aws partner network | competency

AWS Retail Competency

Elenco di controllo per la convalida dei partner tecnologici

Dicembre 2019
Versione 1.0

Indice

Introduzione

L'obiettivo del Programma AWS Competency è di riconoscere i partner dell'AWS Partner Network ("partner APN") che dimostrano di avere competenze tecniche e successo con i clienti in ambito di soluzioni specializzate. L'Elenco di controllo per la convalida dei partner tecnologici ("Elenco di controllo") è destinato ai partner APN interessati a inviare una richiesta di ammissione per un programma AWS Competency. In questo elenco sono contenuti i criteri necessari per ottenere la nomina al Programma AWS Competency. Richiedendo l'ammissione per una specifica competenza, i partner APN si sottopongono a un audit in merito alle proprie competenze. A tale scopo, AWS sfrutta la propria esperienza in-house e aziende terze per facilitare il processo di audit. AWS si riserva il diritto di apportare cambiamenti al presente documento in qualsiasi momento.

Aspettative delle parti

È necessario che i partner APN leggano attentamente il presente documento prima di fare richiesta di ammissione al Programma AWS Competency, anche se tutti i prerequisiti sono stati soddisfatti. In primo luogo, se alcune parti del presente documento sono poco chiare e richiedono un'ulteriore spiegazione, contattare il proprio Partner Development Representative ("PDR") o il Partner Development Manager ("PDM") di AWS. Nel caso in cui fosse necessaria ulteriore assistenza, il tuo PDR/PDM contatterà l'ufficio programmi.

Una volta pronti a inviare la richiesta di ammissione al programma, i partner APN sono tenuti a completare la colonna di autovalutazione dell'Elenco di controllo presente in basso, in questo documento.

Per inviare la tua richiesta di ammissione:

1. Accedi all'APN Partner Central (https://partnercentral.awspartner.com/), come Responsabile Alliance
2. Seleziona "View My APN Account" (visualizza il mio account APN) dal lato sinistro della pagina
3. Passa alla sezione "Program Details" (dettagli del programma)
4. Seleziona "Update" (aggiorna) accanto all'AWS Competency per cui desideri richiedere l'ammissione
5. Compila la richiesta di ammissione al programma e fai clic su "Submit" (invia)
6. Invia l'autovalutazione completa all'indirizzo e-mail competency-checklist@amazon.com.
    - L'autovalutazione deve contenere:
        - La Categoria della soluzione (Coinvolgimento dei clienti, Merchandising e pianificazione aziendale, Catena di approvvigionamento e distribuzione, Punti vendita fisici, digitali e virtuali, Data science avanzata per la vendita al dettaglio e Applicazioni aziendali fondamentali per la vendita)
        - Tipo di distribuzione (SaaS o distribuito su AWS dal cliente)
        - Documentazione per i casi di studio di AWS (consultare la definizione sottostante)

Per eventuali domande relative alle istruzioni di cui sopra, contatta il tuo PDR/PDM.
AWS revisionerà e risponderà alla tua richiesta di ammissione entro cinque giorni lavorativi, al fine di fissare la data del tuo audit o per richiederti delle informazioni aggiuntive.

I partner APN sono tenuti a prepararsi per l'audit leggendo l'Elenco di controllo, completando l'autovalutazione mediante l'ausilio dell'Elenco stesso e raccogliendo e organizzando prove obiettive da mostrare all'incaricato il giorno dell'audit.

AWS raccomanda ai partner APN di contare su professionisti in grado di argomentare nel dettaglio i requisiti durante l'audit. Come best practice, il partner APN deve rendere disponibile il seguente personale per l'audit: uno o più ingegneri/progettisti con profilo altamente tecnico certificati AWS; un responsabile delle attività operative e degli elementi di supporto; un dirigente dello sviluppo aziendale per la presentazione generale. I partner APN devono assicurarsi di disporre di tutti i consensi necessari per poter rivelare all'incaricato tutte le informazioni contenute nelle prove obiettive o dimostrazioni (sia di AWS che di terze parti), prima che abbia luogo la programmazione dell'audit.

Programma AWS Retail Competency

I partner AWS Retail Competency forniscono soluzioni nel settore della Vendita al dettaglio in ambiti quali Coinvolgimento dei clienti, Merchandising e pianificazione aziendale, Catena di approvvigionamento e distribuzione, Punti vendita fisici, digitali e virtuali, Data science avanzata per la vendita al dettaglio e Applicazioni aziendali fondamentali per la vendita.

Categorie Retail Competency

I partner APN devono identificare la Categoria del settore corrispondente alla soluzione che forniscono tra:

- **Coinvolgimento del Cliente:** Fedeltà, Gestione dei canali social, Gestione dei Rapporti con la clientela (CRM), Call Center, Pubblicità (Digitale e Direct Mail), Soluzioni SEO e di Coinvolgimento del pubblico che consentano ai leader nel settore del Marketing al dettaglio di attrarre proattivamente e mantenere clienti prima e dopo l'acquisto.

- **Merchandising e Pianificazione Aziendale:** Merchandising, Rifornimento, Pianificazione dell'inventario, Pianificazione del Pianogramma/Spazio, Ottimizzazione della Promozione e dei Prezzi, Gestione delle Categorie e soluzioni di Collaborazione con i Fornitori con l'aiuto dei team di Merchandising e Pianificazione Aziendale

- **Catena di Approvvigionamento e Distribuzione:** Soluzioni di Catena di approvvigionamento e distribuzione che coprano Sistemi di Gestione del Magazzino (WMS), Pianificazione delle Risorse d'Impresa (ERP), automazione del magazzino, import/export, trasporto e logistica.

