Acquisto di Servizi Cloud nel Settore Pubblico

Manuale, con inclusi testi di esempio per RFP e Contratti Quadro per il Cloud

Note

Il presente documento è fornito a solo scopo informativo. Non è stato sviluppato in base ai requisiti di legge di procedure di appalto pubblico di nessun Paese in particolare. I clienti di servizi cloud sono tenuti a condurre autonomamente una valutazione delle informazioni contenute nel presente documento e dell'uso dei prodotti o dei servizi offerti dal fornitore di servizi cloud. Il presente documento non produce nessuna garanzia o dichiarazione, né impegni contrattuali, condizioni o assicurazioni.

I documenti e i testi di esempio non devono essere interpretati come consulenze legali, istruzioni o consigli. I clienti cloud devono rivolgersi a un consulente legale di fiducia per chiarire quali siano le loro responsabilità ai sensi del diritto applicabile nel Paese di operatività. Il CISPE declina espressamente qualsiasi garanzia o responsabilità o richiesta risarcitoria conseguente a, o in relazione a, informazioni contenute in questo documento.

Informazioni sul CISPE

Il CISPE (*Cloud Infrastructure Services Providers in Europe*, https://cispe.cloud) è una associazione e senza scopo di lucro e indipendente da interessi industriali. Rappresentiamo i fornitori di infrastrutture e servizi cloud in Europa, collaborando con gli operatori del settore e con i legislatori per offrire indicazioni e consigli sui servizi cloud e sul ruolo che occupano nell'industria, nella vita pubblica e nella società in generale.

Il numero dei nostri associati è in costante espansione e include aziende con operatività in tutti i Paesi dell'UE e con sedi legali in ben 16 paesi europei. La nostra è un'associazione aperta alle aziende, con l'unico requisito che almeno uno dei servizi offerti dall'azienda abbia ottenuto la dichiarazione di conformità al Codice di Condotta CISPE sulla Protezione dei Dati. Il nostro ruolo è:

- Sostenere i vantaggi delle politiche "cloud first" negli appalti pubblici dell'UE e degli stati membri dell'UE
- Promuovere l'adozione di requisiti di sicurezza e di standard tecnici uniformi in tutta l'UE
- Sostenere i requisiti di riservatezza generali tramite un Codice di Condotta
- Assicurare che il mercato delle infrastrutture cloud nell'UE sia aperto, competitivo e libero da vincoli (*lock-in*)
- Prevenire l'imposizione ingiustificata di obblighi di monitoraggio dei contenuti nel quadro giuridico dell'UE

Il compito dei nostri associati è fornire e gestire "gli elementi di base dell'IT", per permettere alla pubblica amministrazione, agli enti pubblci e alle imprese di realizzare i propri sistemi ed erogare servizi essenziali a miliardi di cittadini. A tal fine, contribuiamo allo sviluppo di tecnologie e servizi altamente innovativi, che inglobano intelligenza artificiale (IA), oggetti connessi, veicoli a guida autonoma e 5G, fino ad arrivare alle tecnologie di prossima generazione per la connettività cellulare.

Codice di Condotta per i servizi di infrastrutture cloud

Il codice CISPE ha anticipato l'applicazione del regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea. In linea con i severi requisiti del GDPR, il codice aiuta i fornitori di infrastrutture cloud a ottenere la conformità e offre un quadro di riferimento solido per aiutare i clienti a selezionare i fornitori di servizi cloud e a fidarsi dei loro servizi. Nel Codice di Condotta del CISPE sono contemplati più di 100 servizi, che vengono erogati da più di 30 imprese cloud con sedi legali in più di 16 stati membri dell'UE e che vengono utilizzati da milioni di utenti finali e consumatori. https://cispe.cloud/code-of-conduct/

Il CISPE e il Settore Pubblico

Il CISPE partecipa attivamente al dibattito pubblico europeo, promuovendo una migliore comprensione del ruolo, del contributo e del potenziale dell'industria delle infrastrutture cloud in Europa.

Mentre il modello di acquisto della pubblica amministrazione dovrebbe regolamentare l'adozione e l'utilizzo del cloud computing, l'acquisizione dei servizi cloud è diversa dalle acquisizioni delle tecnologie più tradizionali note al settore pubblico. La modalità di acquisto va ripensata. A questo scopo, il CISPE incoraggia i legislatori europei a sviluppare un approccio più ambizioso e lungimirante su scala UE, basato su iniziative politiche "cloud first" che stimolino la crescita del mercato unico delle infrastrutture cloud nell'UE e assicurino il conseguimento degli obiettivi di crescita del mercato unico digitale (Digital Single Market, DSM).

Lo scopo di questo manuale è fornire indicazioni utili agli enti pubblici e assisterli nell'acquisto dei servizi cloud.

