Cloud Management Services

Servizi informatici e amministrativi a portata di Cloud
IT and administrative services in a cloud

Questionario di valutazione del consenso CSA STAR Self-Assessment

Sicurezza delle applicazioni e dell'interfaccia		
Sicurezza dell'applicazione	Utilizzi standard di settore (benchmark Build Security in Maturity Model [BSIMM], Open Group ACS Trusted Technology Provider Framework, NIST, ecc.) Per integrare la sicurezza per il tuo SDLC (Systems / Software Development Lifecycle)?	NO
	Utilizzi uno strumento di analisi del codice sorgente automatizzato per rilevare i difetti di sicurezza nel codice prima della produzione?	NO
	Utilizzi l'analisi manuale del codice sorgente per rilevare i difetti di sicurezza nel codice prima della produzione?	SI
	Verificate che tutti i vostri fornitori di software aderiscano agli standard di settore per la sicurezza del ciclo di vita dei sistemi / sviluppo software (SDLC)?	N/A
	(Solo SaaS) Verifichi le vulnerabilità di sicurezza delle tue applicazioni e risolvi eventuali problemi prima della distribuzione alla produzione?	SI
Requisiti di accesso dei clienti	Tutti i requisiti di sicurezza, contrattuali e normativi identificati per l'accesso dei clienti vengono affrontati contrattualmente e risolti prima di concedere ai clienti l'accesso a dati, risorse e sistemi informativi?	SI
	Tutti i requisiti e i livelli di fiducia per l'accesso dei clienti sono definiti e documentati?	SI
Integrità dei dati	Le routine di integrità di input e output dei dati (ad esempio, riconciliazione e controlli di modifica) sono implementate per le interfacce dell'applicazione e i database per prevenire errori di elaborazione manuali o sistematici o il danneggiamento dei dati?	SI
Sicurezza / integrità dei dati	La tua architettura di sicurezza dei dati è progettata utilizzando uno standard di settore (ad esempio, CDSA, MULITSAFE, CSATrusted Cloud Architectural Standard, FedRAMP, CAESARS)?	N/A
Garanzia e conformità degli audit		
Pianificazione degli audit	Producete asserzioni di audit utilizzando un formato strutturato e accettato dal settore (ad es. CloudAudit / A6 URI Ontology, CloudTrust, SCAP / CYBEX, GRC XML, Cloud Computing Management Audit / Assurance Program di ISACA, ecc.)?	N/A
Audit indipendenti	Consentite agli inquilini di visualizzare i report di audit o certificazione SOC2 / ISO 27001 o simili di terze parti?	N/A
	Conduci regolarmente test di penetrazione della rete della tua infrastruttura di servizi cloud come prescritto dalle best practice e dalle linee guida del settore?	SI
	Conduci regolarmente test di penetrazione delle applicazioni della tua infrastruttura cloud come prescritto dalle best practice e dalle linee guida del settore?	SI
	Conducete regolarmente audit interni come prescritto dalle migliori pratiche e linee guida del settore?	SI
	Conducete regolarmente audit esterni come prescritto dalle migliori pratiche e linee guida del settore?	NO
	I risultati delle prove di penetrazione sono a disposizione degli inquilini su loro richiesta?	SI
	I risultati degli audit interni ed esterni sono a disposizione dei locatari su loro richiesta?	SI

Garanzia e conformità degli audit			
Audit indipendenti	Hai un programma di audit interno che consenta l'audit interfunzionale delle valutazioni?	NO	
Mappatura normativa del sistema informativo	Hai la capacità di segmentare logicamente o crittografare i dati dei clienti in modo tale che i dati possano essere prodotti solo per un singolo ente, senza accedere inavvertitamente ai dati di un altro ente?	SI	
	Hai la capacità di recuperare i dati per un cliente specifico in caso di guasto o perdita di dati?	SI	
	Hai la capacità di limitare la memorizzazione dei dati dei clienti a specifici paesi o località geografiche?	SI	
	Hai un programma in atto che include la capacità di monitorare le modifiche ai requisiti normativi nelle giurisdizioni pertinenti, adattare il tuo programma di sicurezza per le modifiche ai requisiti legali e garantire la conformità ai requisiti normativi pertinenti?	NO	
Gestione della continuità operativa e resilienza operativa			
Pianificazione della continuità aziendale	Offrite agli inquilini opzioni di hosting geograficamente resistenti?	SI	
	Fornite agli enti la capacità di failover del servizio di infrastruttura ad altri provider?	N/A	
Test di continuità aziendale	I piani di continuità aziendale sono soggetti a test a intervalli pianificati oa modifiche organizzative o ambientali significative per garantire un'efficacia continua?	SI	
Alimentazione / Telecomunicazioni	Fornite agli inquilini la documentazione che mostra il percorso di trasporto dei loro dati tra i vostri sistemi?	SI	Il nostro provider IaaS si trova in Italia e il trasporto dei dati è limitato in questo data center fisico.
	Gli inquilini possono definire come vengono trasportati i propri dati e attraverso quali giurisdizioni legali?	SI	Il servizio Cms/Openyourcloud SaaS è limitato a un singolo paese (il nostro provider IaaS si trova in Italia). I dati del cliente rimarrannoall'interno di questo paese
Documentazione	I documenti del Sistema informativo (ad esempio, manuali dell'amministratore e dell'utente, schemi di architettura, ecc.) Sono messi a disposizione del personale autorizzato per garantire la configurazione, l'installazione e il funzionamento del Sistema informativo?	N/A	
Rischi ambientali	La protezione fisica contro i danni (ad esempio, cause naturali, disastri naturali, attacchi deliberati) è prevista e progettata con le contromisure applicate?	SI	
Ubicazione delle apparecchiature	I vostri data center si trovano in luoghi che hanno un'alta probabilità / verificarsi di rischi ambientali ad alto impatto (inondazioni, tornado, terremoti, uragani, ecc.)?	NO	
Manutenzione delle apparecchiature	Se si utilizza l'infrastruttura virtuale, la soluzione cloud include funzionalità di ripristino e ripristino hardware indipendenti?	N/A	
	Se si utilizza l'infrastruttura virtuale, si fornisce agli enti la capacità di ripristinare una macchina virtuale a uno stato precedente nel tempo?	N/A	Cms/Openyourcloud fornisce solo SaaS
	Se si utilizza l'infrastruttura virtuale, si consente il download e il trasferimento delle immagini della macchina virtuale su un nuovo provider cloud?	N/A	Cms/Openyourcloud fornisce solo SaaS
	Se si utilizza l'infrastruttura virtuale, le immagini della macchina vengono messe a disposizione del cliente in un modo che consenta al cliente di replicare quelle immagini nella propria posizione di archiviazione off-site?	N/A	Cms/Openyourcloud fornisce solo SaaS
	La tua soluzione cloud include funzionalità di ripristino e ripristino indipendenti dal software / provider?	SI	
Interruzioni di corrente dell'apparecchiatura	Sono implementati meccanismi di sicurezza e ridondanze per proteggere le apparecchiature dalle interruzioni dei servizi di pubblica utilità (ad esempio, interruzioni di corrente, interruzioni di rete, ecc.)?	SI	

