestione della continuità operativa e resilienza operativa *Analisi dell'impatto*	BCR-09.1	Ai tenant vengono forniti visibilità continua e reporting delle prestazioni operative del contratto sul livello di servizio (SLA, Service Level Agreement)?	AWS CloudWatch assicura il monitoraggio delle risorse cloud AWS e delle applicazioni eseguite dai clienti su AWS. Per ulteriori dettagli, consultare la pagina aws.amazon.com/cloudwatch. AWS pubblica inoltre le informazioni più aggiornate relative alla disponibilità del servizio sul pannello di controllo stato servizi. Fare riferimento a status.aws.amazon.com.
	BCR-09.2	Le metriche di sicurezza delle informazioni basate su standard (CSA, CAMM e così via) sono messe a disposizione dei tenant?	
	BCR-09.3	Ai clienti viene fornita visibilità continua e reporting delle prestazioni del contratto sul livello di servizio (SLA, Service Level Agreement)?	
Gestione della continuità operativa e resilienza operativa *Policy*	BCR-10.1	Policy e procedure vengono stabilite e messe a disposizione di tutto il personale per supportare adeguatamente i ruoli operativi dei servizi?	Sono state stabilite policy e procedure attraverso il framework AWS Information Security in base allo standard NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 e ai requisiti PCI DSS. Per ulteriori dettagli, consultare il whitepaper su rischio e conformità AWS, disponibile all'indirizzo http://aws.amazon.com/compliance.
Gestione della continuità operativa e resilienza operativa *Policy di conservazione*	BCR-11.1	Si dispone delle capacità di controllo tecnico per attuare le policy di conservazione dei dati dei tenant?	AWS consente ai clienti di eliminare i propri dati. Tuttavia, i clienti AWS detengono il controllo e la proprietà dei propri dati, pertanto è responsabilità dei clienti gestire la conservazione dei dati sulla base dei propri requisiti. Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security. AWS si impegna a proteggere la privacy dei clienti ed è vigile nel determinare le richieste di applicazione delle norme che devono essere rispettate. AWS non esita a contestare i provvedimenti delle forze dell'ordine qualora ritenga che tali misure siano prive di una solida base. Per ulteriori informazioni, fare riferimento a https://aws.amazon.com/compliance/data-privacy-faq/.
	BCR-11.2	È stata messa in atto una procedura documentata per rispondere alle richieste di dati dei tenant da parte di governi o di terze parti?	

Gruppo di	CID	Domande sulla	Risposta AWS
	BCR-11.4	Sono stati implementati meccanismi di backup o di ridondanza per garantire il rispetto dei requisiti normativi, legali, contrattuali o aziendali?	I meccanismi di backup e di ridondanza AWS sono stati sviluppati e testati in linea con gli standard ISO 27001. Per ulteriori informazioni sui meccanismi di backup e ridondanza AWS, fare riferimento allo standard ISO 27001, appendice A, dominio 12 e al rapporto AWS SOC 2.
	BCR-11.5	I meccanismi di backup o di ridondanza sono sottoposti a test almeno una volta all'anno?	
Controllo delle modifiche e gestione delle configurazioni *Nuovo sviluppo/ acquisizione*	CCC-01.1	Esistono policy e procedure per la gestione dell'autorizzazione per lo sviluppo o all'acquisizione di nuove applicazioni, sistemi, database, infrastrutture, servizi, operazioni e impianti?	Sono state stabilite policy e procedure attraverso il framework AWS Information Security in base allo standard NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 e ai requisiti PCI DSS. Se il cliente ha mosso i primi passi in AWS oppure se è un utente avanzato, potrà trovare informazioni utili sui servizi, che spaziano dalle nozioni introduttive alle caratteristiche avanzate, nella sezione Documentazione AWS del sito Web all'indirizzo https://aws.amazon.com/documentation/.
	CCC-01.2	È disponibile una documentazione che descriva l'installazione, la configurazione e l'utilizzo di prodotti/ servizi/caratteristiche?	
Controllo delle modifiche e gestione delle configurazioni *Sviluppo in outsourcing*	CCC-02.1	Sono disponibili controlli per assicurare che gli standard di qualità vengano rispettati per tutto lo sviluppo del software?	AWS generalmente non esternalizza lo sviluppo di software. AWS integra standard di qualità nell'ambito dei processi SDLC (System Development Lifecycle, ciclo di vita di sviluppo dei sistemi). Per ulteriori dettagli, fare riferimento allo standard ISO 27001, appendice A, dominio 14. AWS è stato convalidato e certificato da un auditor indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	CCC-02.2	Sono disponibili controlli per rilevare i difetti di sicurezza del codice sorgente per tutte le attività di sviluppo software in outsourcing?	

Gruppo di	CID	Domande sulla	Risposta AWS
Controllo delle modifiche e gestione delle *configurazioni* *Test di qualità*	CCC-03.1	Ai tenant viene fornita la documentazione in cui è descritta la procedura di controllo qualità?	AWS dispone della certificazione ISO 9001. Si tratta di una convalida indipendente del sistema di qualità AWS che ha accertato che le attività di AWS sono conformi ai requisiti della certificazione ISO 9001. I bollettini sulla sicurezza AWS comunicano ai clienti gli eventi relativi alla sicurezza e alla privacy. I clienti possono iscriversi al feed RSS dei bollettini sulla sicurezza AWS nel sito Web di AWS. Fare riferimento aws.amazon.com/security/security-bulletins/. AWS pubblica inoltre le informazioni più aggiornate relative alla disponibilità del servizio sul pannello di controllo stato servizi. Fare riferimento a status.aws.amazon.com. Il ciclo di vita dello sviluppo di sistema AWS (SDLC) integra best practice di settore tra cui revisioni formali da parte del team di sicurezza AWS, modellazione delle minacce e completamento di una valutazione del rischio. Per ulteriori dettagli, consultare il whitepaper AWS Overview of Security Processes (Panoramica sulle procedure di sicurezza AWS). Per ulteriori informazioni, fare inoltre riferimento allo standard ISO 27001, appendice A, dominio 14. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	CCC-03.2	È disponibile una documentazione che descriva i problemi noti di alcuni prodotti/servizi?	
	CCC-03.3	Sono state implementate policy e procedure per valutare e trovare una soluzione a bug e vulnerabilità della sicurezza segnalati per le offerte di prodotti e servizi?	
	CCC-03.4	Sono stati implementati meccanismi per garantire che tutti gli elementi del debug e del codice di prova siano stati rimossi dalle versioni software rilasciate?	
Controllo delle modifiche e gestione delle configurazioni *Installazioni software non autorizzate*	CCC-04.1	Sono disponibili controlli per limitare e monitorare l'installazione di software non autorizzato sui propri sistemi?	Il programma, i processi e le procedure AWS per la gestione del software malware sono conformi agli standard ISO 27001. Per ulteriori dettagli, fare riferimento allo standard ISO 27001, appendice A, dominio 12. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
Controllo delle modifiche e gestione delle configurazioni *Cambi produzione*	CCC-05.1	Ai tenant viene fornita la documentazione in cui sono descritte le procedure di gestione dei cambi in produzione e i loro relativi ruoli/diritti/ responsabilità?	Nei rapporti AWS SOC è fornita una panoramica sui controlli disponibili per gestire le modifiche nell'ambiente AWS. Per ulteriori informazioni, fare inoltre riferimento allo standard ISO 27001, appendice A, dominio 12. AWS è stato convalidato e certificato da un auditor indipendente per confermare la conformità allo standard di certificazione ISO 27001.

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza dei dati e gestione del ciclo di vita delle informazioni *Classificazione*	DSI-01.1	Viene offerta la possibilità di identificare le macchine virtuali tramite tag di policy/metadati (ad esempio tag che possono essere utilizzati per evitare che i sistemi operativi guest possano avviare/creare istanze/trasportare i dati nel paese errato)?	Ai clienti vengono assegnate macchine virtuali nell'ambito del servizio EC2. I clienti mantengono il controllo su quali risorse vengono utilizzate e su dove le risorse risiedono. Per ulteriori dettagli, consultare il sito Web AWS all'indirizzo http://aws.amazon.com.
	DSI-01.2	Viene offerta la possibilità di identificare l'hardware tramite tag di policy/metadati/tag di hardware (ad esempio TXT/TPM, VN-Tag e così via)?	AWS offre la possibilità di aggiungere tag alle risorse EC2. Una forma di metadati, i tag EC2, può essere utilizzata per creare nomi facilmente identificabili dagli utenti, migliorare la ricercabilità e rafforzare il coordinamento tra più utenti. La console di gestione AWS supporta anch'essa i tag.
	DSI-01.3	È possibile utilizzare la posizione geografica del sistema come fattore di autenticazione?	AWS offre la possibilità di eseguire l'accesso utente condizionato in base all'indirizzo IP. I clienti possono aggiungere le condizioni per controllare la modalità di utilizzo di AWS da parte degli utenti, come ad esempio l'ora del giorno, il relativo indirizzo IP di origine o l'eventuale utilizzo di SSL.
	DSI-01.4	Amazon fornisce la posizione fisica/l'area geografica dello storage dei dati di un tenant su richiesta?	AWS offre ai clienti la flessibilità necessaria per avviare istanze e memorizzare dati all'interno di più regioni geografiche. I clienti AWS indicano in quale regione fisica saranno ubicati i propri dati e server. AWS non sposterà i contenuti dei clienti dalle regioni selezionate senza avvisare il cliente, a meno che ciò non sia necessario in osservanza della legge o di richieste da parte di enti governativi. Le dodici regioni presenti al momento della stesura del presente documento sono le seguenti: Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), AWS GovCloud (US) (Oregon), UE (Irlanda), UE (Francoforte), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Tokyo), Asia Pacifico (Sydney), Cina (Pechino) e Sud America (San Paolo).
	DSI-01.5	Amazon fornisce la posizione fisica/l'area geografica dello storage dei dati di un tenant in anticipo?	
	DSI-01.6	Viene seguito uno standard strutturato per l'etichettatura dei dati (ad esempio ISO 15489,	I clienti AWS mantengono il controllo e la proprietà dei propri dati e possono implementare uno standard strutturato di etichettatura dei dati per soddisfare i propri

Gruppo di	CID	Domande sulla	Risposta AWS
		Oasis XML Catalog Specification, CSA Data Type Guidance)?	requisiti.
	DSI-01.7	Si consente ai tenant di definire le posizioni geografiche accettabili per il routing dei dati o la creazione dell'istanza delle risorse?	AWS offre ai clienti la flessibilità necessaria per avviare istanze e memorizzare dati all'interno di più regioni geografiche. I clienti AWS indicano in quale regione fisica saranno ubicati i propri dati e server. AWS non sposterà i contenuti dei clienti dalle regioni selezionate senza avvisare il cliente, a meno che ciò non sia necessario in osservanza della legge o di richieste da parte di enti governativi. Le dodici regioni presenti al momento della stesura del presente documento sono le seguenti: Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), AWS GovCloud (US) (Oregon), UE (Irlanda), UE (Francoforte), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Tokyo), Asia Pacifico (Sydney), Cina (Pechino) e Sud America (San Paolo).
Sicurezza dei dati e gestione del ciclo di vita delle informazioni *Inventario/ flussi dei dati*	DSI-02.1	Vengono inventariati, documentati e gestiti i flussi dei dati residenti (in via permanente o temporanea) nelle applicazioni dei servizi e nella rete e nei sistemi dell'infrastruttura?	I clienti AWS indicano in quale regione fisica saranno ubicati i propri contenuti. AWS non sposterà i contenuti dei clienti dalle regioni selezionate senza avvisare il cliente, a meno che ciò non sia necessario in osservanza della legge o di richieste da parte di enti governativi. Le dodici regioni presenti al momento della stesura del presente documento sono le seguenti: Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), AWS GovCloud (US) (Oregon), UE (Irlanda), UE (Francoforte), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Tokyo), Asia Pacifico (Sydney), Cina (Pechino) e Sud America (San Paolo).
	DSI-02.2	Si garantisce che i dati non migrino al di là di una determinata residenza geografica?	