Ulteriori informazioni
Associati CISPE: https://cispe.cloud/members
Consiglio direttivo: https://cispe.cloud/board-of-directors
Servizi di cloud computing dichiarati ai sensi del Codice di Condotta del CISPE: https://cispe.cloud/publicregister

Sommario

Sommario e scopo del presente manuale

Lo scopo di questo **Manuale per l'acquisto di servizi cloud** è assistere i clienti che desiderano acquistare i servizi cloud tramite una procedura di appalto competitiva, denominata **Richiesta di Offerta (*Request for Proposal* - RFP) per servizi cloud**, ma che non hanno le competenze necessarie per redigere autonomamente un Contratto Quadro per il cloud.

Il presente documento è fornito a solo scopo informativo. Non è stato sviluppato in base ai requisiti di legge delle procedure di appalto pubblico di nessun particolare Paese o regione.

Il manuale contiene inoltre il testo di esempio per specificare i criteri di selezione per gli **ordini a chiamata** e le **mini-gare,** qualora gli acquisti avvengano al di fuori di un Contratto quadro per il cloud. Il manuale è suddiviso in capitoli che riflettono la struttura di una Richiesta di Offerta (RFP) generica per il settore IT. Una RFP generica e il testo di esempio per definire i criteri di selezione sono accompagnati da commenti utili per comprendere cosa distingue una RFP per il cloud da una RFP per il settore IT tradizionale.

*Con **"servizi cloud"** si intendono tutte le tecnologie destinate al cloud e i servizi correlati a cui un utente finale potrebbe dover accedere. Sono compresi i servizi di consulenza/professionali/gestiti che supportano ed eseguono la migrazione al cloud e che supportano i carichi di lavoro nel cloud, oltre all'infrastruttura cloud stessa e ai servizi marketplace per il cloud, ad esempio i prodotti SaaS (Software as a Service).*

L'affermazione del cloud computing come scelta preferenziale per l'IT negli enti pubblici rappresenta anche l'occasione per ammodernare le strategie di appalto esistenti. Con procedure di acquisto orientate al cloud, gli enti pubblici possono sfruttare appieno i vantaggi del cloud (ad esempio, accesso immediato alle innovazioni, aumento di velocità e agilità, miglioramento dell'assetto di sicurezza e della governance della conformità) mentre lavorano a un piano di efficientamento e taglio dei costi.

Le tradizionali procedure di appalto del settore IT finalizzate all'acquisto di hardware, software e data center non possono essere applicate direttamente all'acquisto di servizi cloud. Un modello cloud prevede un approccio diverso ad aspetti come la determinazione del prezzo, la governance dell'appalto, i termini e le condizioni, la sicurezza, i requisiti tecnici, gli accordi sul livello del servizio (SLA) e così via. Per questa ragione, utilizzando le procedure di appalto esistenti si riducono o si annullano i vantaggi offerti dal cloud.

Uno degli strumenti migliori per l'acquisizione efficiente dei servizi cloud nel settore pubblico è un **Contratto quadro per il cloud**: attraverso l'aggiudicazione di un catalogo di servizi cloud per più enti, i responsabili degli acquisti dell'ente acquirente potranno scegliere le tecnologie cloud e i servizi correlati più idonei alle esigenze del loro ente. Come strumento per i contratti cloud, questi "contratti quadro" consentono di acquistare i servizi cloud in modo efficiente e conveniente, di modo che gli uffici acquisti e gli enti utilizzatori finali possano accedere a una gamma completa di servizi cloud e, in definitiva, sfruttare appieno i vantaggi del cloud: agilità, benefici di una grande economia di scala, scalabilità per aumentare la disponibilità a un costo più basso, ampiezza di funzionalità, velocità di innovazione, capacità di adattamento a nuove realtà geografiche.

Nota: **questo documento si concentra in modo specifico sulle tecnologie cloud IaaS (Infrastructure as a Service) e PaaS (Platform as a Service), così come vengono fornite da un *CISP (Cloud Infrastructure Service***

Provider, fornitore di infrastrutture e servizi cloud). È possibile acquistare le tecnologie cloud direttamente da un CISP oppure indirettamente, tramite un rivenditore del CISP. *Ulteriori considerazioni sulla RFP sarebbero necessarie per i distributori di servizi marketplace per cloud (PaaS e SaaS) e di servizi di consulenza per cloud.*

Si noti inoltre che questo documento non tratta tutti gli aspetti della creazione di un contratto quadro completo per gli appalti cloud. Esistono molti altri documenti di analisti ed esperti del settore che trattano di questioni relative al cloud, come le best practice per gli appalti, il budget per il cloud, la governance del cloud ecc. Consigliamo vivamente di tenere conto di questi documenti e raccomandazioni durante lo sviluppo di una strategia generale per gli appalti per il cloud.

Nella Tabella 1 è riportato uno schema del Manuale delle Richieste di Offerta (***Request for Proposal*** - RFP) per servizi cloud e dove è possibile trovare il testo di esempio per ogni argomento.