Gestione della continuità operativa e resilienza operativa		
Analisi d'impatto	Fornite agli inquilini visibilità e reporting continui sulle prestazioni del vostro contratto di servizio operativo (SLA)?	NO
	Metti a disposizione dei tuoi inquilini metriche di sicurezza delle informazioni basate su standard (CSA, CAMM, ecc.)?	NO
	Fornite ai clienti visibilità e reporting continui sulle prestazioni del vostro SLA?	NO
Politica	Le politiche e le procedure sono stabilite e messe a disposizione di tutto il personale per supportare adeguatamente i ruoli delle operazioni dei servizi?	SI
Politica di conservazione	Disponete di capacità di controllo tecnico per applicare i criteri di conservazione dei dati degli inquilini?	SI
	Hai una procedura documentata per rispondere alle richieste di dati sui locatari da parte di governi o terze parti?	SI
	Hai implementato meccanismi di backup o ridondanza per garantire la conformità ai requisiti normativi, legali, contrattuali o aziendali?	SI
	Testate i vostri meccanismi di backup o ridondanza almeno una volta all'anno?	SI
Controllo delle modifiche e gestione della configurazione		
Nuovo sviluppo / acquisizione	Sono stabilite politiche e procedure per l'autorizzazione alla gestione per lo sviluppo o l'acquisizione di nuove applicazioni, sistemi, database, infrastrutture, servizi, operazioni e strutture?	SI
	È disponibile la documentazione che descrive l'installazione, la configurazione e l'uso di prodotti / servizi / funzionalità?	SI
Sviluppo in outsourcing	Sono disponibili controlli per garantire che gli standard di qualità vengano rispettati per tutto lo sviluppo del software?	SI
	Sono disponibili controlli per rilevare i difetti di sicurezza del codice sorgente per qualsiasi attività di sviluppo software in outsourcing?	SI
Test di qualità	Fornite ai vostri inquilini la documentazione che descrive il vostro processo di garanzia della qualità?	NO
	È disponibile la documentazione che descrive problemi noti con determinati prodotti / servizi?	SI
	Sono in atto politiche e procedure per valutare e correggere i bug segnalati e le vulnerabilità di sicurezza per le offerte di prodotti e servizi?	SI
	Sono in atto meccanismi per garantire che tutti gli elementi del codice di debug e di test vengano rimossi dalle versioni software rilasciate?	SI
Installazioni di software non autorizzate	Sono disponibili controlli per limitare e monitorare l'installazione di software non autorizzato sui propri sistemi?	SI
Modifiche alla produzione	Fornite agli inqulini la documentazione che descrive le vostre procedure di gestione del cambiamento di produzione e i loro ruoli / diritti / responsabilità al suo interno?	NO
Sicurezza dei dati e gestione del ciclo di vita delle informazioni		
Classificazione	Fornite la capacità di identificare le macchine virtuali tramite tag / metadati dei criteri (ad esempio, i tag possono essere utilizzati per limitare i sistemi operativi guest dall'avvio / istanziazione / trasporto di dati nel paese sbagliato)?	N/A
	Fornite la capacità di identificare l'hardware tramite tag di criteri / metadati / tag hardware (ad es.TXT / TPM, tag VN, ecc.)?	N/A

Sicurezza dei dati e gestione del ciclo di vita delle informazioni			
Classificazione	Hai la capacità di utilizzare la posizione geografica del sistema come fattore di autenticazione?	SI	
	Potete fornire la posizione fisica / geografica di archiviazione dei dati di un ente su richiesta?	SI	Le istanze di Cms/Openyourcloud SaaS sono limitate a un singolo paese oregione geografica in un cloud privato in Italia.
	Potete fornire in anticipo la posizione fisica / geografia dell'archiviazione dei dati di un ente?	SI	Le istanze di Cms/Openyourcloud SaaS sono limitate a un singolo paese oregione geografica in un cloud privato in Italia.
	Seguite uno standard di etichettatura dei dati strutturato (ad esempio, ISO 15489, Oasis XML Catalog Spécification, CSA data type guidance)?	N/A	L'organizzazione segue le migliori pratiche e gli standard di interoperabilità della pubblica amministrazione (governo locale) per la gestione dei dati
	Consentite agli enti di definire posizioni geografiche accettabili per il routing dei dati o la creazione di istanze delle risorse?	N/A	Le istanze di Cms/Openyourcloud SaaS sono limitate a un singolo paese oregione geografica in un cloud privato in Italia.
Flusso / inventario dei dati	Inventate, documentate e mantenete i flussi di dati per i dati residenti (permanenti o temporanei) all'interno delle applicazioni dei servizi e della rete e dei sistemi dell'infrastruttura?	SI	Le istanze di Cms/Openyourcloud SaaS sono limitate a un singolo paese oregione geografica in un cloud privato in Italia.
	Potete garantire che i dati non migrino oltre una determinata residenza geografica?	SI	Le istanze di Cms/Openyourcloud SaaS sono limitate a un singolo paese oregione geografica in un cloud privato in Italia.
Transazioni e-commerce	Fornisci metodologie di crittografia aperte (3.4ES, AES, ecc.) Agli inquilini in modo che possano proteggere i loro dati se è necessario spostarsi attraverso reti pubbliche (ad esempio, Internet)?	SI	
	Utilizzi metodologie di crittografia aperte ogni volta che i componenti della tua infrastruttura devono comunicare tra loro tramite reti pubbliche (ad esempio, replica dei dati basata su Internet da un ambiente a un altro)?	SI	
Gestione / etichettatura / politica di sicurezza	Sono state stabilite politiche e procedure per l'etichettatura, la gestione e la sicurezza dei dati e degli oggetti che contengono dati?	N/A	
	I meccanismi per l'ereditarietà delle etichette sono implementati per gli oggetti che fungono da contenitori aggregati per i dati?	N/A	
Dati non di produzione	Sono in atto procedure per garantire che i dati di produzione non vengano replicati o utilizzati in ambienti non di produzione?	SI	Cms/Openyourcloud mantiene pratiche percontrollare l'utilizzo dei dati di produzione.
Proprietà / amministrazione	Le responsabilità relative alla gestione dei dati sono definite, assegnate, documentate e comunicate?	SI	
Smaltimento sicuro	Supportate la cancellazione sicura (ad esempio, smagnetizzazione / cancellazione crittografica) dei dati archiviati e di cui è stato eseguito il backup come determinato dall'ente?	SI	Cms/Openyourcloud utilizza provider cloud Infrastructure as a Service (laaS)per fornire l'eliminazione sicura dei dati.
	Potete fornire una procedura pubblicata per uscire dall'accordo di servizio, inclusa la garanzia di disinfettare tutte le risorse di elaborazione dei dati dell'ente una volta che un cliente è uscito dal vostro ambiente o ha lasciato una risorsa?	SI	
Sicurezza del datacenter			
Gestione delle risorse	Mantieni un inventario completo di tutti i tuoi asset critici che include la proprietà del bene?	SI	
	Mantenete un inventario completo di tutte le vostre relazioni con i fornitori critici?	SI	