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza dei dati e gestione del ciclo di vita delle informazioni *Transazioni eCommerce*	DSI-03.1	Ai tenant vengono fornite metodologie di crittografia aperte (3.4ES, AES e così via), in modo da permettere la protezione dei dati se è necessario attraversare reti pubbliche (ad esempio Internet)?	Tutte le API AWS sono disponibili tramite gli endpoint SSH protetti che forniscono l'autenticazione del server. AWS consente ai clienti di utilizzare i propri meccanismi di crittografia per quasi tutti i servizi, inclusi S3, EBS, SimpleDB ed EC2. I tunnel da IPSec a VPC sono anch'essi crittografati. I clienti, inoltre, possono utilizzare AWS Key Management Systems (KMS) per creare e controllare le chiavi di crittografia (fare riferimento a https://aws.amazon.com/kms/). I clienti possono utilizzare anche tecnologie di crittografia di terze parti. Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security.
	DSI-03.2	Vengono utilizzate metodologie di crittografia aperte ogniqualvolta i componenti dell'infrastruttura devono comunicare tra loro su reti pubbliche (ad esempio replica dei dati basata su Internet da un ambiente all'altro)?	
Sicurezza dei dati e gestione del ciclo di vita delle informazioni *Policy di gestione/ etichettatura/ protezione*	DSI-04.1	Sono state stabilite policy e procedure per etichettatura, gestione e protezione di dati e oggetti che contengono dati?	I clienti AWS detengono il controllo e la proprietà dei propri dati e possono implementare una policy di etichettatura e gestione e procedure specifiche per soddisfare le proprie esigenze.
	DSI-04.2	Sono stati implementati meccanismi per l'ereditarietà delle etichette per gli oggetti che fungono da contenitori aggregati per i dati?	
Sicurezza dei dati e gestione del ciclo di vita delle informazioni *Dati non destinati alla produzione*	DSI-05.1	Sono state implementate procedure per garantire che i dati di produzione non possano essere replicati o utilizzati negli ambienti non destinati alla produzione?	I clienti AWS detengono il controllo e la proprietà dei propri dati. AWS offre ai clienti la possibilità di gestire e sviluppare ambienti di produzione e non destinati alla produzione. È responsabilità del cliente assicurarsi che i propri dati di produzione non vengano replicati in ambienti non destinati alla produzione.
Sicurezza dei dati e gestione del ciclo di vita delle informazioni *Proprietà/amministrazione*	DSI-06.1	Le responsabilità relative all'amministrazione dei dati sono definite, assegnate, documentate e comunicate?	I clienti AWS detengono il controllo e la proprietà dei propri dati. Per ulteriori informazioni, fare riferimento al contratto clienti AWS.

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza dei dati e gestione del ciclo di vita delle informazioni *Smaltimento sicuro*	DSI-07.1	L'eliminazione sicura (ad esempio smagnetizzazione/ cancellazione crittografica) dei dati archiviati e di backup, così come determinato dal tenant, è supportata?	Quando un dispositivo di storage raggiunge la fine della sua vita utile, le procedure AWS includono un processo di disattivazione progettato per impedire che i dati del cliente siano accessibili a persone non autorizzate. AWS utilizza le tecniche riportate in dettaglio nel DoD 5220.22-M ("National Industrial Security Program Operating Manual") o NIST 800-88 ("Guidelines for Media Sanitization") per distruggere i dati come parte del processo di disattivazione. Se non è possibile disattivare un dispositivo hardware mediante queste procedure, il dispositivo sarà smagnetizzato o distrutto fisicamente in conformità alle procedure standard del settore. Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security. I volumi Amazon EBS si presentano come dispositivi a blocchi vergini non formattati che sono stati sottoposti a cancellazione prima di essere resi disponibili per l'uso. La cancellazione viene effettuata subito prima del riutilizzo, per essere certi che il processo di cancellazione sia stato completato. Amazon EBS consente di implementare procedure che richiedono la cancellazione di tutti i dati con un metodo specifico, come quelli descritti in DoD 5220.22-M ("National Industrial Security Program Operating Manual") o in NIST 800-88 ("Guidelines for Media Sanitization"). È opportuno effettuare una procedura di cancellazione specializzata prima di procedere alla cancellazione del volume per la conformità ai propri requisiti. La crittografia di dati sensibili è, in genere, una prassi di sicurezza affidabile e AWS consente di crittografare i volumi EBS e le loro snapshot con AES-256. La crittografia viene effettuata sui server che ospitano le istanze EC2, mentre i dati si spostano tra istanze EC2 e storage EBS. Per poter completare tale procedura in modo efficiente e con una bassa latenza, la caratteristica di crittografia EBS è disponibile solo sui tipi di istanze EC2 più potenti (ad esempio M3, C3, R3, G2).
	DSI-07.2	Amazon fornisce una procedura pubblicata per la cessazione dell'accordo di servizio, compresa l'assicurazione per la pulizia di tutte le risorse informatiche dei dati del tenant, dopo che un cliente è uscito dal proprio ambiente o ha lasciato libera una risorsa?	

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza dei data center *Gestione degli asset*	DCS-01.1	Viene mantenuto un inventario completo di tutti gli asset critici che include la proprietà dell'asset?	In linea con gli standard ISO 27001, gli asset hardware AWS sono assegnati ad un responsabile, tracciati e monitorati dal personale AWS mediante gli strumenti di gestione inventario proprietari di AWS. Il team della catena di approvvigionamento e distribuzione AWS mantiene i rapporti con tutti i fornitori AWS. Per ulteriori dettagli, fare riferimento agli standard ISO 27001, appendice A, dominio 8. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	DCS-01.2	Viene mantenuto un inventario completo di tutti i rapporti con i fornitori critici?	
Sicurezza dei data center *Punti di accesso controllati*	DCS-02.1	Sono stati implementati perimetri di sicurezza fisici (ad esempio recinzioni, pareti, barriere, protezioni, cancelli, sorveglianza elettronica, meccanismi di autenticazione fisici, banchi di accoglienza e pattuglie di sicurezza)?	I controlli di sicurezza fisici includono, a titolo esemplificativo, controlli perimetrali, quali recinzioni, pareti, personale addetto alla sicurezza, video sorveglianza, sistemi di rilevamento dell'intrusione e altri dispositivi elettronici. Nei rapporti AWS SOC vengono forniti dettagli aggiuntivi sulle attività di controllo specifiche eseguite da AWS. Per ulteriori informazioni, fare riferimento agli standard ISO 27001, appendice A, dominio 11. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
Sicurezza dei data center *Identificazione delle apparecchiature*	DCS-03.1	L'identificazione automatica delle apparecchiature viene utilizzata come metodo per convalidare l'integrità di autenticazione della connessione sulla base dell'ubicazione nota delle apparecchiature?	AWS gestisce l'identificazione delle apparecchiature in conformità allo standard ISO 27001. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
Sicurezza dei data center *Autorizzazione fuori sede*	DCS-04.1	Ai tenant viene fornita la documentazione che descrive gli scenari in cui i dati possono essere spostati da una posizione fisica a un'altra (ad esempio backup fuori sede, failover della continuità di servizio, replica)?	I clienti AWS indicano in quale regione fisica saranno ubicati i propri dati. AWS non sposterà i contenuti dei clienti dalle regioni selezionate senza avvisare il cliente, a meno che ciò non sia necessario in osservanza della legge o di richieste da parte di enti governativi. Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security.

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza dei data center *Apparecchiature fuori sede*	DCS-05.1	È possibile fornire ai tenant le prove che documentano le policy e le procedure che regolano la gestione degli asset e la riallocazione delle apparecchiature?	In linea con gli standard ISO 27001, quando un dispositivo di storage raggiunge la fine della sua vita utile, le procedure AWS includono un processo di disattivazione progettato per impedire che i dati del cliente siano accessibili a persone non autorizzate. AWS utilizza le tecniche riportate in dettaglio nel DoD 5220.22-M ("National Industrial Security Program Operating Manual") o NIST 800-88 ("Guidelines for Media Sanitization") per distruggere i dati come parte del processo di disattivazione. Se non è possibile disattivare un dispositivo hardware mediante queste procedure, il dispositivo sarà smagnetizzato o distrutto fisicamente in conformità alle procedure standard del settore. Per ulteriori dettagli, fare riferimento agli standard ISO 27001, appendice A, dominio 8. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
Sicurezza dei data center *Policy*	DCS-06.1	Amazon fornisce prova che sono state stabilite policy, standard e procedure per il mantenimento di un ambiente di lavoro sicuro e protetto in uffici, sale, strutture e aree protette?	AWS collabora con organismi di certificazione esterni e revisori indipendenti per esaminare e convalidare la nostra conformità con i quadri di conformità. Nei rapporti AWS SOC vengono forniti dettagli aggiuntivi sulle attività di controllo della sicurezza fisica specifiche eseguite da AWS. Per ulteriori dettagli, fare riferimento agli standard ISO 27001, appendice A, dominio 11. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	DCS-06.2	Si può dimostrare che il personale e le terze parti coinvolte hanno ricevuto un'idonea formazione riguardo alle policy, agli standard e alle procedure documentate?	In linea con lo standard ISO 27001, tutti i dipendenti AWS completano una formazione periodica sulla sicurezza delle informazioni per la quale è richiesta conferma di completamento. Vengono effettuati controlli in materia di conformità a cadenza periodica per assicurarsi che i dipendenti comprendano e seguano le policy definite. Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security. AWS è stato convalidato e certificato da un auditor indipendente per confermare la

Gruppo di	CID	Domande sulla	Risposta AWS
			conformità alla certificazione ISO 27001. Inoltre nei rapporti AWS SOC 1 e SOC 2 vengono fornite ulteriori informazioni.
Sicurezza dei data center *Autorizzazione area protetta*	DCS-07.1	Si consente ai tenant di specificare in quale delle proprie aree geografiche possono essere spostati/estratti i loro dati (per rispondere a considerazioni di ordine giuridico basate sulla posizione di archiviazione dei dati rispetto al punto di accesso)?	I clienti AWS indicano in quale regione fisica saranno ubicati i propri dati. AWS non sposterà i contenuti dei clienti dalle regioni selezionate senza avvisare il cliente, a meno che ciò non sia necessario in osservanza della legge o di richieste da parte di enti governativi. Le dodici regioni presenti al momento della stesura del presente documento sono le seguenti: Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), AWS GovCloud (US) (Oregon), UE (Irlanda), UE (Francoforte), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Tokyo), Asia Pacifico (Sydney), Cina (Pechino) e Sud America (San Paolo).
Sicurezza dei data center *Ingresso di persone non autorizzate*	DCS-08.1	I punti di ingresso e di uscita, come le aree di servizio e altri punti in cui il personale non autorizzato può accedere ai locali, sono monitorati, controllati e isolati dal processo e dallo storage dei dati?	L'accesso fisico viene rigorosamente controllato sia lungo il perimetro che presso i punti di ingresso dell'edificio e include, a titolo esemplificativo, il personale addetto alla sicurezza che si avvale di sistemi di video sorveglianza e di rilevamento dell'intrusione e di altri dispositivi elettronici. Il personale autorizzato deve superare almeno due volte un controllo di autenticazione a due fattori per accedere ai piani dei data center. I punti di accesso fisico ai server vengono ripresi da un sistema di videocamere a circuito chiuso (CCTV) come previsto dalla policy sulla sicurezza fisica dei data center AWS. I meccanismi di sicurezza fisica AWS (AWS Physical Security Mechanisms) vengono verificati da revisori esterni indipendenti durante i controlli per la conformità con gli standard SOC, PCI DSS, ISO 27001 e FedRAMP.
Sicurezza dei data center *Accesso utente*	DCS-09.1	Viene limitato l'accesso fisico agli asset delle informazioni e alle funzioni da parte degli utenti e del personale di supporto?	

Gruppo di	CID	Domande sulla	Risposta AWS
Crittografia e gestione delle chiavi *Diritto*	EKM-01.1	Si dispone di policy per la gestione delle chiavi che vincolano le chiavi a titolari identificabili?	AWS permette ai clienti di utilizzare i propri meccanismi di crittografia per quasi tutti i servizi, inclusi S3, EBS ed EC2. Anche le sessioni VPC sono crittografate. I clienti, inoltre, possono utilizzare AWS Key Management Systems (KMS) per creare e controllare le chiavi di crittografia (fare riferimento a https://aws.amazon.com/kms/). Internamente, AWS definisce e gestisce le chiavi crittografiche per i processi di crittografia richiesti all'interno dell'infrastruttura AWS. Un sistema di gestione sicuro delle chiavi e delle credenziali sviluppato da AWS viene utilizzato per creare, proteggere e distribuire chiavi simmetriche e per la sicurezza e la distribuzione di credenziali AWS richieste sugli host, chiavi pubbliche/private RSA e certificazioni X.509. I processi di crittografia AWS vengono verificati da auditor indipendenti di terze parti nell'ambito dell'impegno continuo di conformità agli standard SOC, PCI DSS, ISO 27001 e FedRAMP.
Crittografia e gestione delle chiavi *Generazione delle chiavi*	EKM-02.1	È possibile consentire la creazione di chiavi di crittografia univoche per ciascun tenant?	AWS consente ai clienti di utilizzare i propri meccanismi di crittografia per quasi tutti i servizi, inclusi S3, EBS ed EC2. I tunnel da IPSec a VPC sono anch'essi crittografati. I clienti, inoltre, possono utilizzare AWS Key Management Systems (KMS) per creare e controllare le chiavi di crittografia (fare riferimento a https://aws.amazon.com/kms/). Per maggiori dettagli su KMS fare riferimento ai rapporti AWS SOC. Per ulteriori dettagli, consultare inoltre il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security. Internamente, AWS definisce e gestisce le chiavi crittografiche per i processi di crittografia richiesti all'interno dell'infrastruttura AWS. AWS produce, controlla e distribuisce chiavi crittografiche simmetriche all'interno del sistema informatico AWS utilizzando la tecnologia e i processi di gestione delle chiavi approvati dal NIST. Un sistema di gestione sicuro delle chiavi e delle credenziali sviluppato da AWS viene utilizzato per creare, proteggere e distribuire chiavi simmetriche e per la sicurezza e la distribuzione di
	EKM-02.2	Offrite la possibilità di gestire le chiavi di crittografia per conto dei tenant?	
	EKM-02.3	Vengono adottate procedure di gestione delle chiavi?	
	EKM-02.4	Esiste una titolarità documentata per ogni fase del ciclo di vita delle chiavi di crittografia?	
	EKM-02.5	Vengono utilizzati framework di terze parti/open source/proprietari per gestire le chiavi di crittografia?	