- **Punti vendita fisici, digitali e virtuali:** Soluzioni in grado di trasformare l'esperienza d'acquisto online o offline che coprano POS, Sistemi di gestione degli ordini (OMS), Commercio unficato, eCommerce, Consegne sull'ultimo miglio, Esperienza in negozio senza vincoli (senza frizioni), Innovazioni digitali, (AR/VR, ESL, IoT, Beacon, Voce, Riconoscimento, Chisco Digitale, Smart Mirrors, Schermi Interattivi), Gestione delle Risorse Digitali (DAM) e Pagamenti.

- **Data science avanzata per la vendita al dettaglio:** Data lake per la Vendita al dettaglio, AI/ML e Soluzioni di Analisi in grado di migliorare l'efficienza operativa e gli spunti e il coinvolgimento della clientela.

- **Applicazioni aziendali fondamentali per la ventita al dettaglio** Soluzioni aziendali fondamentali per la vendita al dettaglio per C-Suite, Finanza, Approvvigionamenti, Risorse Umane, Gestione dei dipendenti, Ufficio Legale e Dipartimento IT.

I Partner APN devono inoltre identificare la Categoria di Consegna applicabile alle rispettive soluzioni:

1. **SaaS:** Serve più clienti da un'infrastruttura AWS condivisa. Tutti gli account AWS sono gestiti dal Partner APN.

2. **Distribuita dal Cliente:** Sono distribuite in un ambiente AWS del cliente. Tutti gli account AWS sono gestiti dal Partner APN.

Prerequisiti del programma AWS Retail Competency

Le seguenti voci verranno convalidate dall'incaricato del programma AWS Competency; informazioni mancanti o incomplete devono essere aggiornate prima di pianificare l'esame di convalida tecnologica.

1.0 Partecipazione al programma APN		Soddisfatto Sì/No
1.1 Livello del partner tecnologico APN	Il partner APN deve leggere attentamente le linee guida del programma e le definizioni prima di richiedere l'ammissione al programma AWS Retail Competency. Fai clic qui per i dettagli sul programma.	
1.2 Livello del partner tecnologico APN	Il partner APN deve essere un partner APN tecnologico di livello Advanced prima di poter richiedere l'ammissione al programma AWS Retail Competency.	
1.3 Categoria della soluzione	Il Partner APN è tenuto a identificare la Categoria di Settore corrispondente alla propria soluzione: ☐ **Modello di coinvolgimento del cliente** ☐ **Merchandising e Pianificazione Aziendale** ☐ **Catena di approvvigionamento e Distribuzione** ☐ **Punti vendita fisci, digitali e virtuali** ☐ **Data Science Avanzata per la Vendita al dettaglio** ☐ **Applicazioni aziendali fondamentali nella vendita al dettaglio** Il Partner APN è tenuto a identificare la Categoria di consegna corrispondente alla propria soluzione: ☐ **SaaS** ☐ **Distribuita dal Cliente**	
1,4 Adozione da parte dei clienti	Il Partner APN è tenuto a indicare il numero totale di clienti che sfruttano la sua soluzione.	

2.0 Casi di studio		Soddisfatto Sì/No
2.1 Casi di studio specifici nell'ambito del programma Retail	Il Partner APN deve disporre di 4 Casi di studio specifici per una singola soluzione Retail sotto esame. Ciascuno dei 4 Casi di studio deve fare riferimento a un esempio della Soluzione del Partner APN in uso in una delle sei Categorie di settore (Coinvolgimento dei clienti, Merchandising e pianificazione aziendale, Catena di approvvigionamento e distribuzione, Punti vendita fisici, digitali e virtuali, Data science avanzata per la vendita al dettaglio e Applicazioni aziendali fondamentali per la vendita) I Partner APN in possesso di Competenze nei campi di AWS Digital Customer Experience (DCX), Data & Analytics, IoT, Migrazione e/o Machine learning, possono riutilizzare fino a un massimo di 4 Casi di studio per i progetti consegnati con soluzioni specificatamente concepite per le esigenze del settore e con pratiche di consulenza che offrano una conoscenza unica del segmento specifico per il settore della Vendita al dettaglio. Per ciascun Caso di studio, il partner APN deve fornire le seguenti informazioni: ▪ Nome del cliente ▪ Sito web del cliente ▪ Esigenza del cliente ▪ Il modo in cui è stata implementata la soluzione per soddisfare l'esigenza del cliente ▪ Applicazioni o soluzioni di terzi utilizzate ▪ Data della produzione di riferimento ▪ Esiti/risultati ▪ Schemi di architettura specifici, guide alla distribuzione e altri materiali, a seconda del tipo di soluzione, come descritto nella sezione successiva. Queste informazioni saranno richieste come parte della procedura di ammissione al programma da APN Partner Central. Le informazioni fornite nell'ambito di tale Caso di studio possono essere private e non verranno rese pubbliche.	