Sicurezza del datacenter			
Punti di accesso controllati	Sono implementati i perimetri di sicurezza fisica (ad esempio recinzioni, muri, barriere, guardie, cancelli, sorveglianza elettronica, meccanismi di autenticazione fisica, banchi di accettazione e pattuglie di sicurezza)?	N/A	
Identificazione dell'equipaggiamento	L'identificazione automatizzata delle apparecchiature viene utilizzata come metodo per convalidare l'integrità dell'autenticazione della connessione in base alla posizione nota dell'apparecchiatura?	SI	Cms/Openyourcloud si avvale di partner IaaS per fornire la sicurezza deldatacenter, inclusa l'identificazione delle apparecchiature.
Autorizzazione fuori sede	Fornite agli enti la documentazione che descrive scenari in cui i dati possono essere spostati da una posizione fisica a un'altra (ad esempio, backup offsite, failover della continuità aziendale, replica)?	SI	
Attrezzatura fuori sede	Potete fornire agli enti le prove che documentano le vostre politiche e procedure che governano la gestione delle risorse e il riutilizzo delle attrezzature?	SI	
Linea di condotta	Potete fornire prove che siano state stabilite politiche, standard e procedure per mantenere un ambiente di lavoro sicuro e protetto in uffici, stanze, strutture e aree protette?	SI	
	Potete fornire prove che il vostro personale e le terze parti coinvolte siano state addestrate in merito alle vostre politiche, standard e procedure documentate?	SI	
Autorizzazione area sicura	Consentite agli inquilini di specificare in quale delle vostre posizioni geografiche i loro dati possono spostarsi da / verso (per affrontare considerazioni legali sulla giurisdizione in base a dove i dati sono archiviati rispetto a cui si accede)?	SI	Le istanze di Cms/Openyourcloud SaaS sono limitate a un singolo paese (Italia).
Ingresso di persone non autorizzate	I punti di ingresso e di uscita, come le aree di servizio e altri punti in cui personale non autorizzato può entrare nei locali, sono monitorati, controllati e isolati dall'archiviazione e dal processo dei dati?	SI	Cms/Openyourcloud si avvale di partner IaaS per fornire sicurezza fisica. Come minimo, i controlli di sicurezza fisica includono controlli perimetrali come controllo di accesso, recinzioni, muri, personale di sicurezza, videosorveglianza, sistemi di rilevamento delle intrusioni e altri mezzi elettronici. L'accesso fisico alle strutture che ospitano l'hardware dell'infrastruttura è limitato dai Controlli di accesso al sito per garantire che l'accesso sia consentito solo alle persone appropriate.
Accesso utente	Limitate l'accesso fisico alle risorse e alle funzioni delle informazioni da parte degli utenti e del personale di supporto?	SI	
Crittografia e gestione delle chiavi			
Diritto	Disponete di politiche di gestione delle chiavi che vincolano le chiavi a proprietari identificabili?	N/A	
Generazione delle chiavi	Hai la capacità di consentire la creazione di chiavi di crittografia univoche per ente?	SI	Cms/Openyourcloud mantiene politiche e pratiche per le proprie istanze SaaS per la gestione delle chiavi di crittografia e dei certificati. Le chiavi di crittografia non vengono distribuite o gestite in base all'ente. La crittografia può essereapplicata al file o alla cartella.
	Hai la capacità di gestire le chiavi di crittografia per conto dell'ente?	SI	
	Mantenete procedure di gestione delle chiavi?	N/A	
	Hai documentato la proprietà per ogni fase del ciclo di vita delle chiavi di crittografia?	N/A	
	Utilizzi framework di terze parti / open source / proprietari per gestire le chiavi di crittografia?	N/A	

Crittografia e gestione delle chiavi			
Crittografia	Crittografi i dati dell'ente a riposo (su disco / archiviazione) nel tuo ambiente?	SI	
	Utilizzi la crittografia per proteggere i dati e le immagini delle macchine virtuali durante il trasporto attraverso e tra le reti e le istanze dell'hypervisor?	N/A	
	Supportate le chiavi di crittografia generate dall'ente o consentite all'ente di crittografare i dati in un'identità senza accesso a un certificato di chiave pubblica (ad esempio, crittografia basata sull'identità)?	N/A	
	Disponete di documentazione che stabilisce e definisce le vostre politiche, procedure e linee guida per la gestione della crittografia?	N/A	
Archiviazione e accesso	Disponi di una crittografia adeguata alla piattaforma e ai dati che utilizza formati aperti / convalidati e algoritmi standard?	SI	
	Le tue chiavi di crittografia sono gestite dal consumatore cloud o da un provider di gestione delle chiavi affidabile?	SI	
	Memorizzate le chiavi di crittografia nel cloud?	N/A	
	Avete funzioni separate per la gestione delle chiavi e per l'utilizzo delle chiavi?	N/A	
Governance e gestione dei rischi			
Requisiti di base	Hai documentato le linee di base della sicurezza delle informazioni per ogni componente della tua infrastruttura (ad es. Hypervisor, sistemi operativi, router, server DNS, ecc.)?	N/A	
	Hai la capacità di monitorare e segnalare continuamente la conformità della tua infrastruttura rispetto alle linee di base della sicurezza delle informazioni?	SI	
	Consentite ai vostri clienti di fornire la propria immagine di macchina virtuale affidabile per garantire la conformità ai propri standard interni?	N/A	La piattaforma viene fornita come Software as a Service (SaaS). Pertanto, i clienti di utilizzano risorse applicative condivise e macchinevirtuali, quindi Cms/Openyourcloud non fornisce loro le proprie macchine virtuali.
Valutazioni dei rischi	Fornite dati sull'integrità del controllo di sicurezza per consentire agli enti di implementare il monitoraggio continuo standard del settore (che consente la convalida continua dell'ente del vostro stato di controllo fisico e logico)?	N/A	La piattaforma viene fornita come Software as a Service (SaaS). Pertanto, i clienti di utilizzano risorse applicative condivise e macchinevirtuali. Cms/Openyourcloud monitora continuamente i dati dei controlli di sicurezza ma non divulga regolarmente tali informazioni ai clienti.
	Effettuate valutazioni del rischio associate ai requisiti di governance dei dati almeno una volta all'anno?	N/A	
Supervisione della direzione	I vostri responsabili tecnici, aziendali e esecutivi sono responsabili del mantenimento della consapevolezza e della conformità con le politiche, le procedure e gli standard di sicurezza sia per se stessi che per i loro dipendenti in quanto riguardano l'area di responsabilità del manager e dei dipendenti?	N/A	
Programma di gestione	Fornite agli inquilini la documentazione che descrive il vostro programma ISMP (Information Security Management Program)?	N/A	
	Rivedi il tuo programma di gestione della sicurezza delle informazioni (ISMP) almeno una volta all'anno?	SI	
Supporto / coinvolgimento della direzione	Assicuri che i tuoi fornitori aderiscano alle tue politiche sulla sicurezza delle informazioni e sulla privacy?	SI	