Gruppo di	CID	Domande sulla	Risposta AWS
			credenziali AWS richieste sugli host, chiavi pubbliche/private RSA e certificazioni X.509. I processi di crittografia AWS vengono verificati da auditor indipendenti di terze parti nell'ambito dell'impegno continuo di conformità agli standard SOC, PCI DSS, ISO 27001 e FedRAMP.
Crittografia e gestione delle chiavi *Crittografia*	EKM-03.1	I dati memorizzati (su disco/storage) vengono crittografati all'interno del proprio ambiente?	AWS consente ai clienti di utilizzare i propri meccanismi di crittografia per quasi tutti i servizi, inclusi S3, EBS ed EC2. I tunnel da IPSec a VPC sono anch'essi crittografati. I clienti, inoltre, possono utilizzare AWS Key Management Systems (KMS) per creare e controllare le chiavi di crittografia (fare riferimento a https://aws.amazon.com/kms/). Per maggiori dettagli su KMS fare riferimento ai rapporti AWS SOC. Per ulteriori dettagli, consultare inoltre il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security.
	EKM-03.2	Si ricorre alla crittografia per proteggere i dati e le immagini delle macchine virtuali durante il trasporto attraverso e tra le reti e le istanze hypervisor?	
	EKM-03.3	Le chiavi di crittografia generate dai tenant sono supportate o ai tenant viene consentito di crittografare i dati in un'identità senza accesso a un certificato a chiave pubblica (ad esempio crittografia basata su identità)?	
	EKM-03.4	Si dispone di una documentazione che stabilisca e definisca le policy, le procedure e le linee guida per la gestione della crittografia?	

Gruppo di	CID	Domande sulla	Risposta AWS
Crittografia e gestione delle chiavi *Storage e accesso*	EKM-04.1	Si dispone di una crittografia idonea per le piattaforme e i dati che utilizzi formati aperti/convalidati e algoritmi standard?	AWS consente ai clienti di utilizzare i propri meccanismi di crittografia per quasi tutti i servizi, inclusi S3, EBS ed EC2. I clienti, inoltre, possono utilizzare AWS Key Management Systems (KMS) per creare e controllare le chiavi di crittografia (fare riferimento a https://aws.amazon.com/kms/). Per maggiori dettagli su KMS fare riferimento ai rapporti AWS SOC. AWS stabilisce e gestisce le chiavi crittografiche per i processi di crittografia impiegati all'interno dell'infrastruttura AWS. AWS produce, controlla e distribuisce chiavi crittografiche simmetriche all'interno del sistema informatico AWS utilizzando la tecnologia e i processi di gestione delle chiavi approvati dal NIST. Un sistema di gestione sicuro delle chiavi e delle credenziali sviluppato da AWS viene utilizzato per creare, proteggere e distribuire chiavi simmetriche e per la sicurezza e la distribuzione di credenziali AWS richieste sugli host, chiavi pubbliche/private RSA e certificazioni X.509. I processi di crittografia AWS vengono verificati da auditor indipendenti di terze parti nell'ambito dell'impegno continuo di conformità agli standard SOC, PCI DSS, ISO 27001 e FedRAMP.
	EKM-04.2	Le chiavi di crittografia sono gestite dal consumatore di servizi cloud o da un provider affidabile di servizi di gestione delle chiavi?	
	EKM-04.3	Le chiavi di crittografia sono archiviate nel cloud?	
	EKM-04.4	Si dispone di compiti distinti per la gestione delle chiavi e l'utilizzo delle chiavi?	
Governance e gestione del rischio *Requisiti baseline*	GRM-01.1	Sono disponibili baseline documentate sulla sicurezza delle informazioni per ogni componente dell'infrastruttura (ad esempio hypervisor, sistemi operativi, router, server DNS e così via)?	In linea con gli standard ISO 27001, AWS gestisce baseline del sistema per i componenti critici. Per ulteriori dettagli, fare riferimento agli standard ISO 27001, appendice A, domini 14 e 18. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001. I clienti possono fornire la propria immagine di macchina virtuale. VM Import consente ai clienti di importare facilmente le immagini della macchina virtuale dall'ambiente esistente nelle istanze EC2 di Amazon.
	GRM-01.2	È possibile eseguire un monitoraggio costante e indicare la conformità dell'infrastruttura in relazione alle baseline di sicurezza delle informazioni?	
	GRM-01.3	Ai clienti è consentito fornire la propria immagine di macchina virtuale collaudata, in modo da garantire la conformità ai propri standard interni?	

Gruppo di	CID	Domande sulla	Risposta AWS
Governance e gestione del rischio *Valutazione dei rischi*	GRM-02.1	Vengono forniti dati sullo stato di controllo della sicurezza, in modo da permettere ai tenant di implementare il monitoraggio continuo standard di settore (che consente la convalida continua del tenant del proprio stato di controllo fisico e logico)?	AWS pubblica certificazioni e rapporti di revisori indipendenti per fornire ai clienti numerose informazioni sulle policy, i processi e i controlli definiti e gestiti da AWS. Le certificazioni e i rapporti pertinenti possono essere forniti ai clienti AWS. Il monitoraggio continuo dei controlli logici può essere eseguito dai clienti nei propri sistemi.
	GRM-02.2	Vengono effettuate valutazioni dei rischi associati ai requisiti di governance dei dati almeno una volta all'anno?	In linea con lo standard ISO 27001, AWS dispone di un programma di gestione del rischio per ridurre e gestire i rischi. AWS dispone inoltre della certificazione AWS ISO 27018. La conformità alla certificazione ISO 27018 dimostra ai clienti che AWS dispone di un sistema di controlli destinato specificamente alla tutela della privacy dei loro contenuti. Per ulteriori informazioni, fare riferimento alle domande frequenti sulla conformità AWS a ISO 27018 all'indirizzo http://aws.amazon.com/compliance/iso-27018-faqs/.
Governance e gestione del rischio *Controllo della direzione*	GRM-03.1	I dirigenti tecnici, commerciali ed esecutivi sono responsabili della sensibilizzazione e della conformità alle policy, procedure e standard di sicurezza per loro stessi e per i dipendenti, nella misura in cui si applicano all'ambito di responsabilità del dirigente e dei dipendenti?	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. Per ulteriori dettagli, consiltare il whitepaper AWS su rischio e conformità, disponibile all'indirizzo http://aws.amazon.com/compliance.

Gruppo di	CID	Domande sulla	Risposta AWS
Governance e gestione del rischio *Programma di gestione*	GRM-04.1	Ai tenant viene fornita la documentazione in cui è descritto il programma di gestione della sicurezza delle informazioni (ISMP, Information Security Management Program)?	AWS fornisce ai clienti la certificazione ISO 27001. La certificazione ISO 27001 riguarda specificamente il sistema ISMS AWS e misura come i processi interni AWS seguono lo standard ISO. Per la certificazione è necessario che un revisore indipendente accreditato da una terza parte abbia eseguito una valutazione dei processi e dei controlli AWS e confermi che questi operano in linea con lo standard di certificazione ISO 27001. Per ulteriori informazioni fare riferimento alle domande frequenti sulla conformità AWS allo standard ISO 27001, disponibili nel sito Web all'indirizzo http://aws.amazon.com/compliance/iso-27001-faqs/.
	GRM-04.2	Viene effettuato il controllo del programma di gestione della sicurezza delle informazioni (ISMP) almeno una volta all'anno?	
Governance e gestione del rischio *Coinvolgimento/ supporto della direzione*	GRM-05.1	Viene garantito che fornitori aderiscano alle policy relative a privacy e sicurezza delle informazioni?	AWS ha stabilito un framework e policy di sicurezza delle informazioni, che ha integrato il framework certificabile ISO 27001 basato sui controlli ISO 27002, sui criteri Trust Services Principles dell'American Institute of Certified Public Accountants (AICPA), sul PCI DSS v3.1 e sulla National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). AWS gestisce i rapporti con le terze parti in conformità agli standard ISO 27001. I requisiti delle terze parti AWS vengono verificati da revisori esterni indipendenti durante i controlli per la conformità con gli standard PCI DSS, ISO 27001 e FedRAMP. Le informazioni relative ai programmi di conformità AWS sono pubblicate sul sito Web disponibile all'indirizzo http://aws.amazon.com/conformità/.
Governance e gestione del rischio *Policy*	GRM-06.1	Le policy adottate in relazione a privacy e sicurezza delle informazioni sono in linea con gli standard di settore (ISO-27001, ISO-22307, CoBIT e così via)?	
	GRM-06.2	Esistono accordi per garantire che fornitori aderiscano alle policy relative a privacy e sicurezza delle informazioni?	
	GRM-06.3	Si può dimostrare che è stata eseguita la mappatura di due diligence di controlli, architettura e procedure in base ai regolamenti e/o agli standard?	
	GRM-06.4	I controlli, gli standard, le certificazioni e/o i regolamenti a cui si è conformi sono resi pubblici?	

Gruppo di	CID	Domande sulla	Risposta AWS
Governance e gestione del rischio *Applicazione delle policy*	GRM-07.1	È stata stabilita una policy disciplinare o sanzionatoria formale per i dipendenti che hanno violato le policy e le procedure di sicurezza?	AWS ha implementato policy di sicurezza e fornisce formazione sulla sicurezza ai dipendenti per educarli sul loro ruolo e sulle responsabilità in relazione alla sicurezza delle informazioni. I dipendenti che violano gli standard o i protocolli di Amazon sono soggetti a indagini e vengono adottati gli opportuni provvedimenti disciplinari (ad esempio avvertimento, piano di prestazioni, sospensione e/o cessazione del rapporto di lavoro). Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security. Per ulteriori dettagli, fare riferimento allo standard ISO 27001, appendice A, dominio 7. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	GRM-07.2	I dipendenti sono a conoscenza di quali azioni potrebbero essere intraprese in caso di violazione facendo riferimento a policy e procedure?	
Governance e gestione del rischio *Impatti sui cambiamenti aziendali/di policy*	GRM-08.1	I risultati delle valutazioni dei rischi includono aggiornamenti di policy, procedure, standard e controlli di sicurezza per assicurare che rimangano pertinenti ed efficaci?	Gli aggiornamenti di policy, procedure, standard e controlli di sicurezza AWS vengono eseguiti una volta l'anno in conformità allo standard ISO 27001. Per ulteriori informazioni, fare riferimento allo standard ISO 27001. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità alla certificazione ISO 27001.
Governance e gestione del rischio *Revisioni delle policy*	GRM-09.1	I tenant sono informati quando vengono apportate modifiche sostanziali alle policy su privacy e sicurezza delle informazioni?	I whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS) e Risk and conformità (Rischio e conformità), disponibili agli indirizzi http://aws.amazon.com/security e http://aws.amazon.com/compliance, vengono aggiornati periodicamente per riflettere gli aggiornamenti alle policy AWS.
	GRM-09.2	Si eseguono valutazioni interne, come minimo annuali, delle policy in materia di privacy e sicurezza?	Nei rapporti AWS SOC vengono forniti dettagli sulla valutazione delle policy in materia di privacy e sicurezza.

Gruppo di	CID	Domande sulla	Risposta AWS
Governance e gestione del rischio *Valutazioni*	GRM-10.1	Le valutazioni dei rischi formali sono allineate con il quadro a livello aziendale ed eseguite almeno una volta l'anno, o a intervalli pianificati, per determinare la probabilità e l'impatto di tutti i rischi individuati, utilizzando metodi qualitativi e quantitativi?	In linea con lo standard ISO 27001, AWS ha sviluppato un programma di gestione del rischio per ridurre e gestire i rischi. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità alla certificazione ISO 27001. consultare il whitepaper AWS Risk and compliance (Rischio e conformità AWS) (disponibile all'indirizzo aws.amazon.com/security) per ulteriori dettagli sul framework di gestione del rischio AWS (RMF, Risk Management Framework).
	GRM-10.2	La probabilità e l'impatto associati a rischio inerente e residuo sono determinati indipendentemente, considerando tutte le categorie di rischio (ad esempio risultati dei controlli, analisi di minacce e vulnerabilità, nonché conformità alle normative)?	
Governance e gestione del rischio *Programma*	GRM-11.1	È presente un programma documentato per la gestione del rischio a livello dell'intera organizzazione?	In linea con lo standard ISO 27001, AWS dispone di un programma di gestione del rischio per ridurre e gestire i rischi. La direzione di AWS dispone di un piano aziendale strategico che include l'identificazione dei rischi e l'implementazione di controlli finalizzati a limitare o gestire 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. Il programma di gestione del rischio AWS viene verificato da auditor esterni indipendenti durante gli audit per la conformità agli standard PCI DSS, ISO 27001 e FedRAMP.
	GRM-11.2	È resa disponibile la documentazione sul programma di gestione del rischio a livello dell'intera organizzazione?	