	Tutti i 4 casi di studio forniti verranno esaminati nell'ambito della Verifica della documentazione della convalida tecnica. Il caso di studio non verrà preso in esame per l'inclusione al programma AWS Competency qualora il partner APN non fosse in grado di fornire la documentazione necessaria a valutare tale Caso di studio in relazione a ciascuna voce dell'elenco di controllo, oppure nel caso in cui non vengano soddisfatte tutte le voci dell'elenco. I Casi di studio devono descrivere le distribuzioni eseguite negli ultimi 18 mesi e devono riguardare progetti in produzione per clienti, non progetti in fase "pilota" o dimostrazioni di concetto.	
2.2 Casi di studio disponibili al pubblico	I casi di studio disponibili al pubblico vengono usati da AWS con l'approvazione al programma Competency, al fine di esibire la dimostrazione di successo da parte del partner APN, sulla base di indicatori di prestazione chiave misurabili in merito alla soluzione, e fornire ai clienti la certezza che il Partner APN gode dell'esperienza e della conoscenza necessarie a sviluppare e offrire soluzioni tali da soddisfare i loro obiettivi. 2 delle 4 distribuzioni per clienti associate ai casi di studio devono essere pubblicizzate dal Partner APN come casi di studio disponibili al pubblico. Tali Casi di studio disponibili al pubblico possono essere sotto forma di casi di studio formali, white paper o post su blog.	
	I Casi di studio disponibili al pubblico devono essere facilmente consultabili dal sito Web del partner APN, per esempio accedendovi dalla rispettiva home page, oltre che dai link presenti all'interno della richiesta di ammissione presentata dal Partner.	
	I Casi di studio disponibili al pubblico devono includere quanto segue: ▪ Riferimenti al nome del cliente, nome del Partner APN e AWS ▪ Esigenza del cliente ▪ Il modo in cui è stata implementata la soluzione per soddisfare l'esigenza del cliente ▪ In che modo sono stati utilizzati i servizi AWS come parte della soluzione ▪ Esiti/risultati	
3.0 Presenza Web e Leadership di pensiero AWS Microsoft Workloads		**Soddisfatto Sì/No**
3.1 Landing Page AWS del Partner APN	La presenza online di un partner APN specifica per le proprie soluzioni AWS Retail offre una certezza ai clienti a livello di capacità ed esperienza Retail da esso possedute. Il partner APN deve disporre di una Landing Page AWS che descriva la propria soluzione AWS Retail, che contenga dei collegamenti ai propri Casi di studio disponibili al pubblico, che elenchi le partnership tecnologiche, che offra qualsiasi altra informazione rilevante a supporto della sua esperienza correlata alla Vendita al dettaglio e che, infine, evidenzi la sua partnership con AWS. La pagina AWS specifica per il campo delle vendite al dettaglio deve essere accessibile dalla home page del partner APN. La home page stessa non è accettabile come Landing Page AWS a meno che il partner APN non sia un'azienda dedicata alla Tecnologia Retail e la home page rifletta l'attenzione del partner APN per questo aspetto.	
3.2 Leadership considerata nelle vendite al dettaglio	I partner AWs Retail Competency si intendono specializzati nel campo delle vendite al dettaglio anche tramite lo sviluppo di soluzioni innovative che sfruttano i servizi AWS. Il partner APN deve disporre di materiali rivolti al pubblico (es. post su blog, articoli, video, ecc.) che dimostrano la propria dedizione e competenza in merito al campo della Vendita al dettaglio. È necessario fornire dei link ad esempi di materiali pubblicati negli ultimi 12 mesi.	
4.0 Requisiti aziendali		
4.1 Strumenti Field-Ready	Il Partner APN deve disporre di documentazione field-ready e strumenti per la vendita che includano una proposta chiara del valore del prodotto che possa essere articolata con l'organizzazione AWS sales con tutte le pertinenti informazioni necessarie a determinare l'idoneità per l'opportunità di un cliente (ad es. collaterali di vendita, presentazione e casi di utilizzo da parte del cliente). Le prove devono essere sotto forma di collaterale di vendita che includa una presentazione, un documento di una pagina e una lista di controllo dell'utilizzo del cliente.	

4.2 Assistenza al prodotto/Help Desk	I partner APN offrono assistenza al prodotto per i propri clienti, via chat Web, telefono, o e-mail. A testimonianza di questo è necessario fornire una descrizione dell'assistenza offerta ai clienti, per il prodotto o la soluzione.	
4.3 Il prodotto è elencato su AWS Marketplace	Il partner APN rende disponibile la soluzione via AWS Marketplace. ☐ Sì ☐ No Se la risposta è "sì", il Partner APN deve fornire un link all'elenco AWS Marketplace. Se la risposta è "no", non sono necessarie ulteriori informazioni.	
4.4 Provvigioni sulle Vendite per le Offerte AWS Congiunte	Il Partner deve disporre di piani di provvigioni sulle vendite per i propri venditori sulle opportunità congiunte con AWS. ☐ Sì ☐ No ☐ Spiegare:_____ Le prove devono essere sotto forma di una breve descrizione del piano di provvigioni per i venditori del Partner APN.	
Vincite Congiunte AWS/Partner APN	Il Partner APN deve disporre di una procedura atta a documentare e pubblicizzare le vincite congiunte. Le prove devono essere sotto forma di descrizioni orali della procedura.	
5.0 Autovalutazione dei partner APN		**Soddisfatto Sì/No**
5.1 Autovalutazione con elenco di controllo per la convalida AWS Competency Partner	Il partner APN deve eseguire un'autovalutazione della sua conformità ai requisiti seguendo l'elenco di controllo per la convalida dei partner tecnologici nell'ambito delle vendite al dettaglio su AWS. ▪ Il partner APN deve completare tutte le sezioni dell'elenco di controllo. ▪ L'autovalutazione completa deve essere inviata via e-mail all'indirizzo **competency-checklist@amazon.com**, utilizzando la seguente convenzione per l'oggetto: "[Nome partner APN], Retail Competency Technology Partner Completed Self-Assessment". ▪ Si raccomanda che il partner APN faccia revisionare l'autovalutazione completa al proprio Solutions Architect, Partner Development Representative (PDR) interno o Partner Development Manager (PDM) prima di inviarla ad AWS. Lo scopo di ciò è assicurare che il team AWS del partner APN si impegni per fornire eventuali raccomandazioni prima della presa in esame, al fine di assicurare un'esperienza produttiva.	