Governance e gestione dei rischi		
Policy	Le tue politiche sulla privacy e sulla sicurezza delle informazioni sono in linea con gli standard del settore (ISO-27001, ISO-22307, CoBIT, ecc.)?	N/A
	Hai accordi per garantire che i tuoi fornitori aderiscano alle tue politiche sulla sicurezza delle informazioni e sulla privacy?	N/A
	Potete fornire prove della mappatura di due diligence dei vostri controlli, architettura e processi rispetto a regolamenti e / o standard?	N/A
	Divulga a quali controlli, standard, certificazioni e / o regolamenti rispetti?	N/A
Applicazione delle politiche	È stata stabilita una politica disciplinare o sanzionatoria formale per i dipendenti che hanno violato le politiche e le procedure di sicurezza?	SI
	I dipendenti sono informati su quali azioni potrebbero essere intraprese in caso di violazione tramite le loro politiche e procedure?	SI
Impatti del cambiamento di politica aziendale	I risultati della valutazione del rischio includono aggiornamenti a policy, procedure, standard e controlli di sicurezza per garantire che rimangano pertinenti ed efficaci?	SI
Revisioni delle linee di condotta	Informi i tuoi inquilini quando apporti modifiche sostanziali alla sicurezza delle informazioni e / o alle politiche sulla privacy?	SI
	Esegui almeno revisioni annuali delle tue politiche sulla privacy e sulla sicurezza?	SI
Valutazioni	Le valutazioni dei rischi formali sono allineate con il framework a livello aziendale ed eseguite almeno una volta all'anno, o ad intervalli pianificati, determinando la probabilità e l'impatto di tutti i rischi identificati, utilizzando metodi qualitativi e quantitativi?	N/A
	La probabilità e l'impatto associati al rischio inerente e residuo sono determinati indipendentemente, considerando tutte le categorie di rischio (ad es. Risultati dell'audit, analisi di minacce e vulnerabilità e conformità normativa)?	N/A
Programma	Disponete di un programma documentato a livello di organizzazione per la gestione del rischio?	N/A
	Rendete disponibile la documentazione del vostro programma di gestione del rischio a livello di organizzazione?	N/A
Risorse umane		
Rendimenti degli asset	Sono in atto sistemi per monitorare le violazioni della privacy e informare tempestivamente gli inquilini se un evento relativo alla privacy può avere avuto un impatto sui loro dati?	SI
	La tua politica sulla privacy è allineata agli standard del settore?	SI
Controllo sullo sfondo	Ai sensi delle leggi locali, dei regolamenti, dell'etica e dei vincoli contrattuali, tutti i candidati all'assunzione, gli appaltatori e le terze parti coinvolte sono soggetti a verifica?	SI
Contratti di lavoro	Formate specificamente i vostri dipendenti riguardo al loro ruolo specifico e ai controlli di sicurezza delle informazioni che devono svolgere?	SI
	Documentate il riconoscimento dei dipendenti della formazione che hanno completato?	SI
	Tutto il personale è tenuto a firmare NDA o Accordi di riservatezza come condizione di impiego per proteggere le informazioni dei clienti / inquilini?	SI
	Il completamento corretto e tempestivo del programma di formazione è considerato un prerequisito per l'acquisizione e il mantenimento dell'accesso a sistemi sensibili?	SI

Risorse umane		
Contratti di lavoro	Il personale viene formato e fornito di programmi di sensibilizzazione almeno una volta all'anno?	SI
Risoluzione del rapporto di lavoro	Sono in atto politiche, procedure e linee guida documentate per governare il cambiamento del rapporto di lavoro e / o il licenziamento?	SI
	Le procedure e le linee guida di cui sopra tengono conto della revoca tempestiva dell'accesso e della restituzione dei beni?	SI
Dispositivi portatili / mobili	Sono state stabilite politiche e procedure e sono state implementate misure per limitare rigorosamente l'accesso ai dati sensibili e ai dati degli inquilini da dispositivi portatili e mobili (ad esempio, laptop, telefoni cellulari e assistenti digitali personali (PDA)), che sono generalmente a più alto rischio rispetto ai non dispositivi portatili (ad esempio, computer desktop presso le strutture dell'organizzazione del fornitore)?	SI
Accordi di non divulgazione	I requisiti per gli accordi di non divulgazione o riservatezza che riflettono le esigenze dell'organizzazione per la protezione dei dati e dei dettagli operativi sono identificati, documentati e riesaminati a intervalli pianificati?	SI
Ruoli e Responsabilità	Fornite agli enti un documento di definizione del ruolo che chiarisca le vostre responsabilità amministrative rispetto a quelle dell'ente?	SI
Uso accettabile	Fornite documentazione su come accedere ai dati e ai metadati dell'ente?	SI
	Raccogli o crei metadati sull'utilizzo dei dati degli enti tramite tecnologie di ispezione (ad es. Motori di ricerca, ecc.)?	NO
	Consentite agli inquilini di rinunciare all'accesso ai propri dati / metadati tramite tecnologie di ispezione?	N/A
Formazione / Consapevolezza	Fornisci un programma di formazione formale, basato sui ruoli e sulla consapevolezza della sicurezza per l'accesso al cloud e le questioni relative alla gestione dei dati (ad es. Multi-tenancy, nazionalità, modello di consegna del cloud, implicazioni di segregazione dei compiti e conflitti di interesse) per accesso ai dati dell'ente?	SI
	Gli amministratori e gli amministratori dei dati sono adeguatamente istruiti sulle loro responsabilità legali in materia di sicurezza e integrità dei dati?	SI
Responsabilità dell'utente	Gli utenti sono consapevoli delle loro responsabilità per mantenere la consapevolezza e la conformità con le politiche di sicurezza pubblicate, le procedure, gli standard e i requisiti normativi applicabili?	SI
	Gli utenti sono consapevoli delle loro responsabilità per il mantenimento di un ambiente di lavoro sicuro e protetto?	SI
	Gli utenti sono consapevoli delle loro responsabilità nel lasciare le apparecchiature incustodite in modo sicuro?	SI
Luogo di lavoro	Le politiche e le procedure di gestione dei dati affrontano i conflitti di interessi degli enti e dei livelli di servizio?	SI
	Le politiche e le procedure di gestione dei dati includono un controllo delle manomissioni o una funzione di integrità del software per l'accesso non autorizzato ai dati dell'ente?	SI
	L'infrastruttura di gestione della macchina virtuale include un controllo delle manomissioni o una funzione di integrità del software per rilevare le modifiche alla build / configurazione della macchina virtuale?	SI
Gestione di identità e accessi		
Accesso agli strumenti di controllo	Limiti, registri e monitori l'accesso ai tuoi sistemi di gestione della sicurezza delle informazioni (ad es. Hypervisor, firewall, scanner di vulnerabilità, sniffer di rete, API, ecc.)?	SI
	Monitorate e registrate l'accesso privilegiato (ad es., Livello amministratore) ai sistemi di gestione della sicurezza delle informazioni?	SI
Politica di accesso degli utenti	Disponete di controlli che assicurano la rimozione tempestiva dell'accesso ai sistemi che non è più necessario per scopi aziendali?	SI