Gruppo di	CID	Domande sulla	Risposta AWS
Risorse umane *Rendiconti degli asset*	HRS-01.1	Sono disponibili sistemi per monitorare le violazioni della privacy e avvertire rapidamente i tenant nel caso in cui un evento di privacy interessi i loro dati?	I clienti AWS hanno la responsabilità di monitorare il proprio ambiente per scongiurare violazioni della privacy. Nei rapporti AWS SOC è fornita una panoramica sui controlli disponibili per monitorare l'ambiente gestito AWS.
	HRS-01.2	La policy sulla privacy di Amazon è conforme agli standard di settore?	
Risorse umane *Controlli dei precedenti penali*	HRS-02.1	Ai sensi delle direttive locali, dei regolamenti, dell'etica e dei vincoli contrattuali, per tutti i candidati, gli appaltatori e le terze parti coinvolte vengono eseguite verifiche sulla storia personale?	AWS esegue controlli sui precedenti penali, nei limiti di quanto consentito dalle leggi in vigore, come parte delle pratiche preliminari di selezione del personale, commisurati alla posizione del dipendente e al livello di accesso alle strutture AWS. Nei rapporti AWS SOC vengono forniti dettagli aggiuntivi sui controlli svolti per la verifica dei precedenti.
Risorse umane *Contratti di lavoro*	HRS-03.1	I dipendenti ricevono formazione specifica in relazione al proprio ruolo e rispetto ai controlli di sicurezza delle informazioni che devono soddisfare?	In linea con lo standard ISO 27001, tutti i dipendenti AWS completano una formazione periodica basata sui ruoli che comprende la formazione AWS sulla sicurezza e per la quale è richiesta conferma di completamento. Vengono effettuati controlli in materia di conformità a cadenza periodica per assicurarsi che i dipendenti comprendano e seguano le policy definite. Per ulteriori dettagli fare riferimento ai rapporti SOC. Tutto il personale di supporto dei sistemi e dei dispositivi AWS deve firmare un accordo di non divulgazione prima di ottenere l'autorizzazione di accesso. Inoltre, al momento dell'assunzione, il personale è tenuto a leggere e accettare l'Acceptable Use Policy (policy di utilizzo accettabile) e la policy Codice di condotta aziendale ed etica di Amazon.
	HRS-03.2	La conferma di completamento della formazione da parte dei dipendenti viene documentata?	
	HRS-03.3	Esiste l'obbligo per tutto il personale di firmare accordi di riservatezza quale condizione per il rapporto di lavoro, a tutela delle informazioni dei clienti/tenant?	
	HRS-03.4	Si ritiene che il positivo completamento del programma di formazione entro il tempo stabilito sia un prerequisito per ottenere e mantenere l'accesso a sistemi sensibili?	

Gruppo di	CID	Domande sulla	Risposta AWS
	HRS-03.5	Il personale riceve un'idonea formazione e partecipa a programmi di sensibilizzazione almeno una volta all'anno?	
Risorse umane *Cessazione del rapporto di lavoro*	HRS-04.1	Esistono policy, procedure e linee guida documentate per gestire la variazione delle procedure di lavoro o la cessazione del rapporto di lavoro?	Il team delle risorse umane AWS definisce le responsabilità di gestione interne da seguire per la cessazione e il cambio di ruolo di dipendenti e fornitori. Nei rapporti AWS SOC sono forniti dettagli aggiuntivi.
	HRS-04.2	Le suddette procedure e linee guida comprendono disposizioni relative alla tempestiva revoca degli accessi e alla restituzione degli asset?	L'accesso è revocato automaticamente quando il profilo di un dipendente viene eliminato dal sistema delle risorse umane di Amazon. Quando una funzione lavorativa del dipendente cambia, l'accesso deve essere esplicitamente approvato per la risorsa o sarà revocato automaticamente. Nei rapporti AWS SOC vengono fornite ulteriori informazioni sulla revoca dell'accesso utente. Ulteriori informazioni sono inoltre fornite nel whitepaper sulla sicurezza AWS, sezione "Employee Lifecycle" (Ciclo di vita dei dipendenti). Per ulteriori informazioni, fare riferimento allo standard ISO 27001, appendice A, dominio 7. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
Risorse umane *Dispositivi portatili/mobili*	HRS-05.1	Sono state stabilite policy e procedure e adottate misure per limitare rigorosamente l'accesso ai dati sensibili AWS e ai dati dei tenant da dispositivi portatili e mobili (ad esempio computer portatili, telefoni cellulari e PDA), che sono generalmente a più alto rischio rispetto ai dispositivi non portatili (ad esempio, computer desktop presso le strutture dell'organizzazione del fornitore)?	I clienti hanno il controllo e la responsabilità dei propri dati e degli asset media associati. È responsabilità del cliente gestire la sicurezza dei dispositivi mobili e l'accesso ai propri contenuti.

Gruppo di	CID	Domande sulla	Risposta AWS
Risorse umane *Accordi di riservatezza*	HRS-06.1	I requisiti per gli accordi di non divulgazione o di riservatezza che riflettono le esigenze dell'organizzazione di protezione dei dati e i dettagli operativi sono identificati, documentati e riesaminati a intervalli pianificati?	L'ufficio legale di Amazon gestisce e rivede periodicamente l'accordo di riservatezza Amazon in modo da riflettere le esigenze aziendali di AWS.
Risorse umane *Ruoli/ responsabilità*	HRS-07.1	Ai tenant viene fornito un documento di definizione dei ruoli che chiarisce le responsabilità amministrative di AWS rispetto a quelle del tenant?	Nei whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS) e AWS Risk and Compliance (Rischio e conformità AWS) vengono forniti dettagli su ruoli e responsabilità di AWS e su quelle dei clienti. I whitepaper sono disponibili all'indirizzo http://aws.amazon.com/security e http://aws.amazon.com/compliance.
Risorse umane *Utilizzo accettabile*	HRS-08.1	Viene fornita la documentazione sulle modalità di utilizzo dei dati e/o dei metadati dei tenant e di accesso a tali dati?	AWS dispone di una policy di controllo dell'accesso che viene revisionata e aggiornata annualmente (o quando si verificano modifiche importanti al sistema in grado di influire sulla policy). La policy affronta argomenti come scopo, ambito, ruoli, responsabilità e coinvolgimento gestionale. AWS si avvale del principio del privilegio minimo, consentendo agli utenti soltanto l'accesso necessario per svolgere le proprie mansioni lavorative. I clienti hanno il controllo e la responsabilità dei propri dati e degli asset media associati. È responsabilità del cliente gestire la sicurezza dei dispositivi mobili e l'accesso ai propri contenuti. Per ulteriori informazioni, fare riferimento allo standard ISO 27001 e al codice di condotta previsto dalla norma ISO 27018. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità alla certificazione ISO 27001 e ISO 27018.
	HRS-08.2	Vengono raccolti o creati metadati relativi all'uso dei dati dei tenant attraverso l'utilizzo di tecnologie di ispezione (motori di ricerca e così via)?	
	HRS-08.3	Ai tenant è permesso di scegliere di non rendere i propri dati/metadati accessibili tramite tecnologie di ispezione?	

Gruppo di	CID	Domande sulla	Risposta AWS
Risorse umane *Formazione /sensibilizza-zione*	HRS-09.1	Viene fornito un programma di formazione per la sensibilizzazione alla sicurezza formale basato su ruoli per i problemi di accesso e gestione dei dati relativi al cloud (ad esempio, multi-tenancy, nazionalità, implicazioni e conflitti di interesse della separazione dei compiti del modello di erogazione cloud) a tutte le persone che hanno accesso ai dati dei tenant?	In linea con lo standard ISO 27001, tutti i dipendenti AWS completano una formazione periodica sulla sicurezza delle informazioni per la quale è richiesta conferma di completamento. Vengono effettuati controlli in materia di conformità a cadenza periodica per assicurarsi che i dipendenti comprendano e seguano le policy definite. Le responsabilità e i ruoli AWS vengono verificati da revisori esterni indipendenti durante i controlli per la conformità con gli standard SOC, PCI DSS, ISO 27001 e FedRAMP.
	HRS-09.2	Gli amministratori e i gestori dei dati sono adeguatamente istruiti sulle proprie responsabilità legali in materia di sicurezza e integrità dei dati?	
Risorse umane *Responsabilità dell'utente*	HRS-10.1	Tutti gli utenti sono consapevoli delle proprie responsabilità di mantenere la sensibilizzazione e la conformità a policy, procedure, standard di sicurezza pubblicati e ai requisiti normativi applicabili?	AWS ha implementato vari metodi di comunicazione interna a livello globale per aiutare i dipendenti a comprendere i loro ruoli e le responsabilità individuali e a comunicare eventi significativi in modo tempestivo. Questi metodi includono programmi di orientamento e formazione per i neo-assunti, nonché messaggi di posta elettronica e la pubblicazione di informazioni attraverso l'intranet di Amazon. Fare riferimento allo standard ISO 27001, appendice A, domini 7 e 8. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001. Il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security, fornisce ulteriori informazioni.
	HRS-10.2	Gli utenti sono consapevoli delle proprie responsabilità di mantenere un ambiente di lavoro sicuro e protetto?	
	HRS-10.3	Gli utenti sono consapevoli delle proprie responsabilità di lasciare le apparecchiature non presidiate in modo sicuro?	

Gruppo di	CID	Domande sulla	Risposta AWS
Risorse umane *Area di lavoro*	HRS-11.1	Policy e procedure di gestione dei dati affrontano i conflitti di interesse a livello di servizio e tenant?	Le policy di gestione dei dati AWS sono conformi allo standard ISO 27001. Fare riferimento allo standard ISO 27001, appendice A, domini 8 e 9. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001. Nei rapporti AWS SOC vengono forniti dettagli aggiuntivi sulle attività di controllo specifiche eseguite da AWS per impedire l'accesso non autorizzato alle risorse di AWS. AWS ha identificato categorie di eventi revisionabili sui sistemi e i dispositivi all'interno del sistema AWS. I team di servizio configurano le caratteristiche di revisione per registrare in modo continuo gli eventi relativi alla sicurezza in base ai requisiti. I record di controllo contengono una serie di elementi che supportano i requisiti di analisi necessari. Inoltre i record di controllo sono a disposizione del team di sicurezza AWS o di altri team autorizzati per eseguire ispezioni o analisi su richiesta e in risposta a eventi che riguardano la sicurezza o che hanno un'influenza sulle attività aziendali.
	HRS-11.2	Policy e procedure di gestione dei dati comprendono una funzione di integrità software o antimanomissione per l'accesso non autorizzato ai dati dei tenant?	
	HRS-11.3	L'infrastruttura di gestione delle macchine virtuali include una funzione di integrità software o antimanomissione per rilevare modifiche alla build/configurazione della macchina virtuale?	
Identity & Access Management *Accesso agli strumenti di controllo*	IAM-01.1	L'accesso ai sistemi di gestione della sicurezza delle informazioni viene limitato, registrato e monitorato (ad esempio hypervisor, firewall, scanner di vulnerabilità, sniffer di rete, API e così via)?	In linea con gli standard ISO 27001, AWS ha definito policy formali e procedure atte a delineare gli standard minimi per l'accesso logico alle risorse AWS. I rapporti SOC di AWS illustrano i controlli in atto per la gestione del provisioning degli accessi alle risorse AWS. Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security.

Gruppo di	CID	Domande sulla	Risposta AWS
	IAM-01.2	L'accesso con privilegi (livello amministratore) ai sistemi di gestione della sicurezza delle informazioni viene monitorato e registrato?	AWS ha identificato categorie di eventi revisionabili sui sistemi e i dispositivi all'interno del sistema AWS. I team di servizio configurano le caratteristiche di revisione per registrare in modo continuo gli eventi relativi alla sicurezza in base ai requisiti. Il sistema di storage del log è progettato per offrire un servizio altamente scalabile e disponibile che aumenta in modo automatico la capacità contemporaneamente alla crescita della richiesta di storage del log. I record di controllo contengono una serie di elementi che supportano i requisiti di analisi necessari. Inoltre i record di controllo sono a disposizione del team di sicurezza AWS o di altri team autorizzati per eseguire ispezioni o analisi su richiesta e in risposta a eventi che riguardano la sicurezza o che hanno un'influenza sulle attività aziendali. Il personale incaricato che fa parte dei team AWS riceve avvisi automatici in caso di errore nell'elaborazione di un controllo. Errori di fallimento di un controllo comprendono ad esempio errori software/hardware. Quando riceve l'avviso, il personale reperibile invia un ticket relativo al problema e segue l'evento fino alla sua risoluzione. I processi di log e monitoraggio AWS vengono verificati da revisori indipendenti di terze parti nell'ambito della conformità continua con gli standard SOC, PCI DSS, ISO 27001 e FedRAMP.
Identity & Access Management *Policy di accesso degli utenti*	IAM-02.1	Sono stati implementati controlli per garantire la rimozione tempestiva dell'accesso ai sistemi non più necessario per motivi di lavoro?	Nei rapporti AWS SOC vengono fornite ulteriori informazioni sulla revoca dell'accesso utente. Ulteriori informazioni sono inoltre fornite nel whitepaper sulla sicurezza AWS, sezione "Employee Lifecycle" (Ciclo di vita dei dipendenti). Per ulteriori informazioni, fare riferimento allo standard ISO 27001, appendice A, dominio 9. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	IAM-02.2	Vengono forniti parametri per tenere traccia della velocità con cui si è in grado di rimuovere l'accesso ai sistemi non più necessario per motivi di lavoro?	