Tabella 1. Capitoli del Manuale delle Richieste di Offerta (*Request for Proposal* - RFP) per servizi cloud

Capitolo	Informazioni generali e RFP di esempio
1.0 Panoramica di un Contratto Quadro per il Cloud	Una panoramica generale del modello di contratto quadro per il cloud (LOTTI, competizione e appalto)
2.0 Panoramica della RFP per servizi cloud	Testo di esempio di una RFP generica che include i paragrafi riportati sotto, insieme ai commenti che spiegano la logica alla base di una RFP per servizi cloud e lo stile utilizzato.
2.1 Impostazione della RFP per servizi cloud	2.1.1 Introduzione e obiettivi strategici 2.1.2 Tempistica delle risposte a una 2.1.3 Definizioni 2.1.4 Descrizione dettagliata del modello di acquisto e concorrenza nell'ambito del Contratto quadro 2.1.5 Requisiti minimi del candidato - Amministrativi
2.2 Requisiti tecnici	2.2.1 Requisiti minimi 2.2.2 Confronto tra fornitori 2.2.3 Appalto
2.3 Sicurezza	2.3.1 Requisiti minimi 2.3.2. Confronto tra fornitori **Error! Reference source not found. Error! Reference source not found.**
2.4 Prezzi	2.4.1 Requisiti minimi 2.4.2 Confronto tra fornitori
2.5 Impostazione/Termini e condizioni per l'esecuzione dell'appalto	2.5.1 Termini e condizioni 2.5.2 Come scegliere l'assegnatario migliore per progetto 2.5.3 Onboarding e offboarding
3.0 Best Practice/Lezioni apprese	3.1 Governance del cloud 3.2 Budget per il cloud 3.3 Comprendere il modello di business dei partner 3.4 Cloud broker

Capitolo	Informazioni generali e RFP di esempio
	3.5 Sourcing/consultazione di mercato pre-
Appendice A - Requisiti tecnici per il confronto tra offerenti	Un elenco di requisiti tecnologici generici per il cloud con riferimento agli ordini a chiamata o alle mini-gare
Appendice B - Demo	Uno script di esempio per dimostrare, tramite assegnazione di punteggio, la qualità di un prodotto tecnologico cloud (le demo cloud possono fare parte di ulteriori chiamate (rilanci competitivi) o mini-gare

1.0 Panoramica di un Contratto Quadro per il Cloud

Se ben strutturato, un contratto quadro per il cloud può agevolare l'acquisto dei servizi cloud e fare in modo che ne traggano beneficio sia gli enti pubblici sia i fornitori di servizi cloud. I principali vantaggi di un contratto quadro per il cloud ben strutturato sono:

- Collaborazione
    - Quando più enti collaborano all'assegnazione di commesse con requisiti simili, si ottengono vantaggi dal punto di vista della convenienza, dell'efficienza e della riduzione dei costi, oltre a creare una procedura semplificata per gli ordini. Si stabilisce un metodo efficace per aggregare più enti pubblici che hanno un comune fabbisogno di tecnologie e di servizi cloud correlati, come le soluzioni per markeplace e consulenza.
- Gamma completa di servizi cloud
    - Può comprendere al suo interno tutti i servizi di consulenza/professionali/gestiti necessari per supportare ed eseguire la migrazione al cloud e per supportare i carichi di lavoro nel cloud, nonché le tecnologie cloud fornite dal CISP e i servizi marketplace.
    - È possibile acquistare le tecnologie cloud direttamente da un CISP oppure indirettamente, tramite un rivenditore autorizzato.
- Governance dell'appalto
    - Allinea diverse tipologie di enti/responsabili degli acquisti a una serie comune di termini e condizioni e all'aggiudicazione di un unico appalto principale, invece di tanti appalti diversi per ogni ente.
    - I vantaggi sono importanti anche per i fornitori, in quanto al posto di tante procedure diverse per ogni ente pubblico, viene stabilita una norma comune per la procedura di acquisto, i termini e le condizioni, il meccanismo delle commesse.
    - Viene garantita la flessibilità. La creazione, l'approvazione e la gestione di un appalto efficace per il cloud nell'ambito delle policy/dei regolamenti della pubblica amministrazione esistenti, sono attività che richiedono sperimentazione e la capacità di adattarsi velocemente. È di gran lunga più vantaggioso creare un contratto quadro che consenta agli enti pubblici e ai fornitori cloud di lavorare insieme per migliorare l'appalto (dal punto di vista contrattuale, dei meccanismi e dell'efficienza). Un appalto pluriennale che non funziona bene e che non può essere corretto può causare un danno agli utenti finali dell'ente pubblico, agli enti appaltanti e ai fornitori cloud.

- Scelta
    - Offre ai responsabili degli acquisti la scelta tra svariati CISP qualificati e sposta in alto l'asticella del livello dei servizi cloud e dei servizi correlati, ad esempio marketplace PaaS/SaaS cloud e consulenze cloud.
    - Consente di controllare il numero di fornitori ammessi in un contratto quadro e assicura che ogni aggiudicatario sia debitamente valutato.