Gestione di identità e accessi			
Politica di accesso degli utenti	Fornite metriche per monitorare la velocità con cui siete in grado di rimuovere l'accesso ai sistemi che non è più necessario per scopi aziendali?	SI	
Accesso alle porte di diagnostica / configurazione	Utilizzi reti sicure dedicate per fornire accesso di gestione alla tua infrastruttura di servizi cloud?	SI	
Politiche e procedure	Gestisci e memorizzi l'identità di tutto il personale che ha accesso all'infrastruttura IT, compreso il loro livello di accesso?	SI	
	Gestisci e memorizzi l'identità dell'utente di tutto il personale che ha accesso alla rete, compreso il loro livello di accesso?	SI	
Separazione dei compiti	Fornite agli inquilini la documentazione su come mantenere la separazione dei compiti all'interno della vostra offerta di servizi cloud?	NO	
Restrizione all'accesso al codice sorgente	Sono in atto controlli per impedire l'accesso non autorizzato all'applicazione, al programma o al codice sorgente dell'oggetto e per garantire che sia limitato solo al personale autorizzato?	SI	
	Sono in atto controlli per impedire l'accesso non autorizzato all'applicazione dell'ente, al programma o al codice sorgente dell'oggetto e per garantire che sia limitato al solo personale autorizzato?	N/A	
Accesso di terze parti	Fornite funzionalità di ripristino di emergenza per più guasti?	SI	
	Monitorate la continuità del servizio con i fornitori a monte in caso di guasto del fornitore?	SI	
	Hai più di un fornitore per ogni servizio da cui dipendi?	NO	Cms/Openyourcloud si affida alla ridondanzadei propri fornitori laaS. nostri fornitori laaS dispongono di fornitori ridondanti per servizi di data center critici.
	Fornite l'accesso alla ridondanza operativa e ai riepiloghi di continuità, inclusi i servizi da cui dipendete?	NO	
	Offrite all'ente la possibilità di dichiarare un disastro?	NO	Cms/Openyourcloud si riserva il diritto di dichiarare un disastro.
	Fornite un'opzione di failover attivata dall'ente?	NO	La piattaforma effettua automaticamente il failover su un'infrastruttura ridondante in caso di emergenza.
	Condividete i vostri piani di continuità aziendale e ridondanza con i vostri inquilini?	NO	
Restrizione / autorizzazione dell'accesso dell'utente	Documenti come concedi e approvi l'accesso ai dati dell'ente?	SI	

Gestione di identità e accessi			
Restrizione / autorizzazione dell'accesso dell'utente	dati dei Disponete di un metodo per allineare le metodologie di classificazione dei dati di provider e enti ai fini del controllo degli accessi?	SI	Cms/Openyourcloud tratta tutti i clienti all'interno della Piattaforma allo stesso livello limitato.
Autorizzazione all'accesso dell'utente	La tua direzione fornisce l'autorizzazione e le restrizioni per l'accesso degli utenti (ad es. Dipendenti, appaltatori, clienti (inquilini), partner commerciali e / o fornitori) prima del loro accesso ai dati ea qualsiasi applicazione e infrastruttura posseduta o gestita (fisica e virtuale) Sistemi e componenti di rete?	SI	
	Fornite su richiesta l'accesso degli utenti (ad es. Dipendenti, appaltatori, clienti (enti, partner commerciali e / o fornitori) ai dati e alle applicazioni (fisiche e virtuali) possedute o gestite, sistemi di infrastruttura e componenti di rete?	N/A	
Revisioni di accesso degli utenti	È necessaria una certificazione almeno annuale dei diritti per tutti gli utenti e gli amministratori di sistema (esclusi gli utenti gestiti dagli enti)?	SI	
	Se si scopre che gli utenti hanno diritti inappropriati, vengono registrate tutte le azioni di riparazione e certificazione?	SI	
	Condividerai i rapporti di correzione e certificazione dei diritti degli utenti con i tuoi enti, se ai dati dell'ente potrebbe essere stato consentito un accesso inappropriato?	SI	Cms/Openyourcloud non condivide gli elenchi di accesso degli utenti. Tuttavia, se dovesse verificarsi un incidente, le parti appropriate verranno informate e verranno condivisi i livelli appropriati di sforzi di riparazione e rapporti di certificazione.
Revoca dell'accesso dell'utente	Il deprovisioning, la revoca o la modifica tempestiva dell'accesso degli utenti ai sistemi, alle risorse informative e ai dati dell'organizzazione vengono implementati in caso di modifica dello stato di dipendenti, appaltatori, clienti, partner commerciali o terze parti coinvolte?	SI	
	Eventuali modifiche allo stato di accesso degli utenti intendono includere la risoluzione del rapporto di lavoro, contratto o accordo, cambio di impiego o trasferimento all'interno dell'organizzazione?	SI	
Credenziali User-ID	Supportate l'uso o l'integrazione con le soluzioni Single Sign On (SSO) esistenti basate sul cliente per il vostro servizio?	N/A	
	Utilizzi standard aperti per delegare le funzionalità di autenticazione ai tuoi enti?	N/A	
	Supportate gli standard di federazione delle identità (ad esempio, SAML, SPML, WS-Federation, ecc.) Come mezzo per autenticare / autorizzare gli utenti?	N/A	
	Si dispone di una capacità di punto di applicazione delle politiche (ad esempio, XACML) per applicare i vincoli legali e politici regionali sull'accesso degli utenti?	NO	
	Si dispone di un sistema di gestione delle identità (che consente la classificazione dei dati per un ente) per consentire l'autorizzazione ai dati sia basata sui ruoli che basata sul contesto?	SI	Cms/Openyourcloud, su richiesta del cliente, può abilitare restrizioni di accesso alla Piattaforma Customer Satisfaction basata su IP
	Fornite agli inquilini opzioni di autenticazione forti (multifattore) (ad esempio certificati digitali, token, biométries, ecc.) per l'accesso degli utenti?	SI	
	Consentite agli enti di utilizzare servizi di garanzia dell'identità di terze parti?	SI	La piattaforma Customer Satisfaction supporta servizi di garanzia dell'identità di terze parti come SPID.

Gestione di identità e accessi			
Credenziali User-ID	Supportate l'applicazione dei criteri per password (ad es. Lunghezza minima, età, cronologia, complessità) e blocco dell'account (ad es. Soglia di blocco, durata del blocco)?	SI	
	Consentite agli inquilini / clienti di definire criteri di blocco della password e dell'account per i loro account?	NO	
	Supportate la possibilità di forzare le modifiche della password al primo accesso?	SI	
	Disponete di meccanismi per sbloccare gli account che sono stati bloccati (ad esempio, self-service tramite e-mail, domande di verifica definite, sblocco manuale)?	SI	
Accesso ai programmi di utilità	Le utilità che possono gestire in modo significativo le partizioni virtualizzate (ad es. Arresto, clonazione, ecc.) Sono adeguatamente limitate e monitorate?	SI	
	Hai la capacità di rilevare gli attacchi che prendono di mira direttamente esempio, shimming, Blue Pill, Hyper jumping, ecc.)?	N/A	I fornitori laaS della piattaforma l'infrastruttura virtuale (ad implementano funzionalità di sicurezza e controlli tecnici per proteggere le infrastrutture virtuali.
	Gli attacchi che prendono di mira l'infrastruttura virtuale vengono prevenuti con controlli tecnici?	SI	I fornitori laaS della piattaforma implementano funzionalità di sicurezza e controlli tecnici per proteggere le infrastrutture virtuali.
Sicurezza dell'infrastruttura e della virtualizzazione			
Registrazione audit / rilevamento intrusioni	Gli strumenti per l'integrità dei file (host) e per il rilevamento delle intrusioni di rete (IDS) sono implementati per facilitare il rilevamento tempestivo, l'indagine per analisi della causa principale e la risposta agli incidenti?	SI	
	L'accesso degli utenti fisici e logici ai log di controllo è limitato al personale autorizzato?	SI	
	Potete fornire la prova che è stata eseguita un'adeguata diligente mappatura di regole e standard per i vostri controlli / architettura / processi?	N/A	
	I registri di controllo vengono archiviati e conservati centralmente?	SI	
	I registri di controllo vengono esaminati regolarmente per eventi di sicurezza (ad es. con strumenti automatizzati)?	SI	
Rilevamento delle modifiche	Registri e avvisi eventuali modifiche apportate alle immagini della macchina virtuale indipendentemente dal loro stato di esecuzione (ad esempio, dormiente, spento o in esecuzione)?	N/A	
	Le modifiche apportate alle macchine virtuali o lo spostamento di un'immagine e la successiva convalida dell'integrità dell'immagine vengono resi immediatamente disponibili ai clienti tramite metodi elettronici (ad es. Portali o avvisi)?	N/A	
Sincronizzazione dell'orologio	Utilizzi un protocollo di servizio dell'ora sincronizzato (ad esempio, NTP) per garantire che tutti i sistemi abbiano un riferimento temporale comune?	SI	
Capacità / pianificazione delle risorse	capacità delFornite la documentazione relativa a quali livelli di sottoscrizione eccessiva del sistema (ad esempio rete, archiviazione, memoria, I / O, ecc.) Mantenete e in quali circostanze / scenari?	SI	Cms/Openyourcloud monitora la sistema per garantire le prestazioni a tutti i clienti. Le risorse dell'hypervisor non vengono sovraccaricate.