AWS Retail Competency: elenco di controllo per la convalida del partner tecnologico

Le voci che seguono saranno convalidate da un Auditor di terze parti e/o da un Solution Architect del partner AWS; informazioni mancanti o incomplete devono essere aggiornate prima di pianificare l'Esame di Convalida Tecnologica.

		Si applica a:		
Convalida tecnica		SaaS	Distribuita dal Cliente su AWS	Soddisfatto S/N
Schema architetturale	In base alla categoria di distribuzione, sono richiesti uno o più schemi architetturali. Ciascuno schema deve dimostrare: ☐ I principali elementi dell'architettura e il modo in cui si combinano per fornire la soluzione del Partner ai clienti ☐ Tutti i Servizi AWS utilizzati, tramite le icone appropriate. ☐ Come sono distribuiti i servizi AWS, tra cui, Amazon Virtual Private Cloud (VPC), Zone di disponibilità, sottoreti e connessioni ai sistemi esterni ad AWS. ☐ Include elementi distribuiti all'esterno di AWS, per es. componenti in locale o dispositivi hardware.	Sì - uno per l'intera soluzione e uno per ogni caso di studio.	Sì - uno per ogni caso di studio.	
Guida alla distribuzione	La guida alla distribuzione deve fornire le best practice per la distribuzione relativa alla soluzione del Partner in AWS, e deve includere tutte le sezioni illustrate nei requisiti di base per le guide di distribuzione ("Baseline Requirements for Deployment Guides")	No	Sì - una per la soluzione	
Elenco di controllo completo per la convalida	Per ognuno dei quattro casi di studio forniti per la Soluzione del Partner, il Partner APN deve fornire una versione completa del seguente elenco di controllo indicando quali voci dell'elenco sono soddisfatte.	Sì	Sì	
1.0 Sicurezza **Il fondamento della sicurezza riguarda la protezione delle informazioni e dei sistemi. Gli argomenti chiave includono la confidenzialità e la riservatezza dei dati, l'identificazione e la gestione dei privilegi, la protezione dei sistemi e la messa a punto di controlli per rilevare eventi legati alla sicurezza.**				
1.1 L'utente root dell'account AWS non viene usato per attività di routine	1.1 L'utente root dell'account AWS non può essere usato per attività di routine. Dopo la creazione del tuo account AWS, devi immediatamente creare degli account utente AWS Identity and Access Management (IAM), utilizzandoli per tutte le attività di routine. Una volta che i tuoi account utente IAM sono stati creati, devi conservare in sicurezza le credenziali dell'account root AWS, utilizzandole per eseguire soltanto le attività di gestione account e assistenza che richiedono espressamente l'utente root dell'account AWS. Per ulteriori informazioni su come impostare account utente IAM e gruppi per l'utilizzo quotidiano, consulta Creating Your First IAM Admin User and Group (creazione del tuo primo utente e gruppo IAM).	Sì	No	
1.2 Multi-Factor Authentication (MFA) abilitata per l'utente root dell'account AWS	Multi-Factor Authentication (MFA) deve essere abilitata per l'utente root del tuo account AWS. Poiché l'utente root può eseguire operazioni sensibili all'interno del tuo account AWS, aggiungere un ulteriore livello di autenticazione contribuisce a una maggiore sicurezza dell'account. Sono disponibili molteplici tipologie di autenticazione MFA, compresa quella virtuale e hardware.	Sì	No	
1.3 Account utente IAM utilizzati per tutte le attività di routine	L'utente root di AWS non deve essere utilizzato per le attività che non lo prevedono espressamente. È necessario creare un nuovo utente IAM per ogni persona che deve accedere come amministratore. Quindi è necessario trasformare in amministratori tali utenti posizionandoli all'interno di un gruppo amministratori con la relativa politica di accesso associata. In seguito, gli utenti del gruppo amministratori dovranno impostare gruppi, utenti e così via per l'account AWS.	Sì	No	