Un Contratto quadro per l'acquisto di servizi cloud funziona al meglio se include le tecnologie chiave IaaS/PaaS fornite dal CISP, insieme a un marketplace PaaS/SaaS e a servizi di consulenza a cui possano accedere, al bisogno, gli utenti finali dell'ente pubblico, consentendo la pianificazione, la transizione, l'utilizzo e la gestione di un carico di lavoro nel cloud. Suggeriamo pertanto che una RFP per servizi cloud che consenta di impostare un Contratto Quadro per il Cloud sia suddivisa nei 3 lotti descritti di seguito:

- 1° LOTTO - TECNOLOGIE CLOUD
  È possibile acquistare le tecnologie cloud direttamente da un CISP oppure indirettamente, tramite un rivenditore del CISP.

- 2° LOTTO - MARKETPLACE
  Accesso a un marketplace di servizi PaaS e SaaS.

- 3° LOTTO - CONSULENZA CLOUD
  Servizi di consulenza correlati al cloud (training, servizi professionali, servizi gestiti ecc.) e supporto tecnico.

*Come accennato in precedenza, questo documento si concentra in particolare sull'acquisto di tecnologie cloud IaaS e PaaS (**1° LOTTO**), così come erogati da un CISP (acquistati direttamente dal CISP o tramite un rivenditore del CISP). Per i fornitori del 2° e 3° LOTTO sarebbero richiesti criteri di qualificazione distinti.*

Nella **Figura 1** è riportata una vista generale di una RFP per servizi cloud ben strutturata, suddivisa in tre lotti, che può portare a un Contratto Quadro per il Cloud e assicurare agli enti pubblici l'agilità (sia tecnica che contrattuale), la visibilità e il controllo sulla spesa e sull'utilizzo del cloud, oltre a mettere a disposizione tutti i servizi cloud necessari per costruire e mantenere le soluzioni richieste.

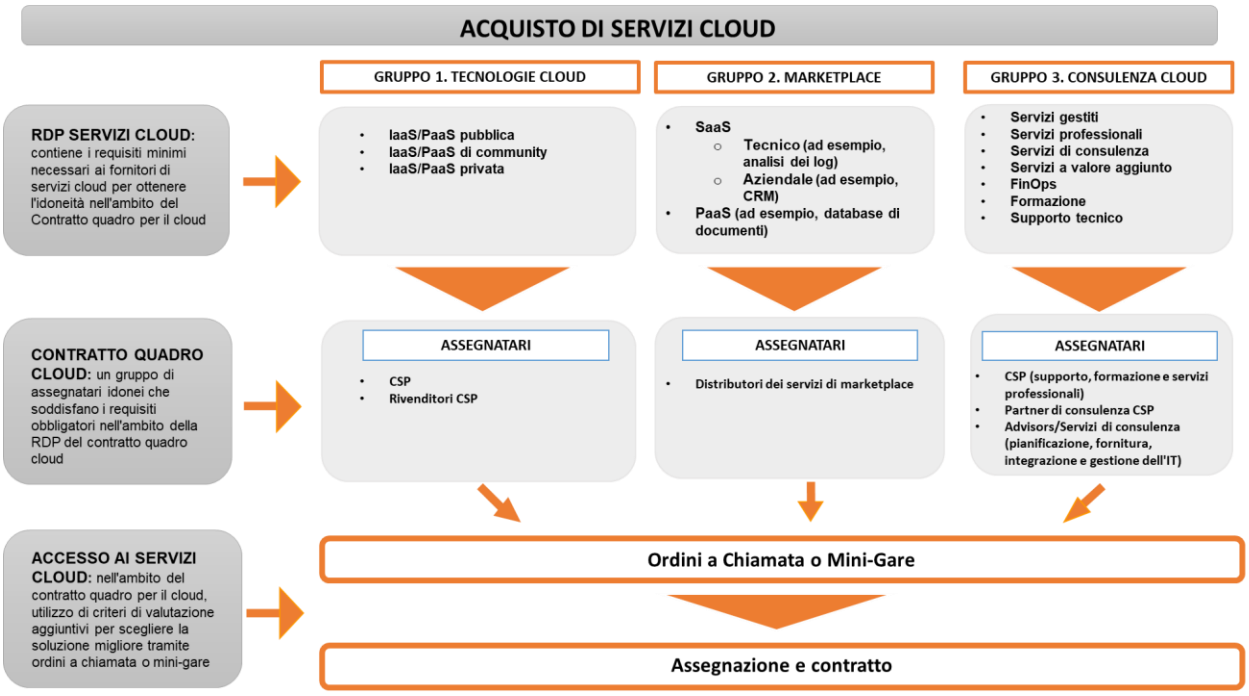

Figura 1. Una RFP per servizi cloud ben strutturata è suddivisa in 3 lotti. Ogni lotto include Categorie o "tipi di offerte" specifiche, per assicurare la conformità tecnica e contrattuale ai requisiti dell'utente finale quando gli acquisti avvengono al di fuori del Contratto quadro per il cloud.

Da notare che:

- Ogni lotto è aperto a più aggiudicazioni.
- Il 3° LOTTO può essere aggiudicato tramite un'altra RFP o eventualmente tramite un appalto esistente per servizi di consulenza.