Sicurezza dell'infrastruttura e della virtualizzazione			
Capacità / pianificazione delle risorse	capacità delLimitate l'uso delle capacità di sottoscrizione in eccesso di memoria presenti nell'hypervisor?	SI	Cms/Openyourcloud monitora la sistema per garantire le prestazioni a tutti i clienti. Le risorse dell'hypervisor non vengono sovraccaricate.
	capacità delI requisiti di capacità del sistema tengono conto delle esigenze di capacità attuali, previste e previste per tutti i sistemi utilizzati per fornire servizi agli inquilini?	SI	Cms/Openyourcloud monitora la sistema per garantire le prestazioni a tutti i clienti. Le risorse dell'hypervisor non vengono sovraccaricate.
	capacità delLe prestazioni del sistema sono monitorate e ottimizzate al fine di soddisfare continuamente i requisiti normativi, contrattuali e aziendali per tutti i sistemi utilizzati per fornire servizi agli inquilini?	SI	Cms/Openyourcloud monitora la sistema per garantire le prestazioni a tutti i clienti. Le risorse dell'hypervisor non vengono sovraccaricate.
Gestione delle vulnerabilità	Gli strumenti di servizi di valutazione della vulnerabilità della sicurezza si adattano alle tecnologie di virtualizzazione utilizzate (ad es., Virtualization aware)?	SI	
Sicurezza della rete	Per la tua offerta IaaS, fornisci ai clienti indicazioni su come creare un'equivalenza di un'architettura di sicurezza a più livelli utilizzando la un'offerta IaaS.tua soluzione virtualizzata?	N/A	Cms/Openyourcloud non ha
	Aggiornate regolarmente i diagrammi dell'architettura di rete che includono flussi di dati tra domini / zone di sicurezza?	N/A	
	Verifichi regolarmente l'adeguatezza dell'accesso / connettività consentiti (ad esempio, regole del firewall) tra i domini / zone di sicurezza all'interno della rete?	N/A	
	Tutti gli elenchi di controllo dell'accesso al firewall sono documentati con giustificazione aziendale?	N/A	
Protezione avanzata del sistema operativo e controlli di base	I sistemi operativi sono rafforzati per fornire solo le porte, i protocolli ei servizi necessari per soddisfare le esigenze aziendali utilizzando controlli tecnici (ad es. Antivirus, monitoraggio dell'integrità dei file e registrazione) come parte dello standard o del modello di build di base?	N/A	
Ambienti di produzione / non di produzione	Per la vostra offerta SaaS o PaaS, fornite agli enti ambienti separati per i processi di produzione e test?	N/A	
	Per la vostra offerta IaaS, fornite agli enti una guida su come creare dispone diambienti di produzione e test adeguati?	N/A	Cms/Openyourcloud non un'offerta IaaS.
	Separate logicamente e fisicamente gli ambienti di produzione e quelli non di produzione?	SI	
Segmentazione	Gli ambienti di sistema e di rete sono protetti da un firewall o firewall virtuale per garantire i requisiti di sicurezza dell'azienda e dei clienti?	N/A	
	Gli ambienti di sistema e di rete sono protetti da un firewall o firewall virtuale per garantire la conformità ai requisiti legislativi, normativi e contrattuali?	N/A	
	Gli ambienti di sistema e di rete sono protetti da un firewall o firewall virtuale per garantire la separazione degli ambienti di produzione e non di produzione?	N/A	
	Gli ambienti di sistema e di rete sono protetti da un firewall o firewall virtuale per garantire la protezione e l'isolamento dei dati sensibili?	N/A	
Sicurezza delle Macchine Virtuali - Protezione dei dati	I canali di comunicazione protetti e crittografati vengono utilizzati durante la migrazione di server fisici, applicazioni o dati su server virtuali?	N/A	
	Utilizzi una rete separata dalle reti a livello di produzione durante la migrazione di server fisici, applicazioni o dati a server virtuali?	N/A	

Sicurezza dell'infrastruttura e della virtualizzazione			
Sicurezza delle Macchine Virtuali – Rafforzamento dell'Hypervisor	Limitate l'accesso del personale a tutte le funzioni di gestione dell'hypervisor o alle console amministrative per i sistemi che ospitano sistemi virtualizzati basati sul principio del minimo privilegio e supportati tramite controlli tecnici (ad esempio, autenticazione a due fattori, audit trail, filtro degli indirizzi IP, firewall e TLS incapsulato comunicazioni alle console amministrative)?	N/A	
Sicurezza Wireless	Sono stabilite politiche e procedure e meccanismi configurati e implementati per proteggere il perimetro dell'ambiente di rete wireless e per limitare il traffico wireless non autorizzato?	N/A	
	Sono state stabilite politiche e procedure e implementati meccanismi per garantire che le impostazioni di sicurezza wireless siano abilitate con una crittografia avanzata per l'autenticazione e la trasmissione, sostituendo le impostazioni predefinite del fornitore (ad esempio, chiavi di crittografia, password, stringhe di comunità SNMP)?	N/A	
	Sono stabilite politiche e procedure e implementati meccanismi per proteggere gli ambienti di rete wireless e rilevare la presenza di dispositivi di rete non autorizzati (canaglia) per una disconnessione tempestiva dalla rete?	N/A	
Architettura della rete	I diagrammi dell'architettura di rete identificano chiaramente ambienti e flussi di dati ad alto rischio che possono avere impatti sulla conformità legale?	N/A	
	Implementate misure tecniche e applicate tecniche di difesa in profondità (ad esempio, analisi approfondita dei pacchetti, limitazione del traffico e black-holing) per il rilevamento e la risposta tempestiva agli attacchi basati sulla rete associati a modelli anomali di traffico in ingresso o in uscita (ad esempio, spoofing MAC e Attacchi di avvelenamento ARP) e / o attacchi DDoS (Distributed Denial of Service)?	N/A	
Interoperabilità e portabilità			
API	Pubblichi un elenco di tutte le API disponibili nel servizio e indichi quali sono standard e quali sono personalizzate?	SI	Le procedure API sono disponibili per i clienti della piattaforma che utilizzano la funzionalità API.
Richiesta dati	I dati dei clienti non strutturati sono disponibili su richiesta in un formato standard del settore (ad esempio, .doc, .xls o .pdf)?	SI	
Politica e legge	Fornisci politiche e procedure (ad esempio accordi sul livello di servizio) che disciplinano l'uso delle API per l'interoperabilità tra il tuo servizio e le applicazioni di terze parti?	SI	Le procedure API sono disponibili per i clienti della piattaforma che utilizzano la funzionalità API.
	Fornisci politiche e procedure (ad esempio accordi sul livello di servizio) che disciplinano la migrazione dei dati dell'applicazione da e verso il tuo servizio?	SI	I clienti della piattaforma hanno la capacità di esportare tutti i loro dati probatori. I clienti non sviluppano applicazioni sulla piattaforma .