	Tutte le interazioni future dovranno avere luogo attraverso gli utenti dell'account AWS e le relative chiavi di accesso, anziché tramite l'utente root. Tuttavia, per eseguire alcune attività di gestione account e assistenza, dovrai accedere utilizzando le credenziali dell'utente root.			
1.4 Multi-Factor Authentication (MFA) abilitata per tutti gli utenti IAM interattivi	È necessario abilitare l'autenticazione MFA per tutti gli utenti IAM interattivi. Grazie alla MFA, gli utenti hanno a disposizione un dispositivo che genera un codice di autenticazione univoco (password monouso, OTP). Gli utenti devono fornire sia le proprie credenziali (nome utente e password) sia l'OTP. Il dispositivo MFA può essere uno speciale dispositivo hardware oppure un dispositivo virtuale (per esempio, può essere eseguito all'interno di una app o di uno smartphone).	Sì	No	
1.5 Le credenziali IAM sono soggette a rotazione con scadenza regolare	È necessario cambiare la propria password e le chiavi di accesso con scadenza regolare, accertandosi che anche tutti gli utenti IAM del proprio account eseguano tale operazione. In questo modo, se una password o chiave di accesso viene compromessa a propria insaputa, è possibile limitare il periodo durante il quale le credenziali possono essere usate per accedere alle risorse. Puoi applicare una politica per le password al tuo account al fine di richiedere a tutti i tuoi utenti IAM di cambiare la propria password, inoltre puoi decidere con che frequenza richiedere tale rotazione. Per ulteriori informazioni sulla rotazione delle chiavi di accesso per gli utenti IAM, consulta Rotating Access Keys (rotazione delle chiavi di accesso).	Sì	No	
1.6 È in atto una politica per password forti rivolta agli utenti IAM	Devi adottare una politica per password forti rivolta ai tuoi utenti IAM. Se consenti agli utenti di creare le proprie password, devi richiedere che queste siano password forti e che vengano cambiate a scadenze regolari. Alla pagina di impostazioni account della console IAM, puoi creare una politica per password relativa al tuo account. Potrai utilizzare la politica per password al fine di definire i requisiti per le password, come per esempio lunghezza minima, se sono richiesti caratteri non alfabetici, quanto spesso bisogna effettuare la rotazione, e così via. Per ulteriori informazioni, consultare Setting an Account Password Policy for IAM Users (impostazione di una politica per password rivolta agli utenti IAM).	Sì	No	
1.7 Le credenziali IAM non sono condivise tra utenti multipli	Devi creare un account utente IAM individuale per chiunque debba accedere al tuo account AWS. Crea un utente IAM anche per te stesso, concedi a tale utente dei privilegi amministrativi, e utilizza tale utente IAM per lavorare. Creando utenti IAM individuali per le persone che accedono al tuo account, potrai fornire a ciascun utente IAM un set univoco di credenziali di sicurezza. Potrai inoltre accordare autorizzazioni differenti per ciascun utente IAM. Ove necessario, puoi concedere o revocare un'autorizzazione a un utente IAM in qualsiasi momento. (Nel caso in cui cedessi a qualcuno le tue credenziali utente root potrebbe essere difficile revocarle, ed è impossibile limitarne le relative autorizzazioni).	Sì	No	
1.8 Le politiche IAM sono limitate al minimo privilegio	Devi attenerti al principio di sicurezza standard di concedere il minimo privilegio. Ciò significa accordare soltanto le autorizzazioni necessarie per eseguire un'attività. Determina ciò che devono fare gli utenti, quindi personalizza le politiche in modo tale che possano eseguire soltanto le attività necessarie. Inizia da un set minimo di autorizzazioni e concedi autorizzazioni aggiuntive in base all'occorrenza. Questo procedimento è più sicuro rispetto a un inizio troppo permissivo con conseguente tentativo di restringere le autorizzazioni in un secondo momento. La definizione del giusto set di autorizzazioni richiede un po' di ricerca. Determina ciò che serve per una specifica attività, quali azioni supporta un particolare servizio, e quali autorizzazioni sono necessarie per eseguire tali azioni.	Sì	No	

1.9 Non sono utilizzate credenziali a codifica fissa (es. chiavi di accesso)	Devi attenerti alle best practice per la gestione delle chiavi di accesso AWS evitando l'uso di credenziali a codifica fissa. Quando accedi ad AWS a livello di codice, utilizzi una chiave di accesso per verificare la tua identità e l'identità delle tue applicazioni. Chiunque abbia la tua chiave di accesso gode del tuo stesso livello di accesso alle tue risorse AWS. Considerando che AWS fa il possibile per proteggere le tue chiavi di accesso, anche tu dovresti fare lo stesso, in linea con il modello di responsabilità condivisa.	Sì	Sì	
1.10 A riposo, tutte le credenziali sono crittografate	Il requisito di base consiste nell'assicurare la crittografia di ogni credenziale a riposo.	Sì	Sì	
1.11 Le chiavi di accesso AWS sono utilizzate soltanto dagli utenti interattivi	Nessuna chiave di accesso AWS deve essere in uso, eccetto nei seguenti casi: 1 Durante l'utilizzo da parte di persone per accedere ai Servizi AWS e archiviate in sicurezza su un dispositivo controllato da una persona. 2. Durante l'utilizzo da parte di un servizio per accedere ai Servizi AWS, ma solo nei casi in cui: a) non sia possibile usare un ruolo dell'istanza Amazon EC2, un ruolo dell'attività Amazon Elastic Container Service (Amazon ECS) o un meccanismo simile, b) Le chiavi di accesso AWS siano sottoposte a rotazione almeno settimanale, e c) La politica IAM sia molto stringente, così da: i) consentire l'accesso solo in base a metodi e target specifici e ii) restringere l'accesso alle sottoreti dalle quali viene effettuato l'accesso alle risorse.	Sì	Sì	
1.12 AWS CloudTrail è abilitato per tutti gli account AWS in ogni regione	AWS CloudTrail deve essere abilitato per tutti gli account AWS in ogni regione. La visibilità nell'attività del tuo account AWS costituisce un aspetto chiave della sicurezza e delle best practice in fatto di operatività. Puoi utilizzare AWS CloudTrail per visualizzare, ricercare, scaricare, archiviare, analizzare e reagire all'attività dell'account nell'ambito della tua infrastruttura AWS. Puoi identificare chi o cosa ha effettuato una determinata azione, su quali risorse è stata eseguita, quando ha avuto luogo l'evento e altri dettagli per aiutarti ad analizzare le attività all'interno del tuo account AWS e reagire di conseguenza.	Sì	No	
1.13 I log AWS CloudTrail sono archiviati in un bucket S3 di un altro account AWS	I log di AWS CloudTrail devono essere posizionati in un bucket di un altro account AWS e configurati per un accesso estremamente limitato, come per esempio un audit o un ripristino.	Sì	No	
1.14 Il bucket dei log CloudTrail S3 dispone di Versioning o MFA Delete abilitati.	I contenuti relativi al bucket dei log AWS CloudTrail devono essere protetti con versioning o MFA Delete.	Sì	No	
1.15 I gruppi di sicurezza Amazon EC2 sono strettamente limitati	Tutti i gruppi di sicurezza Amazon EC2 devono restringere l'accesso il più possibile. Ciò include almeno 1. Implementazione di gruppi di sicurezza per restringere il traffico tra internet e Amazon VPC, 2. Implementazione di gruppi di sicurezza per restringere il traffico all'interno di Amazon VPC, e 3. In tutti i casi, consenti soltanto le impostazioni più stringenti.	Sì	Sì	
1.16 I bucket Amazon S3 all'interno del tuo account hanno un livello di accesso adeguato	Devi assicurare che sono stati adottati controlli adeguati per controllare l'accesso a ogni bucket Amazon S3. Quando utilizzi AWS, è buona prassi limitare l'accesso alle tue risorse soltanto per le persone a cui servono davvero (il principio del privilegio minimo).	Sì	Sì	
1.17 I bucket Amazon S3 non sono stati mal configurati per consentire	Devi assicurare che i bucket che non devono consentire l'accesso pubblico siano adeguatamente configurati per impedire l'accesso pubblico. Per impostazione predefinita, tutti i bucket Amazon S3 sono privati, e possono accedervi soltanto gli utenti a cui è stato esplicitamente accordato l'accesso. La maggior	Sì	Sì	