Categorie del 1° LOTTO

I Contratti quadro per il cloud impongono ai CISP di descrivere quale modello di cloud offrono, in base alle categorie specifiche di ogni lotto. Consigliamo di fare riferimento agli standard del settore per il cloud computing (Caratteristiche Essenziali del Cloud del National Institute of Standards and Technology- NIST) per quel che riguarda le definizioni di cloud **pubblico**, cloud di **community** e cloud **privato**. Con un contratto quadro per il cloud così strutturato, l'organismo acquirente e gli enti pubblici possono scegliere tra i tanti modelli cloud quello più adatto alle loro esigenze.

Per le definizioni fornite dal NIST per i singoli modelli cloud del 1° LOTTO (IaaS/PaaS pubblico, IaaS/PaaS di community e IaaS/PaaS privato), *vedere il paragrafo 2.1.3 Definizioni*.

Scelta tra Ordini a Chiamata e Mini-Gare

I criteri di qualificazione di una RFP per servizi cloud devono includere gli elementi critici e gli standard minimi e non devono includere standard di secondaria importanza/opzionali. Aggiungendo standard

supplementari, di livello superiore a quello base, si rischia di escludere dalla gara d'appalto alcuni fornitori qualificati e di limitare così le opzioni per i responsabili degli acquisti.

Dopo aver creato la RFP e aver impostato il contratto quadro per il cloud, gli enti pubblici che fanno riferimento al contratto quadro possono ricorrere all'uso degli "ordini a chiamata" per ottenere i servizi cloud di cui hanno bisogno nel momento in cui ne hanno bisogno. Inserendo un ordine a chiamata nell'ambito del Contratto quadro, i responsabili degli acquisti possono correggere o aggiungere dei requisiti tecnici per l'ordine a chiamata specifico, senza dover rinunciare ai vantaggi offerti dal Contratto quadro.

È eventualmente possibile indire una mini-gara per individuare il fornitore migliore per un determinato carico di lavoro o progetto. Si parla di mini-gara quando un cliente aumenta il livello della concorrenza nell'ambito del Contratto quadro e chiede a tutti i fornitori di un determinato lotto di rispondere a una serie di requisiti. Il cliente invita tutti i fornitori qualificati per il lotto a fare un'offerta, per questo è importante che gli aggiudicatari di una RFP per servizi cloud siano in possesso dei requisiti minimi, così da garantire uno standard elevato delle opzioni per ciascun lotto.

È importante che siano previsti ***termini e condizioni contrattuali distinti*** *per ogni lotto (vedere la Figura 1). L'adozione di un unico approccio indifferenziato per appaltare tutti i lotti potrebbe causare problemi di fattibilità e compatibilità tecnica.*

2.0 Panoramica della RFP per servizi cloud

Questo capitolo descrive il modello e l'ambito di applicazione di una RFP per servizi cloud: obiettivi strategici, partecipanti, definizioni, tempistica, requisiti amministrativi minimi. Va ribadito che questo manuale si concentra in modo specifico sul **1° LOTTO: TECNOLOGIE CLOUD**.

2.1 Impostazione della RFP per servizi cloud

Consigliamo vivamente agli enti pubblici di chiarire fin dall'introduzione alla RFP per servizi cloud quali siano esattamente gli obiettivi e i requisiti generali che perseguono.

2.1.1 Introduzione e obiettivi strategici

Per dichiarare gli obiettivi strategici, è buona regola scrivere già nell'introduzione alla RFP per servizi cloud quanto segue: **(1)** quali sono gli obiettivi commerciali e i vantaggi che l'ente intende perseguire utilizzando il cloud; **(2)** come è strutturato il Contratto quadro (chi compra, chi opera, chi decide il budget ecc.); **(3)** qual è il modello di responsabilità condivisa tra ente pubblico e fornitori di servizi cloud (CISP), che è fondamentale per acquistare e utilizzare in modo produttivo i servizi cloud; e **(4)** qual è la relazione che si instaura tra i CISP, i distributori di servizi marketplace, i partner di consulenza, appalti pubblici/enti appaltanti e gli utenti finali dell'ente pubblico. Mettendo questi quattro punti nero su bianco, gli enti possono sviluppare una RFP perfettamente rispondente alle loro esigenze, oltre a offrire ai clienti e ai fornitori la massima chiarezza su quali siano gli obiettivi realizzabili della RFP.

La RFP per servizi cloud ha una finalità diversa rispetto a una classica RFP per il settore IT. La tecnologia cloud non è semplicemente un sostituto dell'informatica classica, ma introduce un modo completamente nuovo di consumare la tecnologia. Le RFP per servizi cloud ben strutturate possono aiutare gli enti pubblici a sfruttare rapidamente i vantaggi del cloud.

Quando si parla di "good practice" con riferimento agli acquisti per il cloud, il punto di partenza migliore è senz'altro una spiegazione chiara del modello di responsabilità condivisa. Il modello di responsabilità condivisa[1] è utilizzato perlopiù quando si parla di sicurezza e conformità del cloud, ma la delineazione delle responsabilità si applica a tutti gli aspetti delle tecnologie cloud. In una RFP per servizi cloud è necessario dichiarare quali aspetti sono di competenza del CISP in un ambiente cloud e quali aspetti restano invece di competenza del cliente. Ad esempio, il CISP mette a disposizione le funzionalità di monitoraggio delle risorse e delle applicazioni eseguite nel cloud, ***ma*** l'utilizzo di queste funzionalità messe a disposizione dal CISP è responsabilità del cliente, dato che un CISP che ha milioni di clienti e opera su grande scala non può farsene carico.