Interoperabilità e portabilità		
Protocolli di rete standardizzati	È possibile eseguire l'importazione, l'esportazione dei dati e la gestione dei servizi tramite protocolli di rete standardizzati e sicuri accettati dal settore (ad es. testo non in chiaro e autenticato)?	N/A
	Fornite ai consumatori (enti) la documentazione che descrive in dettaglio gli standard di protocollo di rete di interoperabilità e portabilità pertinenti coinvolti?	N/A
Virtualizzazione	Utilizzi una piattaforma di virtualizzazione riconosciuta nel settore e formati di virtualizzazione standard (ad es. OVF) per garantire l'interoperabilità?	N/A
	Sono state documentate modifiche personalizzate apportate a qualsiasi hypervisor in uso e tutti gli hook di virtualizzazione specifici della soluzione disponibili per la revisione del cliente?	N/A

Sicurezza dei dispositivi mobili		
Anti-malware	Fornisci formazione anti-malware specifica per i dispositivi mobili come parte della tua formazione sulla consapevolezza della sicurezza delle informazioni?	N/A
Repository di applicazioni	Documentate e rendete disponibili elenchi approvati di store di applicationi per dispositivi mobili che accedono o archiviano dati aziendali e / o sistemi aziendali?	N/A
Applicazioni approvate	Si dispone di una capacità di applicazione delle policy (ad es. XACML) per garantire che solo le applicazioni approvate e quelle provenienti da application store approvati possano essere caricate su un dispositivo mobile?	N/A
Software approvato per BYOD (Bring Your Own Device)	La tua politica e formazione BYOD indica chiaramente quali applicazioni e archivi di applicazioni sono approvati per l'uso sui dispositivi BYOD?	N/A
Conoscenza e formazione	Nella formazione dei dipendenti disponi di una policy documentata sui dispositivi mobili che definisca chiaramente i dispositivi mobili e l'utilizzo e i requisiti accettati per i dispositivi mobili?	N/A
Servizi basati su cloud	Si dispone di un elenco documentato di servizi basati su cloud preapprovati che possono essere utilizzati per l'utilizzo e l'archiviazione dei dati aziendali aziendali tramite un dispositivo mobile?	N/A
Compatibilità	Hai un processo di convalida delle applicazioni documentato per testare i problemi di dispositivo, sistema operativo e compatibilità delle applicazioni?	N/A
Idoneità del dispositivo	Hai una policy BYOD che definisce i dispositivi e i requisiti di idoneità consentiti per l'utilizzo BYOD?	N/A
Inventario dei dispositivi	Mantieni un inventario di tutti i dispositivi mobili che archiviano e accedono ai dati aziendali che include lo stato del dispositivo (ad es., Sistema operativo e livelli di patch, smarrito o disattivato, dispositivo assegnato)?	N/A
Gestione dei dispositivi	Disponi di una soluzione di gestione centralizzata dei dispositivi mobili distribuita su tutti i dispositivi mobili a cui è consentito archiviare, trasmettere o elaborare i dati aziendali?	N/A
Crittografia	La policy del tuo dispositivo mobile richiede l'uso della crittografia per l'intero dispositivo o per i dati identificati come sensibili, applicabili tramite controlli tecnologici per tutti i dispositivi mobili?	N/A

Sicurezza dei dispositivi mobili		
Jailbreaking e rooting	La tua politica sui dispositivi mobili proibisce l'elusione dei controlli di sicurezza incorporati sui dispositivi mobili (ad esempio, jailbreak o rooting)?	N/A
	Disponi di controlli investigativi e preventivi sul dispositivo o tramite un sistema di gestione dei dispositivi centralizzato che vieta l'elusione dei controlli di sicurezza integrati?	N/A
Legale	La tua politica BYOD definisce chiaramente le aspettative di privacy, i requisiti per contenzioso, e-discovery e blocchi legali?	N/A
	Disponi di controlli investigativi e preventivi sul dispositivo o tramite un sistema di gestione dei dispositivi centralizzato che vieta l'elusione dei controlli di sicurezza integrati?	N/A
Schermata di blocco	Richiedi e imponi tramite controlli tecnici una schermata di blocco automatico per dispositivi BYOD e di proprietà dell'azienda?	N/A
Sistemi operativi	Gestisci tutte le modifiche ai sistemi operativi dei dispositivi mobili, ai livelli di patch e alle applicazioni tramite i processi di gestione delle modifiche della tua azienda?	N/A
Password	Sono disponibili criteri per le password per dispositivi mobili aziendali e / o dispositivi mobili BYOD?	N/A
	I criteri per le password vengono applicati tramite controlli tecnici (ad esempio MDM)?	N/A
	I criteri per le password vietano la modifica dei requisiti di autenticazione (ad es. Lunghezza password / PIN) tramite un dispositivo mobile?	N/A
Linea di condotta	Hai una policy che richiede agli utenti BYOD di eseguire backup di dati aziendali specifici?	N/A
	Esiste una politica che richiede agli utenti BYOD di vietare l'utilizzo di archivi di applicazioni non approvati?	N/A
	Hai una policy che richiede agli utenti BYOD di utilizzare software anti-malware (se supportato)?	N/A
Cancellazione remota	Il tuo IT fornisce la cancellazione remota o la cancellazione dei dati aziendali per tutti i dispositivi BYOD accettati dall'azienda?	N/A
	Il tuo IT fornisce la cancellazione remota o la cancellazione dei dati aziendali per tutti i dispositivi mobili assegnati dall'azienda?	N/A
Patch di sicurezza	I tuoi dispositivi mobili dispongono delle ultime patch disponibili relative alla sicurezza installate al rilascio generale dal produttore del dispositivo o dall'operatore?	N/A
	I tuoi dispositivi mobili consentono la convalida remota per scaricare le ultime patch di sicurezza da parte del personale IT dell'azienda?	N/A
Utenti	La tua politica BYOD chiarisce i sistemi e i server consentiti per l'uso o l'accesso sul dispositivo abilitato BYOD?	N/A
	Il criterio BYOD specifica i ruoli utente a cui è consentito l'accesso tramite un dispositivo abilitato BYOD?	N/A
Gestione degli incidenti di sicurezza, E-Discovery e Attività Giudiziaria nel Cloud		
Contatto / Manutenzione autorità	Mantenete contatti e punti di contatto con le autorità locali in conformità contatti con lecon i contratti e le normative appropriate?	NO
Gestione degli incidenti	Hai un piano di risposta agli incidenti di sicurezza documentato?	NO
	Integrate requisiti personalizzati di enti nei vostri piani di risposta agli incidenti di sicurezza?	SI
	Pubblichi un documento sui ruoli e le responsabilità che specifica di cosa sei responsabile rispetto ai tuoi enti durante gli incidenti di sicurezza?	NO
	Hai testato i tuoi piani di risposta agli incidenti di sicurezza nell'ultimo anno?	NO