l'accesso pubblico.	parte dei casi d'uso non richiede l'accesso pubblico per la lettura dei file dal tuo bucket Amazon S3, a meno che tu non stia usando Amazon S3 per degli asset pubblici (per esempio per immagini da utilizzare in un sito Web pubblico), inoltre è buona prassi non rendere mai pubblico l'accesso.			
1.18 È in atto un meccanismo di monitoraggio per rilevare quando i bucket oppure gli oggetti S3 vengono resi pubblici	Devi adottare un monitoraggio o degli avvisi per rilevare quando i bucket Amazon S3 vengono resi pubblici. Una possibile opzione per questa prassi è l'utilizzo di AWS Trusted Advisor. AWS Trusted Advisor controlla i bucket Amazon S3 con autorizzazione ad accesso libero. Le autorizzazioni bucket che concedono un accesso agli elenchi per chiunque possono dare luogo a spese impreviste se gli oggetti presenti nel bucket sono elencati da utenti non voluti, a una frequenza elevata. Le autorizzazioni bucket che concedono un accesso Upload/Delete per chiunque danno origine a vulnerabilità in fatto di sicurezza, consentendo a chiunque di aggiungere, modificare o rimuovere voci in un bucket. Il controllo di Trusted Advisor esamina le autorizzazioni bucket esplicite e le politiche associate che possono prevalere sulle autorizzazioni bucket.	Sì	No	
1.19 È in atto un meccanismo di monitoraggio per rilevare le modifiche nelle istanze Amazon EC2 e nei Container	Qualsiasi modifica alle tue istanze Amazon S3 o ai tuoi Container può indicare un'attività non autorizzata e deve come minimo essere registrata in una posizione permanente per consentire eventuali indagini forensi in futuro. Il meccanismo impiegato a tale scopo deve quantomeno: 1. Rilevare qualsiasi modifica al sistema operativo o ai file dell'applicazione nelle istanze di Amazon S3 o nei Container utilizzati nella soluzione. 2. Conservare i dati che registrano tali modifiche in una posizione permanente, esterna all'istanza Amazon S3 o al Container. Tra gli esempi di meccanismi adeguati vi sono: a. Distribuzione di un controllo di integrità dei file tramite la gestione della configurazione pianificata (es. Chef, Puppet, ecc.) o uno strumento specializzato (es. OSSEC, Tripwire o simili), oppure b. Estensione degli strumenti per la gestione della configurazione al fine di convalidare la configurazione host di Amazon S3 e avvisare in caso di aggiornamenti su file di configurazione chiave o pacchetti con eventi no-op configurati per assicurare che il servizio rimanga operativo su tutti gli host rilevanti durante il tempo di esecuzione, oppure c. Distribuzione di un sistema di rilevamento di intrusione nell'host come per esempio una soluzione open source quale OSSEC con ElasticSearch e Kibana oppure una soluzione partner. Si noti che i seguenti meccanismi non soddisfano il requisito: a. Compiere cicli frequenti di istanze Amazon S3 o container.	Sì	No	
1.20 Tutti i dati sono riservati	Tutti i dati del cliente elaborati e archiviati nel carico di lavoro sono considerati confidenziali per determinarne la sensibilità e metodi di manipolazione appropriati.	Sì	Sì	
1.21 Tutti i dati sensibili sono soggetti a crittografia	Tutti i dati dei clienti classificati come sensibili sono crittografati sia in transito sia a riposo.	Sì	Sì	
1.22 Le chiavi crittografiche sono gestite in sicurezza	Tutte le chiavi crittografiche sono crittografate sia a riposo sia in transito, inoltre l'accesso per l'utilizzo di tali chiavi viene controllato mediante una soluzione AWS come AWS Key Management Service (KMS) oppure tramite una soluzione di un partner APN quale per esempio HashiCorp Vault.	Sì	Sì	
1.23 Tutti i dati in transito sono crittografati	Tutti i dati in transito al di fuori di Amazon Virtual Private Cloud sono crittografati.	Sì	Sì	
1.24 Il processo di reazione agli incidenti sulla sicurezza è definito e testato	È necessario definire un processo di reazione agli incidenti sulla sicurezza per gestire incidenti quali la compromissione dell'account AWS. Questo processo va testato implementando procedure tali da collaudare il processo di reazione agli incidenti, per esempio completando delle verifiche sulla sicurezza. Durante gli ultimi 12 mesi almeno un test deve essere stato completato	Sì	No	