Inoltre i clienti cloud devono comprendere come la rete di partner del CISP possa aiutare i clienti a utilizzare il cloud e a gestire le loro responsabilità. Ad esempio, un fornitore di servizi gestiti (Managed Service Provider, MSP) per il cloud può aiutare un cliente a configurare e a utilizzare le funzionalità di monitoraggio messe a disposizione dal CISP e così soddisfare i requisiti di conformità e audit specifici del cliente.

Per riassumere, le responsabilità nel modello cloud sono:

[1] Vedere il capitolo 5 del Codice di Condotta CISPE: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

Un CISP mette a disposizione la tecnologia cloud

Un cliente utilizza la tecnologia cloud

Le **società di consulenza**, se presenti, aiutano il cliente ad accedere e usarea tecnologia cloud

Le **"società di consulenza"** sono aziende di servizi gestiti/professionali che aiutano i clienti a progettare, strutturare, costruire, migrare e gestire i carichi di lavoro e le applicazioni nel cloud. *Queste società includono integratori di sistemi, consulenti strategici, agenzie, Managed Service Providers e Value-Added Resellers.*

Acquistare i servizi cloud è un po' come fare la spesa in una ferramenta. Un negozio di ferramenta può fornire tutto il materiale e tutti gli arnesi che servono per realizzare un progetto. Il progetto può riguardare la costruzione di un armadietto, di una piscina o addirittura di una casa intera: è il cliente a decidere. Al momento dell'acquisto del materiale e degli arnesi, il commesso della ferramenta può dare delle indicazioni basate sulla sua esperienza, ma non può andare a casa del cliente a realizzare il progetto. Le opzioni sono:

1. Acquistare il materiale e gli arnesi e mettersi al lavoro per realizzare il proprio progetto.
2. Acquistare il materiale e gli arnesi e appaltare il lavoro ad altri.
3. Appaltare il lavoro ad altri e incaricare questo soggetto di procurarsi anche il materiale e gli arnesi necessari.

Se un ente possiede internamente le competenze necessarie per costruire e gestire autonomamente le soluzioni e l'ambiente cloud, avrà soltanto bisogno di poter accedere alle tecnologie cloud e agli strumenti standardizzati messi a disposizione dal CISP (direttamente dal CISP o tramite un rivenditore del CISP; vedere il **1° LOTTO**). Le applicazioni software SaaS e PaaS necessarie dovrebbero essere disponibili su un marketplace cloud (**2° LOTTO**). Se occorre ulteriore assistenza per consulenza, migrazione, implementazione e/o gestione, entra in gioco il Partner Network del CISP (**3° LOTTO**).

Testo di esempio di una RFP: introduzione e obiettivi strategici

Il cloud computing garantisce agli enti pubblici l'accesso rapido a un'ampia gamma di risorse IT flessibili, a basso costo, pagate al consumo. Gli enti possono acquistare le risorse più adatte, per tipologia e dimensione, per sviluppare alcune idee innovative o per mandare avanti il lavoro del reparto IT, evitando investimenti importanti in prodotti hardware e/o contratti di licenza software a lungo termine.

*L'**<ENTE>** ha la necessità di accedere a questi tipi di tecnologie cloud disponibili in commercio per rispondere alle proprie esigenze aziendali attraverso un ampio spettro di enti affiliati.*

*L'obiettivo principale della RFP è sottoscrivere un **<CONTRATTO QUADRO>** parallelo e non esclusivo con un numero massimo di **<x>** fornitori, che rappresentano diverse tecnologie cloud e servizi correlati.*

1. ***1° LOTTO**. Fornitore di servizi cloud (CISP) o rivenditori del CISP per l'acquisto di tecnologie cloud*
2. ***2° LOTTO.** Fornitori di servizi marketplace.*

3. ***3° LOTTO.*** *Fornitori di servizi di consulenza che offrono competenze ulteriori rispetto alla migrazione alle offerte del CISP e al loro utilizzo.*

*Per quanto riguarda il **1° LOTTO**, gli enti che partecipano alla gara d'appalto (CISP o rivenditori del CISP) sono tenuti a dimostrare in che modo la loro proposta soddisfa i seguenti questi obiettivi:*