Gruppo di	CID	Domande sulla	Risposta AWS
Identity & Access Management *Accesso porte di diagnostica/ configurazione*	IAM-03.1	Vengono utilizzate reti sicure dedicate per fornire accesso alla gestione per l'infrastruttura del servizio cloud?	I controlli esistenti limitano l'accesso ai sistemi e ai dati e prevedono che l'accesso ai sistemi o ai dati sia limitato e monitorato secondo la policy di accesso AWS. I dati dei clienti e le istanze server, inoltre, sono isolati a livello logico da quelli di altri clienti per impostazione predefinita. I controlli sugli accessi da parte di utenti con privilegi sono verificati da un revisore indipendente durante i controlli AWS SOC, ISO 27001, PCI, ITAR e FedRAMP.
Identity & Access Management *Policy e procedure*	IAM-04.1	È stata implementata la gestione e l'archiviazione dell'identità di tutto il personale che ha accesso all'infrastruttura IT, compreso il livello di accesso?	
	IAM-04.2	È stata implementata la gestione e l'archiviazione dell'identità degli utenti che hanno accesso alla rete, compreso il livello di accesso?	
Identity & Access Management *Separazione dei compiti*	IAM-05.1	Ai tenant viene fornita la documentazione su come mantenere la separazione dei compiti all'interno dell'offerta di servizi cloud?	I clienti mantengono la capacità di gestire le separazioni dei compiti delle loro risorse AWS. Internamente, AWS è conforme agli standard ISO 27001 per la gestione della separazione dei compiti. Per ulteriori dettagli, fare riferimento allo standard ISO 27001, appendice A, dominio 6. AWS è stato convalidato e certificato da un auditor indipendente per confermare la conformità allo standard di certificazione ISO 27001.
Identity & Access Management *Restrizione dell'accesso al codice sorgente*	IAM-06.1	Sono presenti controlli per impedire l'accesso non autorizzato all'applicazione, al programma o al codice sorgente oggetto e per garantire che l'accesso sia limitato solo al personale autorizzato?	In linea con gli standard ISO 27001, AWS ha definito policy formali e procedure atte a delineare gli standard minimi per l'accesso logico alle risorse AWS. I rapporti SOC di AWS illustrano i controlli in atto per la gestione del provisioning degli accessi alle risorse AWS. Per ulteriori dettagli, consultare il whitepaper AWS Overview of Security Processes (Panoramica sulle procedure di sicurezza AWS), disponibile all'indirizzo http://aws.amazon.com/security.
	IAM-06.2	Sono presenti controlli per impedire l'accesso non autorizzato all'applicazione, al programma o al codice sorgente oggetto dei tenant e per garantire che l'accesso sia limitato solo al personale autorizzato?	

Gruppo di	CID	Domande sulla	Risposta AWS
Identity & Access Management *Accesso di terze parti*	IAM-07.1	Viene fornita la funzionalità di disaster recovery multi-failure?	AWS offre ai clienti la flessibilità necessaria per avviare istanze e memorizzare dati all'interno di più regioni geografiche e in più zone di disponibilità all'interno di ogni regione. Ciascuna zona di disponibilità è progettata per essere indipendente dai guasti delle altre zone. In caso di problemi, i processi automatizzati spostano il traffico dati del cliente dall'area colpita. I rapporti AWS SOC forniscono ulteriori dettagli. Per ulteriori informazioni, fare riferimento allo standard ISO 27001, appendice A, dominio 15. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità alla certificazione ISO 27001.
	IAM-07.2	La continuità del servizio con i fornitori a monte viene monitorata in caso di inadempienza del fornitore?	
	IAM-07.3	Si dispone di più di un fornitore per ogni servizio da cui si dipende?	
	IAM-07.4	Viene fornito accesso ai riepiloghi di continuità e ridondanza operativa, compresi i servizi da cui si dipende?	
	IAM-07.5	Ai tenant è offerta la possibilità di dichiarare una situazione grave?	
	IAM-07.6	Viene fornita un'opzione di failover attivata dal tenant?	
	IAM-07.7	I piani di ridondanza e continuità dell'azienda vengono condivisi con i tenant?	
Identity & Access Management *Restrizione/ autorizzazione dell'accesso utente*	IAM-08.1	La modalità di autorizzazione e approvazione dell'accesso ai dati del tenant viene documentata?	I clienti AWS detengono il controllo e la proprietà dei propri dati. I controlli esistenti limitano l'accesso ai sistemi e ai dati e fanno sì che l'accesso venga monitorato e sottoposto a restrizioni. Inoltre, i dati dei clienti e le istanze dei server sono isolati logicamente da quelli di altri clienti per impostazione predefinita. I controlli sugli accessi da parte di utenti con privilegi sono verificati da un revisore indipendente durante i controlli AWS SOC, ISO 27001, PCI, ITAR e FedRAMP.
	IAM-08.2	Si utilizza un metodo specifico per allineare le metodologie di classificazione dei dati di tenant e fornitore ai fini di controllo degli accessi?	

Gruppo di	CID	Domande sulla	Risposta AWS
Identity & Access Management *Autorizzazione dell'accesso utente*	IAM-09.1	La direzione esegue il provisioning delle autorizzazioni e delle limitazioni dell'accesso utente (ad esempio di dipendenti, appaltatori, clienti (tenant), partner commerciali e/o fornitori) prima del loro accesso ai dati e a qualsiasi applicazione, sistema dell'infrastruttura e componente di rete di proprietà o gestito (fisico e virtuale)?	Gli identificatori unici dell'utente vengono creati nell'ambito del processo del flusso di lavoro che riguarda l'inserimento del personale all'interno del sistema di gestione delle risorse umane AWS. Il processo di fornitura dei dispositivi aiuta a garantire l'assegnazione di identificatori unici. Entrambi i processi comportano l'approvazione da parte del responsabile per determinare l'account utente sul dispositivo. Gli autenticatori iniziali vengono assegnati direttamente all'utente e ai dispositivi nell'ambito del processo di fornitura. Gli utenti interni possono associare le chiavi pubbliche SSH al proprio account. Gli autenticatori dell'account del sistema vengono assegnati al richiedente nell'ambito del processo di creazione dell'account dopo che l'identità del richiedente è stata verificata.
	IAM-09.2	Viene fornito l'accesso utente su richiesta (ad esempio a dipendenti, appaltatori, clienti (tenant), partner commerciali e/o fornitori) ai dati e a qualsiasi applicazione, sistema dell'infrastruttura e componente di rete di proprietà o gestito (fisico e virtuale)?	AWS dispone di controlli per gestire la minaccia di accessi non autorizzati a informazioni privilegiate. Tutte le certificazioni e le attestazioni di terze parti effettuano una valutazione dei controlli di prevenzione e rilevazione degli accessi logici. Valutazioni periodiche del rischio, inoltre, sono incentrate sulle modalità di controllo e monitoraggio dell'accesso a informazioni privilegiate.
Identity & Access Management *Analisi degli accessi utente*	IAM-10.1	Viene richiesta almeno la certificazione annuale dei diritti per tutti gli utenti e gli amministratori di sistema (esclusivi di utenti gestiti dai tenant)?	In linea con lo standard ISO 27001, tutte le autorizzazioni concesse vengono riesaminate periodicamente; è richiesta l'approvazione specifica, altrimenti l'accesso alla risorsa viene revocato automaticamente. I controlli specifici delle analisi degli accessi utente sono descritti specificatamente nei rapporti SOC. Le eccezioni nei controlli dei diritti utente sono documentate nei rapporti SOC. Per ulteriori informazioni, fare riferimento agli standard ISO 27001, appendice A, dominio 9. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	IAM-10.2	Se viene rilevato che degli utenti non dispongono di diritti appropriati, vengono registrate tutte le azioni di correzione e di certificazione?	
	IAM-10.3	I rapporti di correzione e certificazione dei diritti utente verranno condivisi con i tenant nel caso in cui sia stato consentito un accesso improprio ai dati dei tenant?	

Gruppo di	CID	Domande sulla	Risposta AWS
Identity & Access Management *Revoca dell'accesso utente*	IAM-11.1	Il deprovisioning, la revoca o la modifica tempestiva dell'accesso utente ai sistemi delle organizzazioni, agli asset delle informazioni e ai dati sono implementati a ogni cambiamento di stato di dipendenti, appaltatori, clienti, partner commerciali o terze parti coinvolte?	L'accesso è revocato automaticamente quando il profilo di un dipendente viene eliminato dal sistema delle risorse umane di Amazon. Quando una funzione lavorativa del dipendente cambia, l'accesso deve essere esplicitamente approvato per la risorsa o sarà revocato automaticamente. Nei rapporti AWS SOC vengono fornite ulteriori informazioni sulla revoca dell'accesso utente. Ulteriori informazioni sono inoltre fornite nel whitepaper sulla sicurezza AWS, sezione "Employee Lifecycle" (Ciclo di vita dei dipendenti). Per ulteriori informazioni, fare riferimento allo standard ISO 27001, appendice A, dominio 9. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	IAM-11.2	Qualsiasi cambiamento di stato dell'accesso utente è destinato a includere la cessazione del rapporto di lavoro, del contratto o dell'accordo, il cambiamento del posto di lavoro o il trasferimento all'interno dell'organizzazione?	
Identity & Access Management *Credenziali ID utente*	IAM-12.1	L'utilizzo di soluzioni SSO (Single Sign On) basate sul cliente, o l'integrazione con esse, è supportato nel servizio offerto?	Il servizio AWS Identity and Access Management (IAM) fornisce la federazione delle identità alla console di gestione AWS. L'autenticazione a più fattori è una funzionalità opzionale utilizzabile dai clienti. Per ulteriori dettagli, consultare il sito Web AWS all'indirizzo http://aws.amazon.com/mfa. Il servizio AWS Identity and Access Management (IAM) supporta la federazione delle identità per l'accesso delegato alla Console di gestione AWS o alle API AWS. Con la federazione delle identità, le identità esterne (utenti federati) possono accedere in modo sicuro alle risorse dell'account AWS senza necessità di creare utenti IAM. Tali identità esterne possono provenire dal provider delle identità aziendali (ad esempio Microsoft Active Directory oppure da AWS Directory Service) oppure da un provider di identità Web, come Amazon Cognito, Login with Amazon, Facebook, Google o qualsiasi provider compatibile con OpenID Connect (OIDC).
	IAM-12.2	Sono utilizzati standard aperti per delegare le funzionalità di autenticazione ai tenant?	
	IAM-12.3	Gli standard della federazione delle identità (SAML, SPML, WS-Federation e così via) sono supportati come mezzo di autenticazione/autorizzazione degli utenti?	
	IAM-12.4	Si dispone di una funzionalità Policy Enforcement Point (ad esempio, XACML) per far rispettare i vincoli giuridici regionali e delle policy in materia di accesso degli utenti?	

Gruppo di	CID	Domande sulla	Risposta AWS
	IAM-12.5	È stato implementato un sistema di gestione delle identità (che consenta la classificazione dei dati di un tenant) per consentire accesso ai dati basato sia sul ruolo sia sul contesto?	
	IAM-12.6	Ai tenant vengono fornite complesse opzioni di autenticazione (multifattore) (certificati digitali, token, biometrica e così via) per l'accesso degli utenti?	
	IAM-12.7	Ai tenant è permesso utilizzare servizi di garanzia delle identità di terze parti?	
	IAM-12.8	È supportata l'applicazione di policy relative alle password (lunghezza minima, durata, cronologia, complessità) e al blocco degli account (limite per il blocco, durata del blocco)?	AWS Identity and Access Management (IAM) consente ai clienti di controllare in modo sicuro l'accesso ai servizi e alle risorse AWS per gli utenti. Ulteriori informazioni su IAM sono disponibili nel sito Web, all'indirizzo https://aws.amazon.com/iam/. Nei rapporti AWS SOC vengono forniti dettagli sulle attività di controllo specifiche eseguite da AWS.
	IAM-12.9	Si consente ai tenant/clienti di definire policy relative alle password e al blocco degli account per i propri account?	
	IAM-12.10	È supportata la possibilità di forzare modifiche delle password alla prima connessione?	
	IAM-12.11	Sono stati implementati meccanismi di sblocco degli account che sono stati bloccati (ad esempio self-service tramite e-mail, domande di recupero definite, sblocco manuale)?	