	per confermate che: a. L'accesso all'ambiente è consentito soltanto per chi è idoneo. b. Sono disponibili strumenti adeguati. c. Il personale di competenza sa come reagire di fronte ai vari incidenti in fatto di sicurezza indicati nel piano.			
1.25 Standard di Sicurezza dei Dati (DSS) per il Settore delle Carte di Pagamento (PCI) – Certificazione o SAQ	Per le applicazioni eCommerce, Unified Commerce e Point of Sale, dove sono presenti i dati del titolare della carte, viene stabilita una procedura per eseguire una valutazione annuale della portata degli Standard di Sicurezza dei Dati (DSS) per il Settore delle Carte di Pagamento (PCI) rapportata al carico di lavoro. Sulla base della valutazione della portata viene eseguita una Certificazione PCI DSS o SAQ secondo necessità. Le prove devono essere sotto forma di una Relazione di Conformità per la certificazione PCI DSS o di un Questionario di Autovalutazione (SAQ) compilato.	Sì	Sì	
1.26 crittografia end-to-end dei dati PCI	Per le applicazioni eCommerce, Unfied commerce e Point of Sale dove sono presenti i dati del titolare della carta, essi vengono crittografati durante il trasferimento anche all'interno del VPC Amazon.	Sì	Sì	
1.27 Protezione contro gli attacchi Distributed Denial Of Service (DDoS).	Fornire un'infrastruttura e un servizio atti a mitigare gli attacchi Distributed Denial Of Service (DDoS) attraverso tutti i livelli nel modello di Interconnessione di Sistemi Aperti (OSI).	Sì	No	
Adozione di procedure atte a mitigare i principali 10 attacchi Open Web Application Security Project (OWASP)	Fornire un'infrastruttura e un servizio atti a mitigare le vulnerabilità Open Web Application Security Project (OWASP).	Sì	No	
2.0 Affidabilità. Il pilastro dell'affidabilità si concentra sulla capacità di impedire il verificarsi di situazioni avverse ed eventualmente effettuare un ripristino in modo rapido per soddisfare le esigenze aziendali e del cliente. Gli argomenti principali includono gli elementi fondamentali attorno all'organizzazione, ai requisiti di progetto, alla pianificazione del ripristino e al modo in cui gestiamo il cambiamento.				
2.1 La connettività di rete è altamente disponibile	La connettività di rete alla soluzione deve essere altamente disponibile. Sia che si utilizzi una VPN oppure AWS Direct Connect, per connettersi alle reti dei clienti, la soluzione deve supportare connessioni ridondanti, anche quando i clienti non effettuano l'implementazione.	Sì	Sì	
2.2 I meccanismi di scalabilità infrastrutturale si allineano ai requisiti aziendali	I meccanismi di scalabilità infrastrutturale devono allinearsi ai requisiti aziendali: 1. Implementando meccanismi di dimensionamento automatico su ogni livello dell'architettura. 2. Confermando che gli attuali requisiti aziendali, inclusi i requisiti relativi ai costi e la crescita dell'utente prevista, non necessitano di meccanismi di dimensionamento automatico E che le procedure di dimensionamento manuale sono interamente documentate e testate di frequente.	Sì	Sì	
2.3 I log AWS e dell'applicazione sono gestiti centralmente	Tutte le informazioni sui log dell'applicazione e sull'infrastruttura AWS devono essere consolidate all'interno di un unico sistema.	Sì	No	
2.4 Il monitoraggio e gli allarmi AWS e dell'applicazione sono gestiti centralmente	L'applicazione e l'infrastruttura AWS devono essere gestite centralmente, inviando gli allarmi generati al personale addetto.	Sì	No	
2.5 La gestione e il provisioning dell'infrastruttura sono automatizzati	La soluzione deve utilizzare uno strumento automatizzato come AWS CloudFormation o Terraform per il provisioning e la gestione dell'infrastruttura AWS. La console AWS non deve essere utilizzata per apportare modifiche di routine all'infrastruttura AWS di produzione.	Sì	Sì	