- ***Agilità**: mettere le risorse IT a disposizione degli utenti finali entro pochi minuti, non settimane o mesi.*
- ***Innovazione**: garantire l'accesso immediato alle tecnologie più innovative disponibili sul mercato.*
- ***Costi**: passare dagli investimenti in conto capitale alle spese variabili (da CapEx a OpEx). In altre parole, pagare solo per ciò che si consuma.*
- ***Bilancio**: poter visualizzare i dati sulla fatturazione e sul consumo sia a livello granulare che di riepilogo, per avere una panoramica dei modelli di spesa nel tempo e una previsione di spesa per il futuro.*
- ***Elasticità**: ottenere un abbassamento dei costi variabili grazie alle economie di scala di alto livello fornite dal cloud.*
- ***Capacità**: capire le esigenze in fatto di infrastrutture evitando di tirare a indovinare.*
- ***Dismissione dei data center**: concentrare l'attenzione sulle attività utili ai cittadini, anziché accumulare tonnellate di server che occupano spazio e consumano energia.*
- ***Sicurezza**: formalizzare la progettazione degli account rendendo le risorse più visibili e verificabili ed eliminando i costi per la protezione degli impianti e dell'hardware fisico.*
- ***Responsabilità condivisa**: ridurre gli oneri operativi grazie al fatto che il CISP opera, gestisce e controlla tutti i componenti, dal sistema operativo host e dalla virtualizzazione, alla sicurezza degli impianti in cui opera il servizio.*
- ***Automazione**: integrare l'automazione nell'architettura cloud per aumentare la scalabilità in modo sicuro, rapido ed economicamente conveniente.*
- ***Governance del cloud**: (1) iniziare con un inventario completo di tutti i beni IT; (2) gestire tutti questi beni centralmente; e (3) predisporre un meccanismo di avvisi su utilizzo/fatturazione/sicurezza ecc., sfruttando le funzionalità di localizzazione dei beni, gestione dell'inventario, gestione del cambiamento, gestione e analisi dei registri, oltre a visibilità generale e governance del cloud.*
- ***Controllo**: ottenere piena visibilità su come vengono consumati i servizi IT e su quali aspetti è possibile perfezionare per migliorare sicurezza, affidabilità, prestazioni e costi.*
- ***Reversibilità**: fornire strumenti e servizi di portabilità per aiutare la migrazione verso/dall'infrastruttura del CISP, riducendo al minimo i vincoli (vendor lock-in) e rispettando il codice (o i codici) di condotta del* settore.
- ***Protezione dei dati**: capacità di dimostrare la conformità al regolamento generale sulla protezione dei dati (GDPR) tramite l'adozione di un codice di condotta specifico per i servizi di infrastrutture cloud, cioè il Codice di Condotta CISPE sulla protezione dei dati.*
- ***Trasparenza**: garantire ai clienti il diritto di sapere dove si trovano le infrastrutture utilizzate per l'elaborazione e l'archiviazione dei loro dati (area urbana).*

2.1.2 Tempistica delle risposte a una RFP

In fase di redazione del Contratto quadro per il cloud e della RFP per servizi cloud correlata, è buona prassi indicare ai candidati la tempistica della gara di appalto. Maggiore sarà il coinvolgimento del settore,

maggiori saranno le garanzie che tutte le parti in causa comprendano chiaramente i requisiti della RFP e che le offerte dei servizi da parte dei fornitori siano adeguate al modello di cloud.

La tempistica di una RFP non può prescindere dalle leggi locali e dagli obblighi giuridici, pertanto l'elenco fornito di seguito va inteso come best practice e non come norma da applicare obbligatoriamente alle attività e alle tempistiche.

Testo di esempio di una RFP: tempistica della risposta

La tempistica di una RFP per servizi cloud è la seguente:

Tempistica di una RFP per servizi cloud
• *Pubblicazione della richiesta di informazioni (RDI):* • *Risposta alla RDI:* • *Pubblicazione della bozza della Richiesta di Offerta (Request for Proposal - RFP):* • *Termine di presentazione della risposta alla RFP:* • *Fase di consultazione del settore: <tempistica>* • *Pubblicazione della RFP di preselezione:* • *Risposta alla RFP di preselezione:* • *Pubblicazione della RFP:* • *Fase 1 Termine di presentazione dei quesiti:* • *Fase 1 Risposte:* • *Fase 2 Termine di presentazione dei quesiti:* • *Fase 2 Risposte:* • *Termine di presentazione della risposta alla RFP:* • *Periodo dedicato alle richieste di precisazioni sull'offerta:* • *Periodo di trattativa:* • *Data di aggiudicazione prevista:* • *Aggiudicazione dell'appalto:* • *Durata dell'appalto (opzioni di proroga):*

La tempistica di una RFP non può prescindere dalle leggi locali e dagli obblighi giuridici, pertanto l'elenco fornito di seguito va inteso come best practice e non come norma da applicare obbligatoriamente alle attività e alle tempistiche.