Gruppo di	CID	Domande sulla	Risposta AWS
Identity & Access Management *Accesso ai programmi di utilità*	IAM-13.1	I programmi di utilità in grado di gestire in modo significativo le partizioni virtualizzate (ad esempio arresto, clone e così via) sono limitati e monitorati in modo appropriato?	In linea con gli standard ISO 27001, le utilità di sistema sono opportunamente limitate e monitorate. Nei rapporti AWS SOC vengono forniti dettagli sulle attività di controllo specifiche eseguite da AWS. Per ulteriori dettagli, consultare il whitepaper AWS Overview of Security Processes (Panoramica sulle procedure di sicurezza AWS) disponibile all'indirizzo http://aws.amazon.com/security.
	IAM-13.2	È possibile rilevare gli attacchi che prendono di mira direttamente l'infrastruttura virtuale (ad esempio shimming, Blue Pill, Hyper jumping e così via)?	
	IAM-13.3	Gli attacchi che prendono di mira l'infrastruttura virtuale vengono prevenuti con controlli tecnici?	
Sicurezza infrastrutturale e della virtualizzazione *Log di controllo/ rilevamento delle intrusioni*	IVS-01.1	Sono stati implementati strumenti di rilevamento delle intrusioni di rete (IDS) e di integrità dei file (host) per facilitare il rilevamento tempestivo, le indagini tramite analisi delle cause principali e la risposta agli eventi imprevisti?	Il programma di risposta ai problemi AWS (rilevamento, indagine e risposta ai problemi) è stato sviluppato in conformità allo standard ISO 27001 e le utilità di sistema sono opportunamente limitate e monitorate. Nei rapporti AWS SOC vengono fornite ulteriori informazioni sui controlli esistenti per limitare l'accesso al sistema. Per ulteriori dettagli, consultare il whitepaper AWS Overview of Security Processes (Panoramica sulle procedure di sicurezza AWS), disponibile all'indirizzo http://aws.amazon.com/security.
	IVS-01.2	L'accesso utente fisico e logico ai log di controllo è limitato al personale autorizzato?	
	IVS-01.3	Si può dimostrare che è stata eseguita la mappatura di due diligence dei regolamenti e degli standard per controlli/architettura/processi?	
	IVS-01.4	I log di controllo sono archiviati e conservati centralmente?	In linea con gli standard ISO 27001, i sistemi informatici di AWS utilizzano clock di sistema interni sincronizzati tramite NTP (Network

Gruppo di	CID	Domande sulla	Risposta AWS
	IVS-01.5	I log di controllo sono verificati periodicamente per individuare eventi legati alla sicurezza (ad esempio con strumenti automatizzati)?	Time Protocol). AWS è stato convalidato e certificato da un auditor indipendente per confermare la conformità allo standard di certificazione ISO 27001. AWS utilizza sistemi di monitoraggio automatizzati per offrire un alto livello di prestazioni e disponibilità del servizio. Il monitoraggio proattivo è disponibile attraverso una varietà di strumenti online sia per uso interno che per uso esterno. I sistemi all'interno di AWS sono altamente strumentati per monitorare i parametri operativi chiave. Gli allarmi sono configurati in modo da inviare notifiche al personale che si occupa del funzionamento e della gestione nel momento in cui vengono superate le soglie di notifica sui parametri operativi chiave. Viene utilizzata una pianificazione della reperibilità in modo che il personale sia sempre disponibile per rispondere ai problemi operativi. Questa pianificazione comprende un sistema cercapersone in modo che gli allarmi siano comunicati in modo rapido e affidabile al personale operativo. Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security.
Sicurezza infrastrutturale e della virtualizzazione *Rilevamento delle modifiche*	IVS-02.1	Sono disponibili log e avvisi per le eventuali modifiche apportate alle immagini di macchine virtuali, indipendentemente dal loro stato di funzionamento (ad esempio inattive, spente o operative)?	Ai clienti vengono assegnate macchine virtuali nell'ambito del servizio EC2. I clienti mantengono il controllo su quali risorse vengono utilizzate e su dove le risorse risiedono. Per ulteriori dettagli, consultare il sito Web AWS all'indirizzo http://aws.amazon.com.
	IVS-02.2	Le modifiche apportate alle macchine virtuali o lo spostamento di un'immagine e la successiva convalida dell'integrità dell'immagine sono resi immediatamente disponibili ai clienti tramite mezzi elettronici (ad esempio portali o avvisi)?	

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza infrastrutturale e della virtualizzazione *Sincronizza-zione dell'orologio*	IVS-03.1	Viene utilizzato un protocollo servizio-tempo sincronizzato (ad esempio NTP) per garantire che tutti i sistemi abbiano un riferimento temporale comune?	In linea con gli standard ISO 27001, i sistemi informatici di AWS utilizzano clock di sistema interni sincronizzati tramite NTP (Network Time Protocol). AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
Sicurezza infrastrutturale e della virtualizzazione *Pianificazione di capacità/ risorse*	IVS-04.1	Viene fornita la documentazione relativa ai livelli di richieste in eccesso dei sistemi (ad esempio rete, storage, memoria, I/O e così via) gestiti e in quali circostanze/scenari?	Per ulteriori informazioni sui limiti dei servizi AWS e su come richiedere un aumento per servizi specifici, consultare il sito Web AWS all'indirizzo http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html. AWS gestisce i dati di capacità e utilizzo in conformità allo standard ISO 27001. AWS è stato convalidato e certificato da un auditor indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	IVS-04.2	Viene limitato l'utilizzo delle capacità di richieste di memoria in eccesso presenti nell'hypervisor?	
	IVS-04.3	I requisiti di capacità del sistema tengono conto delle esigenze di capacità attuali, previste e anticipate di tutti i sistemi utilizzati per fornire i servizi ai tenant?	
	IVS-04.4	Si esegue il monitoraggio e l'ottimizzazione delle prestazioni del sistema per soddisfare in maniera continuativa i requisiti normativi, contrattuali e aziendali di tutti i sistemi utilizzati per fornire servizi ai tenant?	

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza infrastrutturale e della virtualizzazione *Gestione - gestione delle vulnerabilità*	IVS-05.1	Si dispone di strumenti o servizi di valutazione delle vulnerabilità di sicurezza che tengano conto delle tecnologie di virtualizzazione in uso (ad esempio ottimizzati per la virtualizzazione)?	Attualmente, Amazon EC2 utilizza una versione dell'hypervisor Xen con elevata personalizzazione. L'hypervisor viene sottoposto a valutazioni regolari sulle vulnerabilità nuove ed esistenti e sui vettori di attacco da parte di team di intrusione interni ed esterni ed è idoneo a mantenere un forte isolamento tra macchine virtuali ospiti. La sicurezza dell'hypervisor AWS Xen viene verificata regolarmente da revisori indipendenti durante valutazioni e controlli. Le scansioni per individuare vulnerabilità interne ed esterne vengono eseguite sul sistema operativo host, sull'applicazione Web e sui database nell'ambiente AWS utilizzando diversi strumenti. Le procedure di scansione e correzione delle vulnerabilità vengono revisionate periodicamente nell'ambito della conformità continua AWS con gli standard PCI DSS e FedRAMP.
Sicurezza infrastrutturale e della virtualizzazione *Sicurezza di rete*	IVS-06.1	Per l'offerta IaaS, ai clienti viene fornita una guida su come creare un'architettura di sicurezza stratificata equivalente utilizzando la soluzione virtualizzata?	Il sito Web AWS fornisce indicazioni sulla creazione di un'architettura di sicurezza stratificata in diversi whitepaper disponibili tramite il sito Web AWS pubblico, all'indirizzo http://aws.amazon.com/documentation/.
	IVS-06.2	Vengono eseguiti aggiornamenti periodici dei diagrammi dell'architettura di rete che includono i flussi di dati tra domini/zone di sicurezza?	I dispositivi di protezione di confine che impiegano serie di regole, ACL (access control lists, liste di controllo degli accessi) e configurazioni implementano il flusso di dati tra i fabric di rete. Amazon dispone di numerosi fabric di rete, ognuno separato da dispositivi che controllano il flusso di informazioni tra i fabric, che viene definito da autorizzazioni approvate, sotto forma di liste di controllo accessi (ACL), che a loro volta si trovano all'interno dei dispositivi. Questi dispositivi controllano il flusso di informazioni tra i fabric come ordinato dalle liste. Le liste di controllo degli accessi sono definite e approvate dal personale preposto e gestite e distribuite utilizzando lo strumento di gestione ACL AWS. Il team della sicurezza delle informazioni di Amazon approva queste ACL. I set di regole sul firewall approvate e le liste di controllo
	IVS-06.3	Viene eseguita una verifica periodica dell'adeguatezza degli accessi/connettività consentiti (ad esempio regole del firewall) tra domini/zone di sicurezza all'interno della rete?	
	IVS-06.4	Si dispone di una documentazione delle liste di controllo accessi al firewall con adeguata giustificazione?	

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza infrastrutturale e della virtualizzazione *Protezione avanzata del sistema operativo e controlli di base*	IVS-07.1	Si dispone di una protezione avanzata per i sistemi operativi che consenta di fornire solo le porte, i protocolli e i servizi necessari a soddisfare le esigenze aziendali, con l'utilizzo di controlli tecnici (ossia e antivirus, monitoraggio dell'integrità dei file e log) facenti parte del loro standard o modello baseline?	accessi tra i fabric di rete limitano il flusso di informazioni ai servizi specifici del sistema informatico. Le liste di controllo accessi e i set di regole vengono verificati e approvati e trasmessi periodicamente in modo automatico ai dispositivi di protezione perimetrale (almeno ogni 24 ore) per garantire l'aggiornamento dei set di regole e delle liste di controllo accessi. La gestione della rete AWS viene verificata regolarmente da auditor indipendenti di terze parti nell'ambito dell'impegno continuo di AWS per garantire la conformità agli standard SOC, PCI DSS, ISO 27001 e FedRAMPsm. AWS implementa il privilegio minimo nei componenti dell'infrastruttura. AWS proibisce tutte le porte e i protocolli che non hanno uno scopo aziendale specifico. AWS segue un approccio rigoroso all'implementazione minima esclusivamente delle caratteristiche e delle funzioni essenziali per l'utilizzo del dispositivo. Viene eseguita la scansione della rete e le porte o protocolli in uso non necessari vengono corretti. Le scansioni per individuare vulnerabilità interne ed esterne vengono eseguite sul sistema operativo host, sull'applicazione Web e sui database nell'ambiente AWS utilizzando diversi strumenti. Le procedure di scansione e correzione delle vulnerabilità vengono revisionate periodicamente nell'ambito della conformità continua AWS con gli standard PCI DSS e FedRAMP.
Sicurezza infrastrutturale e della virtualizzazione *Ambienti di produzione/non destinati alla produzione*	IVS-08.1	Per le offerte SaaS o PaaS, ai tenant vengono forniti ambienti separati per i processi di produzione e test?	I clienti AWS mantengono la capacità e la responsabilità di creare e gestire ambienti di produzione e di test. Il sito Web AWS fornisce indicazioni sulla creazione di un ambiente utilizzando i servizi AWS, all'indirizzo http://aws.amazon.com/documentation/.
	IVS-08.2	Per l'offerta IaaS, ai tenant viene fornita una guida su come creare ambienti di produzione e test adeguati?	
	IVS-08.3	Viene effettuata la separazione logica e fisica per garantire la separazione degli ambienti di produzione e non destinati alla produzione?	I clienti AWS mantengono la responsabilità di gestire la propria segmentazione di rete conformemente ai requisiti definiti. Internamente, la segmentazione di rete AWS è conforme agli standard ISO 27001. Per ulteriori informazioni, fare riferimento allo standard ISO 27001, appendice A,

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza infrastrutturale e della virtualizzazione *Segmentazione*	IVS-09.1	Gli ambienti di rete e di sistema sono protetti da un firewall o un firewall virtuale per soddisfare i requisiti di sicurezza di azienda e cliente?	dominio 13. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	IVS-09.2	Gli ambienti di rete e di sistema sono protetti da un firewall o un firewall virtuale per soddisfare i requisiti legislativi, normativi e contrattuali?	
	IVS-09.3	Gli ambienti di rete e di sistema sono protetti da un firewall o firewall virtuale per garantire la separazione degli ambienti di produzione e non destinati alla produzione?	
	IVS-09.4	Gli ambienti di rete e di sistema sono protetti da un firewall o un firewall virtuale per garantire la protezione e l'isolamento dei dati sensibili?	
Sicurezza infrastrutturale e della virtualizzazione *Sicurezza VM - Protezione dei dati vMotion*	IVS-10.1	Si utilizzano canali di comunicazione protetti e crittografati per la migrazione di server fisici, applicazioni o dati nei server virtuali?	AWS permette ai clienti di utilizzare i propri meccanismi di crittografia per quasi tutti i servizi, inclusi S3, EBS ed EC2. Anche le sessioni VPC sono crittografate.
	IVS-10.2	Si utilizza una rete separata dalle reti impiegate per la produzione, ai fini della migrazione di server fisici, applicazioni o dati nei server virtuali?	I clienti AWS detengono il controllo e la proprietà dei propri dati. AWS offre ai clienti la possibilità di gestire e sviluppare ambienti di produzione e non destinati alla produzione. È responsabilità del cliente assicurarsi che i propri dati di produzione non vengano replicati in ambienti non destinati alla produzione.