Gestione degli incidenti di sicurezza, E-Discovery e Attività Giudiziaria nel Cloud			
Segnalazione di incidenti	Il tuo sistema di gestione delle informazioni di sicurezza e degli eventi (SIEM) unisce le origini dati (ad es. Registri delle app, registri del firewall, registri IDS, registri di accesso fisico, ecc.) Per analisi granulari e avvisi?	N/A	
	Il tuo framework di registrazione e monitoraggio consente l'isolamento di un incidente a enti specifici?	SI	
Preparazione legale per la risposta agli incidenti	Il tuo piano di risposta agli incidenti è conforme agli standard del settore per i processi e i controlli di gestione della catena di custodia legalmente ammissibili?	SI	
	La tua capacità di risposta agli incidenti include l'uso di tecniche di raccolta e analisi dei dati forensi legalmente ammissibili?	NO	
	Sei in grado di supportare le sospensioni per controversia legale (blocco dei dati da un determinato momento) per un ente specifico senza congelare i dati di altri enti?	SI	
	Applichi e attesti la separazione dei dati degll enti quando produci dati in risposta a citazioni legali?	SI	
Metriche di risposta agli incidenti	Monitorate e quantificate i tipi, i volumi e gli impatti su tutti gli incidenti di sicurezza delle informazioni?	SI	
	Condividerete le informazioni statistiche per i dati sugli incidenti di sicurezza con i vostri inquilini su richiesta?	SI	Le pratiche di risposta agli incidenti di sicurezza di Cms/Openyourcloudper la piattaforma Customer Satisfaction includono la segnalazione alle parti appropriate. Tuttavia, le informazioni statistiche non vengono condivise con gli inquilini.
Gestione della catena di fornitura, trasparenza e responsabilità			
Qualità e integrità dei dati	Ispezionate e tenete conto degli errori di qualità dei dati e dei rischi associati e collaborate con i vostri partner della catena di fornitura cloud per correggerli?	NO	
	Progettate e implementate controlli per mitigare e contenere i rischi per laas non la sicurezza dei dati attraverso un'adeguata separazione dei compiti, l'accesso basato sui ruoli e l'accesso con privilegi minimi per tutto il personale all'interno della vostra catena di fornitura?	SI	I fornitori di Cms/Openyourcloud hanno accesso all'applicazione o ai dati della piattaforma Customer Satisfaction.
Segnalazione di incidenti	Rendi disponibili le informazioni sugli incidenti di sicurezza a tutti i clienti e fornitori interessati periodicamente tramite metodi elettronici (ad esempio, portali)?	NO	
Servizi di rete / infrastruttura	Raccogli capacità e utilizzi dati per tutti i componenti rilevanti della tua offerta di servizi cloud?	SI	
	Fornite agli enti la pianificazione della capacità e i report sull'utilizzo?	SI	Su richiesta
Valutazioni interne del fornitore	Eseguite valutazioni interne annuali di conformità ed efficacia delle vostre politiche, procedure e misure e metriche di supporto?	SI	
Accordi con terze parti	Selezionate e monitorate fornitori in outsourcing in conformità con le leggi del paese in cui i dati vengono elaborati, archiviati e trasmessi?	SI	Il servizio Cms/Openyourcloud SaaS è limitato a un singolo paese (il nostro provider laaS si trova in Italia). I dati del cliente rimarranno all'interno della regione selezionata.
	Selezionate e monitorate fornitori in outsourcing in conformità con le leggi del paese in cui provengono i dati?	SI	Il servizio Cms/Openyourcloud SaaS è limitato a un singolo paese (il nostro provider laaS si trova in Italia). I dati del cliente rimarranno all'interno della regione selezionata.
	Il consulente legale esamina tutti gli accordi con terze parti?	SI	

Gestione della catena di fornitura, trasparenza e responsabilità			
Accordi con terze parti	Gli accordi con terze parti includono disposizioni per la sicurezza e la protezione di informazioni e risorse?	N/A	
	Fornite al cliente un elenco e copie di tutti gli accordi di subelaborazione e lo mantenete aggiornato?	N/A	
Revisioni sulla governance della catena di fornitura	Esaminate la gestione del rischio e i processi governativi dei partner per tenere conto dei rischi ereditati da altri membri della catena di fornitura di quel partner?	N/A	
Metriche della catena di fornitura	Sono state stabilite politiche e procedure e sono implementati processi aziendali e misure tecniche di supporto per mantenere accordi completi, accurati e pertinenti (ad es. SLA) tra fornitori e clienti (inquilini)?	N/A	
	Hai la capacità di misurare e affrontare la non conformità delle disposizioni e / o dei termini lungo l'intera catena di fornitura (a monte / a valle)?	SI	
	Riesci a gestire i conflitti a livello di servizio o le incongruenze derivanti da rapporti con i fornitori disparati?	N/A	
	Esaminate tutti gli accordi, le politiche e i processi almeno una volta all'anno?	SI	
Valutazione di terze parti	Assicurate una ragionevole sicurezza delle informazioni lungo la vostra catena di fornitura delle informazioni eseguendo una revisione annuale?	SI	
	La tua revisione annuale include tutti i partner / fornitori di terze parti da cui dipende la tua catena di fornitura delle informazioni?	N/A	
Audit di terze parti	Consentite agli inquilini di eseguire valutazioni di vulnerabilità indipendenti?	NO	Le valutazioni web avviate dal cliente della piattaforma Customer Satisfaction non sono autorizzate.
	regolarmenteHai servizi di terze parti esterni che eseguono scansioni di vulnerabilità e test periodici di penetrazione sulle tue applicazioni e reti?	SI	Cms/Openyourcloud conduce test di vulnerabilità delle applicazioni e della rete e test di penetrazione.
Gestione delle minacce e delle vulnerabilità			
Antivirus / Malware	Disponete di programmi anti-malware che supportano o si connettono alle vostre offerte di servizi cloud installati su tutti i vostri sistemi?	SI	
	Ti assicuri che i sistemi di rilevamento delle minacce alla sicurezza che utilizzano firme, elenchi o schemi comportamentali vengano aggiornati su tutti i componenti dell'infrastruttura entro tempi accettati dal settore?	SI	
Gestione delle vulnerabilità / patch	Conducete regolarmente scansioni di vulnerabilità a livello di rete come prescritto dalle migliori pratiche del settore?	N/A	
	Conducete regolarmente scansioni della vulnerabilità a livello di applicazione come prescritto dalle best practice del settore?	N/A	
	Eseguite regolarmente scansioni di vulnerabilità a livello del sistema operativo locale come prescritto dalle migliori pratiche del settore?	N/A	
	I risultati delle scansioni delle vulnerabilità verranno resi disponibili agli inquilini su loro richiesta?	N/A	
	Hai la capacità di applicare rapidamente le vulnerabilità a tutti i tuoi dispositivi, applicazioni e sistemi informatici?	N/A	
	Fornirete i vostri tempi di patching basati sul rischio dei sistemi informatici ai vostri inquilini su richiesta?	N/A	

Gestione delle minacce e delle vulnerabilità			
Codice mobile	Il codice mobile è autorizzato prima della sua installazione e utilizzo e la configurazione del codice viene controllata, per garantire che il codice mobile autorizzato operi secondo una politica di sicurezza chiaramente definita?	N/A	Nessun codice mobile attualmente in uso
	È impedita l'esecuzione di un codice mobile non autorizzato?	N/A	