2.6 Vengono effettuati backup dei dati con scadenza regolare	Devi effettuare backup regolari in un servizio di storage permanente. I backup garantiscono la possibilità di effettuare un ripristino successivamente a scenari di errore amministrativo, logico o fisico. Amazon S3 e Amazon Glacier sono servizi preferenziali per il backup o l'archiviazione. Entrambi i servizi sono piattaforme di storage permanenti e a basso costo. Entrambi offrono capacità limitata e non richiedono una gestione dei volumi o dei supporti con l'aumentare dei set di dati. Il modello di pagamento in base all'utilizzo e il basso costo per GB/mese rendono tali servizi adatti per la protezione dei dati.	Sì	Sì	
2.7 I meccanismi di ripristino vengono testati con scadenza regolare e successivamente a modifiche architetturali significative.	Devi testare i meccanismi di ripristino e le procedure, sia con scadenza periodica sia dopo aver apportato modifiche significative all'ambiente cloud. AWS offre risorse utili per aiutarti a gestire il backup e il ripristino dei tuoi dati.	Sì	No	
2.8 La soluzione è resiliente alle interruzioni della zona di disponibilità	La soluzione deve continuare ad essere operativa nel caso in cui tutti i servizi interni a una specifica zona di disponibilità vengano interrotti.	Sì	Sì	
2.9 La resilienza della soluzione è stata testata	La resilienza dell'infrastruttura all'interruzione di una singola zona di disponibilità è stata testata in produzione, per esempio tramite esercizi di verifica negli ultimi 12 mesi.	Sì	No	
2.10 È stato definito un piano di disaster recovery (DR)	Un piano di disaster recovery ben definito include un Recovery Point Objective (RPO) e un Recovery Time Objective (RTO). È necessario definire un RPO e un RTO per tutti i servizi pertinenti, inoltre tali parametri devono essere in linea con il contratto SLA offerto alla clientela.	Sì	Sì	
2.11 L'RTO impiega meno di 24 ore	In base al requisito di riferimento, l'RTO deve impiegare meno di 24 ore per i servizi core.	Sì	No	
2.12 Il piano di Disaster Recovery (DR) è adeguatamente testato	Il tuo piano DR deve essere testato in merito ai parametri RPO e RTO sia con scadenza periodica sia a seguito di aggiornamenti importanti. Prima dell'approvazione relativa alla richiesta di ammissione al livello avanzato per partner APN, è necessario completare almeno un test DR.	Sì	No	
2.13 Il piano di Disaster Recovery (DR) include il ripristino a un'altra Regione	Il tuo piano DR deve includere una strategia di ripristino a un'altra Regione AWS, inoltre i tuoi test di ripristino periodici devono verificare tale scenario. Devi aver portato a termine almeno un test completo del piano DR, compreso il ripristino a un'altra Regione AWS, entro gli ultimi 12 mesi. Nota: sebbene i processi di ripristino dei dati all'interno di ambienti di test o di esportazione dei dati per gli utenti siano utili per verificare i backup, tali processi non soddisfano il requisito per cui è necessario eseguire un test di ripristino completo in un'altra Regione AWS.	Sì	No	
3.0 Eccellenza operativa Il pilastro dell'eccellenza operativa si focalizza sull'esecuzione e il monitoraggio dei sistemi per offrire valore aziendale e migliorare senza sosta i processi e le procedure. Argomenti chiave includono la gestione e l'automatizzazione delle modifiche, la reazione agli eventi, e la definizione di standard per gestire con successo le operazioni quotidiane.				
3.1 La distribuzione delle modifiche relative al codice è automatizzata	La soluzione deve usare un metodo automatizzato di distribuzione del codice nell'infrastruttura AWS. Le sessioni interattive con protocollo Secure Shell (SSH) o Remote Desktop (RDP) non possono essere usate per distribuire aggiornamenti nell'infrastruttura AWS.	Sì	No	

3.2 Runbook e processo di escalation sono stati definiti	È necessario sviluppare i runbook per definire le procedure standard usate in risposta alle diverse applicazioni e ai diversi eventi AWS. È necessario definire un processo di escalation per gestire gli avvisi e gli allarmi generati dal sistema, e per reagire ai problemi riportati dai clienti. Il processo di escalation deve inoltre includere il passaggio ad AWS Support, ove appropriato.	Sì	No	
3.3 Il supporto AWS Business è attivo per l'account AWS	Il supporto Business deve essere attivo. Il supporto Business (o superiore) è un requisito AWS Partner Network per i partner tecnologici di livello avanzato. Per qualificarti nel livello avanzato, devi attivare il supporto Business su almeno uno dei tuoi account AWS.	Sì	No	
4.0 Efficienza delle prestazioni Il pilastro dell'efficienza delle prestazioni si concentra sull'utilizzo efficiente di risorse IT e di calcolo. Gli argomenti principali includono la selezione delle dimensioni e dei tipi appropriati di risorse in base ai requisiti dei carichi di lavoro, il monitoraggio delle prestazioni e il prendere decisioni informate per mantenere l'efficienza mentre il business evolve.				
4.1 Il test delle prestazioni viene abilitato in seguito alle distribuzioni	Definisci target di prestazioni misurabili e fai eseguire dei test delle prestazioni per verificare che tali target siano raggiunti prima di un rilascio in produzione.	Sì	Sì	
4.2 Soglie di monitoraggio adottate	Monitora le prestazioni dell'applicazione e adotta meccanismi che attivino degli allarmi al superamento delle soglie.	Sì	Sì	

Risorse AWS:

Titolo	Descrizione
Come costruire una landing page sulla prassi	Fornisce una guida su come costruire una pagina delle prassi/soluzioni che risponda ai prerequisiti del programma.
Come scrivere un caso di studio pubblico	Fornisce una guida su come scrivere un caso di studio pubblico che risponda ai prerequisiti del programma.
Come costruire un diagramma architetturale	Fornisce una guida su come costruire un diagramma architetturale che risponda ai prerequisiti del programma.
Documentazione sulla disponibilità del partner	Fornisce una guida e indica esempi di best practice dei prerequisiti del Programma.
Sito web secondo i Canoni di Architettura AWS	Copre le best practice relative ai Canoni di Architettura