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza infrastrutturale e della virtualizzazione *Sicurezza VMM - Protezione avanzata dell'hypervisor*	IVS-11.1	Si limita l'accesso del personale a tutte le funzioni di gestione dell'hypervisor o alle console di amministrazione dei sistemi che ospitano sistemi virtualizzati sulla base del principio del privilegio minimo e con l'ausilio di controlli tecnici (ad esempio autenticazione a due fattori, audit trail, filtro degli indirizzi IP, firewall e comunicazioni con incapsulamento TLS per le console di amministrazione)?	AWS si avvale del principio del privilegio minimo, consentendo agli utenti soltanto l'accesso necessario per svolgere le proprie mansioni lavorative. Gli account utente vengono creati per disporre dell'accesso minimo. Per accedere a livelli superiori rispetto a quello minimo è necessario ottenere l'autorizzazione adeguata. Per maggiori informazioni sui controlli sugli accessi fare riferimento ai rapporti AWS SOC.
Sicurezza infrastrutturale e della virtualizzazione *Sicurezza wireless*	IVS-12.1	Sono state stabilite policy e procedure e sono stati configurati e implementati meccanismi per la protezione del perimetro dell'ambiente di rete wireless e per limitare il traffico wireless non autorizzato?	Sono presenti policy, procedure e meccanismi per proteggere l'ambiente di rete AWS. I controlli di sicurezza AWS vengono verificati da revisori esterni indipendenti durante i controlli per la conformità con gli standard SOC, PCI DSS, ISO 27001 e FedRAMP.
	IVS-12.2	Sono state stabilite policy e procedure e sono stati implementati meccanismi per garantire l'attivazione delle impostazioni di sicurezza wireless con crittografia avanzata per l'autenticazione e la trasmissione, in sostituzione delle impostazioni predefinite del fornitore (ad esempio, chiavi di crittografia, password, stringhe community SNMP)?	

Gruppo di	CID	Domande sulla	Risposta AWS
	IVS-12.3	Sono state stabilite policy e procedure e sono stati implementati meccanismi per proteggere gli ambienti di rete wireless e rilevare la presenza di dispositivi di rete non autorizzati (rogue) per una disconnessione tempestiva dalla rete?	
Sicurezza infrastrutturale e della virtualizzazione *Architettura di rete*	IVS-13.1	I diagrammi dell'architettura di rete identificano chiaramente gli ambienti ad alto rischio e i flussi di dati che potrebbero avere ripercussioni sulla conformità legale?	I clienti AWS mantengono la responsabilità di gestire la propria segmentazione di rete conformemente ai requisiti definiti. Internamente, la segmentazione di rete AWS è conforme allo standard ISO 27001. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	IVS-13.2	Sono state applicate misure e tecniche difensive valide (ad esempio analisi approfondita dei pacchetti, limitazione del traffico e blackholing) per il rilevamento e la reazione tempestiva ad attacchi basati sulla rete associati a modelli anomali di traffico in ingresso e in uscita (ad esempio attacchi MAC spoofing e ARP poisoning) e/o attacchi Distributed Denial of Service (DDoS)?	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. Inoltre, l'ambiente di controllo AWS è soggetto a periodiche valutazioni del rischio interne ed esterne. AWS collabora con organi di certificazione esterni e revisori indipendenti per verificare e testare l'ambiente di controllo AWS nel suo insieme. I controlli di sicurezza AWS vengono verificati da revisori esterni indipendenti durante i controlli per la conformità con gli standard SOC, PCI DSS, ISO 27001 e FedRAMP.
Interoperabilità e portabilità *API*	IPY-01	Viene pubblicato un elenco di tutte le API disponibili nel servizio, con l'indicazione di quali sono standard e di quali sono invece personalizzate?	I dettagli relativi alle API AWS sono disponibili nel sito Web AWS all'indirizzo https://aws.amazon.com/documentation/. In linea con gli standard ISO 27001, AWS ha definito policy formali e procedure atte a delineare gli standard minimi per l'accesso logico alle risorse AWS. I rapporti SOC di

Gruppo di	CID	Domande sulla	Risposta AWS
Interoperabilità e portabilità *Richiesta di dati*	IPY-02	I dati non strutturati dei clienti sono disponibili su richiesta in un formato standard del settore (ad esempio .doc, .xls o .pdf)?	AWS illustrano i controlli in atto per la gestione del provisioning degli accessi alle risorse AWS. Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security.
Interoperabilità e portabilità *Policy e aspetti legali*	IPY-03.1	Vengono fornite policy e procedure (ossia contratti sul livello di servizio) che disciplinano l'utilizzo delle API ai fini dell'interoperabilità tra il servizio AWS e le applicazioni di terze parti?	
	IPY-03.2	Vengono fornite policy e procedure (ossia contratti sul livello di servizio) che disciplinano la migrazione dei dati delle applicazioni da e verso il servizio?	I clienti detengono il controllo e la proprietà dei propri contenuti. I clienti possono scegliere come migrare le applicazioni e i contenuti da e verso la piattaforma AWS, a loro discrezione.
Interoperabilità e portabilità *Protocolli di rete standardizzati*	IPY-04.1	È possibile importare ed esportare dati e gestire servizi su protocolli di rete standardizzati, accettati nel settore e sicuri (ad esempio, con testo crittografato e autenticazione)?	AWS permette ai clienti di spostare i dati all'interno e fuori dallo storage AWS in base alle necessità. Per ulteriori informazioni sulle opzioni di storage, fare riferimento a http://aws.amazon.com/choosing-a-cloud-platform.
	IPY-04.2	Ai clienti (tenant) viene fornita una documentazione che descriva nei dettagli gli standard dei protocolli di rete pertinenti relativi a interoperabilità e portabilità?	
Interoperabilità e portabilità *Virtualizzazione*	IPY-05.1	Per garantire l'interoperabilità si utilizzano una piattaforma di virtualizzazione riconosciuta dal settore e formati di virtualizzazione standard (ad esempio, OVF)?	Attualmente, Amazon EC2 utilizza una versione dell'hypervisor Xen con elevata personalizzazione. L'hypervisor viene sottoposto a valutazioni regolari sulle vulnerabilità nuove ed esistenti e sui vettori di attacco da parte di team di intrusione interni ed esterni ed è idoneo a mantenere un forte isolamento tra macchine virtuali ospiti.

Gruppo di	CID	Domande sulla	Risposta AWS
	IPY-05.2	I clienti hanno la possibilità di esaminare le modifiche personalizzate e documentate apportate agli hypervisor in uso e tutti i punti di aggancio per la virtualizzazione specifici per soluzione?	La sicurezza dell'hypervisor AWS Xen viene verificata regolarmente da revisori indipendenti durante valutazioni e controlli. Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security.
Sicurezza dei dispositivi mobili *Anti-malware*	MOS-01	La formazione di sensibilizzazione alla sicurezza delle informazioni include una formazione anti-malware specifica per dispositivi mobili?	Il programma, i processi e le procedure AWS per la gestione del software antivirus/malware sono conformi agli standard ISO 27001. Per ulteriori informazioni, fare riferimento allo standard ISO 27001, appendice A, dominio 12.
Sicurezza dei dispositivi mobili *Store di applicazioni*	MOS-02	Gli elenchi di store approvati di applicazioni per dispositivi mobili che accedono ai dati e/o ai sistemi aziendali ed effettuano operazioni di archiviazione sono documentati e disponibili?	AWS ha stabilito un framework e policy di sicurezza delle informazioni e ha efficacemente integrato il framework certificabile ISO 27001 basato sui controlli ISO 27002, sui criteri Trust Services Principles dell'American Institute of Certified Public Accountants (AICPA), sul PCI DSS v3.1 e sulla National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). I clienti hanno il controllo e la responsabilità dei propri dati e degli asset media associati. È responsabilità del cliente gestire la sicurezza dei dispositivi mobili e l'accesso ai propri contenuti.
Sicurezza dei dispositivi mobili *Applicazioni approvate*	MOS-03	È presente una funzionalità Policy Enforcement Point (ad esempio, XACML) per garantire che sui dispositivi mobili vengano caricate solo le applicazioni e i relativi store approvati?	
Sicurezza dei dispositivi mobili *Software approvato per BYOD*	MOS-04	La policy e la formazione per BYOD (Bring Your Own Device) indicano con precisione quali applicazioni e relativi store sono approvati per i dispositivi BYOD?	
Sicurezza dei dispositivi mobili *Sensibilizza-zione e formazione*	MOS-05	La formazione per i dipendenti include una policy documentata sui dispositivi mobili che indica con precisione sia i dispositivi mobili che i requisiti e l'utilizzo accettato per tali dispositivi?	

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza dei dispositivi mobili *Servizi basati sul cloud*	MOS-06	È disponibile un elenco documentato di servizi preapprovati basati su cloud che è consentito utilizzare per gestire e archiviare dati aziendali sui dispositivi mobili?	
Sicurezza dei dispositivi mobili *Compatibilità*	MOS-07	È stato implementato un processo di convalida delle applicazioni documentato per testare dispositivi, sistemi operativi e compatibilità delle applicazioni?	
Sicurezza dei dispositivi mobili *Idoneità dei dispositivi*	MOS-08	È presente una policy BYOD che indica i dispositivi e i requisiti di idoneità per l'utilizzo BYOD?	
Sicurezza dei dispositivi mobili *Inventario dei dispositivi*	MOS-09	Viene mantenuto un inventario di tutti i dispositivi mobili utilizzati per archiviare e accedere ai dati aziendali che includa lo stato dei dispositivi (sistema operativo e livelli di patch, dispositivi persi o disattivati, assegnatari dei dispositivi)?	
Sicurezza dei dispositivi mobili *Gestione dei dispositivi*	MOS-10	È presente una soluzione di gestione centralizzata dei dispositivi mobili distribuita su tutti i dispositivi mobili autorizzati ad archiviare, trasmettere o elaborare i dati aziendali?	
Sicurezza dei dispositivi mobili *Crittografia*	MOS-11	La policy sui dispositivi mobili richiede l'utilizzo della crittografia, per l'intero dispositivo o per i dati considerati sensibili, applicabile mediante controlli tecnologici per tutti i dispositivi mobili?	

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza dei dispositivi mobili *Jailbreak e root*	MOS-12.1	La policy sui dispositivi mobili vieta la circonvenzione dei controlli di sicurezza integrati nei dispositivi mobili (ad esempio, jailbreak o root)?	
	MOS-12.2	I dispositivi o il sistema di gestione centralizzata dei dispositivi dispongono di controlli di prevenzione e rilevazione che impediscono la circonvenzione dei controlli di sicurezza integrati?	
Sicurezza dei dispositivi mobili *Note legali*	MOS-13.1	La policy BYOD indica con precisione le aspettative relative a privacy, requisiti in caso di contenzioso, E-Discovery e conservazione a fini legali?	I clienti hanno il controllo e la responsabilità dei propri dati e degli asset media associati. È responsabilità del cliente gestire la sicurezza dei dispositivi mobili e l'accesso ai propri contenuti.
	MOS-13.2	I dispositivi o il sistema di gestione centralizzata dei dispositivi dispongono di controlli di prevenzione e rilevazione che impediscono la circonvenzione dei controlli di sicurezza integrati?	
Sicurezza dei dispositivi mobili *Schermata di blocco*	MOS-14	Per i dispositivi BYOD e aziendali è richiesta e attivata una schermata di blocco automatica gestita da controlli tecnici?	
Sicurezza dei dispositivi mobili *Sistemi operativi*	MOS-15	Tutte le modifiche apportate ai sistemi operativi, ai livelli di patch e alle applicazioni dei dispositivi mobili vengono amministrate mediante processi aziendali di gestione delle modifiche?	

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza dei dispositivi mobili *Password*	MOS-16.1	Si dispone di policy sulle password per i dispositivi mobili aziendali e/o BYOD?	
	MOS-16.2	Le policy sulle password vengono applicate mediante controlli tecnici (ad esempio, MDM)?	
	MOS-16.3	Le policy sulle password vietano di modificare i requisiti di autenticazione (ad esempio, lunghezza di password/PIN) mediante dispositivi mobili?	
Sicurezza dei dispositivi mobili *Policy*	MOS-17.1	È presente una policy che richiede agli utenti BYOD di eseguire il backup di determinati dati aziendali?	
	MOS-17.2	È presente una policy che richiede agli utenti BYOD di vietare l'utilizzo di store di applicazioni non approvati?	
	MOS-17.3	È presente una policy che richiede agli utenti BYOD di utilizzare software anti-malware (se supportato)?	
Sicurezza dei dispositivi mobili *Cancellazione remota*	MOS-18.1	Il reparto IT è in grado di eseguire la cancellazione, anche remota, dei dati aziendali su tutti i dispositivi BYOD accettati dall'azienda?	
	MOS-18.2	Il reparto IT è in grado di eseguire la cancellazione, anche remota, dei dati aziendali su tutti i dispositivi BYOD assegnati dall'azienda?	

Gruppo di	CID	Domande sulla	Risposta AWS
Sicurezza dei dispositivi mobili *Patch di sicurezza*	MOS-19.1	Nei dispositivi mobili sono state installate le patch di sicurezza più aggiornate dopo il rilascio generale da parte del produttore o del carrier dei dispositivi?	
	MOS-19.2	I dispositivi mobili consentono la convalida remota per permettere al personale IT dell'azienda di scaricare le patch di sicurezza più aggiornate?	
Sicurezza dei dispositivi mobili *Utenti*	MOS-20.1	La policy BYOD specifica i sistemi e i server che i dispositivi BYOD possono utilizzare e a cui sono autorizzati ad accedere?	
	MOS-20.2	La policy BYOD specifica i ruoli utente autorizzati a eseguire l'accesso mediante dispositivi BYOD?	
Gestione dei problemi di sicurezza, e-discovery e procedure forensi per il cloud *Gestione dei contatti e delle relazioni con le autorità*	SEF-01.1	Vengono mantenuti rapporti e punti di contatto con gli enti locali, conformemente ai contratti e alla normativa pertinente?	AWS mantiene contatti con organismi di settore, organizzazioni che operano nell'ambito del rischio e della conformità, enti locali e organismi di regolamentazione, come prescritto dallo standard ISO 27001. AWS è stato convalidato e certificato da un auditor indipendente per confermare la conformità allo standard di certificazione ISO 27001.
Gestione dei problemi di sicurezza, e-discovery e procedure forensi per il cloud *Gestione degli eventi imprevisti*	SEF-02.1	Si dispone di un piano di intervento documentato per gli incidenti di sicurezza?	I piani, le procedure e il programma di risposta agli incidenti AWS sono stati sviluppati in conformità allo standard ISO 27001. AWS è stato convalidato e certificato da un auditor indipendente per confermare la conformità allo standard di certificazione ISO 27001. Nei rapporti AWS SOC vengono forniti dettagli sulle attività di controllo specifiche eseguite da AWS. Tutti i dati archiviati da AWS per conto dei clienti dispongono di solide funzionalità di sicurezza e controllo dell'isolamento dei tenant. Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security.
	SEF-02.2	Le esigenze personalizzate dei tenant vengono integrate nei piani di risposta agli incidenti di sicurezza?	
	SEF-02.3	Viene pubblicato un documento su ruoli e responsabilità in cui sono specificate le proprie responsabilità e quelle dei tenant in caso di incidenti di sicurezza?	

Gruppo di	CID	Domande sulla	Risposta AWS
	SEF-02.4	I piani di risposta agli incidenti di sicurezza sono stati sottoposti a test durante l'ultimo anno?	
Gestione dei problemi di sicurezza, e-discovery e procedure forensi per il cloud *Segnalazione degli incidenti*	SEF-03.1	Il sistema SIEM (Security Information and Event Management) unisce le origini dati (log app, log firewall, log IDS, log accessi fisici e così via) per l'analisi granulare e gli avvisi?	
	SEF-03.2	Il framework di log e monitoraggio consente l'isolamento di un incidente a tenant specifici?	
Gestione dei problemi di sicurezza, e-discovery e procedure forensi per il cloud *Aspetti giuridici della risposta agli incidenti*	SEF-04.1	Il piano di risposta agli incidenti è conforme agli standard di settore per i processi e i controlli di gestione della catena di custodia giuridicamente ammissibili?	
	SEF-04.2	La capacità di risposta agli incidenti comprende l'uso di tecniche di raccolta e analisi dei dati forensi giuridicamente ammissibili?	
	SEF-04.3	È possibile supportare i contenziosi (congelamento dei dati da un determinato momento) per un tenant specifico senza congelare i dati degli altri tenant?	
	SEF-04.4	La separazione dei dati dei tenant viene applicata e attestata durante la produzione di dati in risposta a citazioni legali?	

Gruppo di	CID	Domande sulla	Risposta AWS
Gestione dei problemi di sicurezza, e-discovery e procedure forensi per il cloud *Parametri di risposta agli incidenti*	SEF-05.1	Tipi, volumi e impatti vengono monitorati e quantificati su tutti gli incidenti di sicurezza informatica?	I parametri di sicurezza AWS sono monitorati e analizzati in conformità allo standard ISO 27001. Per ulteriori dettagli, fare riferimento allo standard ISO 27001, appendice A, dominio 16. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	SEF-05.2	I dati statistici sugli incidenti della sicurezza delle informazioni vengono condivisi con i tenant su richiesta?	
Gestione della catena di distribuzione, trasparenza e responsabilità *Qualità e integrità dei dati*	STA-01.1	L'azienda esamina e si assume la responsabilità dei problemi legati alla qualità dei dati e i relativi rischi e collabora con i partner della catena di fornitura cloud per risolverli?	I clienti detengono il controllo e la proprietà della qualità dei propri dati e dei potenziali problemi di qualità che possono sorgere durante l'utilizzo dei servizi AWS. Per informazioni dettagliate su integrità dei dati e gestione dell'accesso (incluso l'accesso con privilegi minimi), fare riferimento al rapporto AWS SOC.
	STA-01.2	Sono stati definiti e implementati obiettivi di controllo per ridurre e contenere i rischi legati alla sicurezza dei dati mediante una corretta separazione di compiti, accessi basati sui ruoli e accessi con privilegi minimi per tutto il personale coinvolto nella catena di fornitura?	
Gestione della catena di distribuzione, trasparenza e responsabilità *Segnalazione degli incidenti*	STA-02.1	Le informazioni sugli incidenti legati alla sicurezza vengono messe periodicamente a disposizione di tutti i clienti e i fornitori interessati tramite mezzi elettronici (ad esempio, portali)?	I piani, le procedure e il programma di risposta agli incidenti AWS sono stati sviluppati in conformità allo standard ISO 27001. Nei rapporti AWS SOC vengono forniti dettagli sulle attività di controllo specifiche eseguite da AWS. Per ulteriori dettagli, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security.

Gruppo di	CID	Domande sulla	Risposta AWS
Gestione della catena di distribuzione, trasparenza e responsabilità *Servizi infrastrutturali/ di rete*	STA-03.1	Vengono raccolti dati su capacità e utilizzo per tutti i componenti rilevanti del servizio cloud offerto?	AWS gestisce i dati di capacità e utilizzo in conformità allo standard ISO 27001. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	STA-03.2	Ai tenant vengono forniti i rapporti su utilizzo e pianificazione della capacità?	
Gestione della catena di distribuzione, trasparenza e responsabilità *Valutazioni interne dei fornitori*	STA-04.1	Si eseguono valutazioni interne annuali della conformità e dell'efficacia di policy, procedure e misure e parametri a supporto?	Il team della catena di approvvigionamento e distribuzione AWS mantiene i rapporti con tutti i fornitori AWS. Per ulteriori informazioni, fare riferimento agli standard ISO 27001, appendice A, dominio 15. AWS è stato convalidato e certificato da un auditor indipendente per confermare la conformità allo standard di certificazione ISO 27001.
Gestione della catena di distribuzione, trasparenza e responsabilità *Accordi con terze parti*	STA-05.1	I fornitori di outsourcing sono selezionati e monitorati in conformità con la legislazione del paese in cui i dati vengono elaborati, memorizzati e trasmessi?	I requisiti di sicurezza del personale per i fornitori di terze parti che supportano sistemi e dispositivi AWS sono stabiliti in un accordo di non divulgazione reciproco tra l'organizzazione padre di AWS, Amazon.com e il rispettivo fornitore terzo. L'ufficio legale di Amazon e l'ufficio acquisti di AWS definiscono i requisiti del personale per i fornitori terzi AWS in accordi contrattuali con il fornitore terzo. Tutte le persone che lavorano con le informazioni AWS devono come minimo superare il processo di selezione per i controlli preliminari sui precedenti penali e firmare un accordo di non divulgazione prima di poter essere autorizzate ad accedere alle informazioni AWS. AWS generalmente non esternalizza lo sviluppo di servizi AWS a subappaltatori.
	STA-05.2	I fornitori di outsourcing sono selezionati e monitorati in conformità con la legislazione del paese in cui sono stati originati i dati?	
	STA-05.3	L'ufficio legale esamina tutti gli accordi con terze parti?	
	STA-05.4	Gli accordi con terze parti includono la garanzia di sicurezza e protezione di informazioni e asset?	
	STA-05.5	Ai client vengono forniti elenchi e copie sempre aggiornati di tutti gli accordi secondari di trattamento?	

Gruppo di	CID	Domande sulla	Risposta AWS
Gestione della catena di distribuzione, trasparenza e responsabilità *Revisioni della governance della catena di distribuzione*	STA-06.1	Viene effettuato il controllo dei processi di governance e gestione dei rischi dei partner per verificare i rischi ereditati da altri membri della catena di fornitura di tali partner?	AWS sottoscrive accordi formali con i principali fornitori di terze parti e implementa appropriati meccanismi di gestione dei rapporti in linea con le relazioni con l'azienda. I processi AWS per la gestione di terze parti vengono verificati da revisori indipendenti nell'ambito della conformità continua di AWS con gli standard SOC e ISO 27001.
Gestione della catena di distribuzione, trasparenza e responsabilità *Metriche della catena di distribuzione*	STA-07.1	Sono stata stabilite policy e procedure e sono stati implementati processi aziendali e misure tecniche a supporto per mantenere accordi completi, accurati e rilevanti (ad esempio, SLA, Service Level Agreement, contratto sul livello di servizio) tra fornitori e clienti (tenant)?	
	STA-07.2	È possibile rilevare e risolvere i problemi di non conformità delle disposizioni e/o dei termini lungo l'intera catena di fornitura (a monte/a valle)?	
	STA-07.3	È possibile gestire conflitti o incoerenze a livello di servizio derivanti dai rapporti con diversi fornitori?	
	STA-07.4	Accordi, policy e processi vengono revisionati almeno una volta l'anno?	
Gestione della catena di distribuzione, trasparenza e responsabilità *Valutazione di terze parti*	STA-08.1	Viene garantita una ragionevole sicurezza delle informazioni lungo la relativa catena di fornitura mediante l'esecuzione di una verifica annuale?	

Gruppo di	CID	Domande sulla	Risposta AWS
	STA-8.2	La verifica annuale include tutti i partner/fornitori di terze parti da cui la catena di fornitura dipende?	
Gestione della catena di distribuzione, trasparenza e responsabilità *Audit di terze parti*	STA-09.1	Si consente ai tenant di eseguire valutazioni indipendenti della vulnerabilità?	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. AWS Security chiede periodicamente a imprese che operano nel settore della sicurezza di eseguire valutazioni di vulnerabilità alle minacce esterne. Nei rapporti AWS SOC vengono forniti dettagli aggiuntivi sulle attività di controllo specifiche eseguite da AWS.
	STA-09.2	Vengono fatte eseguire a servizi di terze parti esterni scansioni di vulnerabilità e test di intrusione periodici su applicazioni e reti?	
Gestione di minacce e vulnerabilità *Software antivirus/ malware*	TVM-01.1	Sono stati installati su tutti i sistemi programmi anti-malware che supportano o si connettono ai servizi cloud offerti?	Il programma, i processi e le procedure AWS per la gestione del software antivirus/malware sono conformi agli standard ISO 27001. Ulteriori dettagli sono disponibili nei rapporti AWS SOC. Per ulteriori informazioni, fare inoltre riferimento allo standard ISO 27001, appendice A, dominio 12. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	TVM-01.2	Ci si assicura che i sistemi di rilevamento delle minacce alla sicurezza che utilizzano firme, elenchi o modelli di comportamento siano aggiornati su tutti i componenti dell'infrastruttura entro intervalli di tempo accettati nel settore?	

Gruppo di	CID	Domande sulla	Risposta AWS
Gestione di minacce e vulnerabilità *Gestione patch/ vulnerabilità*	TVM-02.1	Vengono eseguite periodicamente scansioni di vulnerabilità a livello di rete come prescritto dalle best practice di settore?	I clienti mantengono il controllo dei propri sistemi operativi, software e applicazioni guest e sono responsabili dell'esecuzione delle scansioni di vulnerabilità e dell'applicazione delle patch ai propri sistemi. 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. AWS Security esegue scansioni regolari di tutti gli indirizzi IP dell'endpoint del servizio connessi a Internet per individuare le vulnerabilità. AWS Security notifica alle parti interessate le eventuali vulnerabilità identificate a cui è necessario porre rimedio. La manutenzione e l'applicazione di patch ai sistemi AWS non ha, in genere, alcun impatto sui clienti. Per ulteriori informazioni, consultare il whitepaper AWS Cloud Security (Panoramica sulla sicurezza del cloud AWS), disponibile all'indirizzo http://aws.amazon.com/security. Per ulteriori dettagli, fare riferimento allo standard ISO 27001, appendice A, dominio 12. AWS è stato convalidato e certificato da un revisore indipendente per confermare la conformità allo standard di certificazione ISO 27001.
	TVM-02.2	Vengono eseguite periodicamente scansioni di vulnerabilità a livello di applicazione come prescritto dalle best practice di settore?	
	TVM-02.3	Vengono eseguite periodicamente scansioni di vulnerabilità a livello di sistema operativo locale come prescritto dalle best practice di settore?	
	TVM-02.4	I risultati delle scansioni di vulnerabilità saranno messi a disposizione dei tenant su richiesta?	
	TVM-02.5	È possibile correggere rapidamente le vulnerabilità attraverso tutti i dispositivi informatici, le applicazioni e i sistemi?	
	TVM-02.6	Ai tenant saranno forniti su richiesta gli intervalli di tempo basati sul rischio per l'applicazione di patch ai sistemi?	
Gestione di minacce e vulnerabilità *Codice mobile*	TVM-03.1	Il codice mobile è stato autorizzato prima dell'installazione e dell'utilizzo e la configurazione del codice è stata verificata per assicurarsi che il codice mobile autorizzato funzioni secondo una politica di sicurezza chiaramente definita?	AWS permette ai clienti di gestire le applicazioni client e per dispositivi mobili in base alle proprie esigenze.
	TVM-03.2	È stata impedita l'esecuzione di tutto il codice mobile autorizzato?	

Approfondimenti

Per ulteriori informazioni, consultare le seguenti fonti:

- Panoramica su gestione dei rischi e conformità in AWS
- Certificazioni AWS, programmi, rapporti e attestazioni di terze parti
- Risposte di AWS alle principali domande sulla conformità

Revisioni del documento

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