2.1.3 Definizioni

La RFP per servizi cloud deve includere un elenco dettagliato delle definizioni. L'elenco deve includere i ruoli dei fornitori (ad esempio, fornitore di servizi cloud, rivenditore cloud, fornitore partner), i concetti tecnologici generali (calcolo, storage, IaaS/PaaS, SaaS) e altri elementi fondamentali del contratto. Ecco un esempio di definizioni:

Testo di esempio di una RFP: definizioni

Le definizioni di cloud computing fornite di seguito sono del National Institute of Standards and Technology (NIST).[2]

- ***Infrastructure as a Service (IaaS).*** *Capacità di fornire al consumatore le funzionalità di elaborazione, storage, rete e le altre risorse informatiche fondamentali affinché il consumatore possa distribuire ed eseguire il software in modo arbitrario, inclusi sistemi operativi e applicazioni. Il consumatore non gestisce e non controlla l'infrastruttura cloud sottostante, ma controlla i sistemi operativi, lo storage e le applicazioni distribuite e, se possibile, esercita un controllo limitato sulla scelta dei componenti delle reti (ad esempio, firewall host).*

- ***Platform as a Service (PaaS).*** *Capacità fornita al consumatore di implementare, nell'infrastruttura cloud applicazioni acquisite o create dal consumatore stesso, utilizzando linguaggi di programmazione, librerie, servizi e strumenti supportati dal fornitore. Il consumatore non gestisce e non controlla l'infrastruttura cloud sottostante (rete, server, sistemi operativi e storage), ma controlla le applicazioni distribuite e, se possibile, le impostazioni di configurazione per l'ambiente di hosting delle applicazioni.*

- ***Software as a Service (SaaS).*** *Capacità di garantire al consumatore l'utilizzo delle applicazioni del fornitore che sono eseguite nell'infrastruttura cloud. L'accesso a tali applicazioni è consentito da diversi dispositivi client, tramite un'interfaccia Thin Client come un browser web (ad esempio, e-mail basata sul web) o tramite l'interfaccia di un programma. Il consumatore non gestisce e non controlla l'infrastruttura cloud sottostante (rete, server, sistemi operativi e storage) e neppure le funzionalità delle singole applicazioni, con la sola possibile eccezione di alcune e limitate impostazioni di configurazione specifiche dell'utente.*

- ***Cloud pubblico.*** *L'infrastruttura cloud è a disposizione per il libero uso da parte del pubblico. Il proprietario, gestore o operatore può essere un'azienda, un'istituzione accademica o la pubblica amministrazione, o una combinazione delle tre. Risiede presso la sede del fornitore di servizi cloud.*

- ***Cloud di community.*** *L'infrastruttura cloud viene messa a disposizione esclusiva di una specifica comunità di consumatori da parte di enti che hanno un comune interesse (ad esempio una missione, dei requisiti di sicurezza, delle considerazioni di policy e conformità). Il proprietario, gestore o operatore può essere uno o più enti presenti nella comunità, un soggetto terzo o una combinazione di questi. Può risiedere o meno presso la loro sede.*

- ***Cloud ibrido.*** *L'infrastruttura cloud è composta da due o più infrastrutture cloud distinte (private, community o pubbliche) che rimangono entità univoche e distinte, ma legate da una tecnologia standardizzata o proprietaria che consente la portabilità di dati e applicazioni (ad esempio, cloud bursting per il bilanciamento del carico tra i cloud).*

- ***Cloud privato.*** *L'infrastruttura cloud viene messa a disposizione esclusiva di un unico ente che comprende più consumatori (ad esempio, varie unità operative di un'azienda). Il proprietario, gestore o operatore può essere l'ente stesso, un soggetto terzo o una combinazione di questi. Può risiedere o meno presso la loro sede.*

2.1.4 Descrizione dettagliata del modello di acquisto e concorrenza nell'ambito del Contratto quadro

Come già sottolineato, gli enti pubblici devono individuare un modello in base al quale applicare il Contratto quadro dal punto di vista del meccanismo di acquisto delle tecnologie cloud e dei servizi correlati per implementazione e gestione. Questo aspetto deve essere chiarito nella RFP per servizi cloud, di modo che i fornitori delle tecnologie cloud, gli enti che forniscono servizi di consulenza, i distributori marketplace e i soggetti acquirenti conoscano perfettamente i loro ruoli.

[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Per definire l'ambito di applicazione del Contratto quadro, oltre che degli ordini a chiamata e delle mini-gare che ne deriveranno, gli enti devono considerare quanto segue:

- Chi sarà responsabile dell'integrazione e dei servizi gestiti che implicano l'uso delle tecnologie cloud come da contratto?
- Esiste l'esigenza di avere un rivenditore CISP/partner in grado di fornire servizi a valore aggiunto oltre il mantenimento delle relazioni contrattuali con il CISP, ad esempio la fornitura di sevizi di fatturazione consolidati e l'accesso diretto e puntuale ai dati relativi a fatturazione e consumo associati all'uso dei servizi del fornitore di servizi cloud?
- Esiste l'esigenza di avere a pieno servizio un VAR, un integratore di sistemi o un fornitore di servizi gestiti, o qualsiasi altra forma di servizi di manodopera IT?

È importante sottolineare che un CISP non è né un integratore di sistemi (Systems Integrator, SI) né un fornitore di servizi gestiti (Managed Service Provider, MSP). Molti clienti del settore pubblico avranno bisogno di un CISP per i loro servizi IaaS/PaaS e di un SI o un MSP a cui esternalizzare le attività di pianificazione, migrazione e gestione. Nella Figura 2 sono illustrati i ruoli e le responsabilità in un modello di servizi cloud.

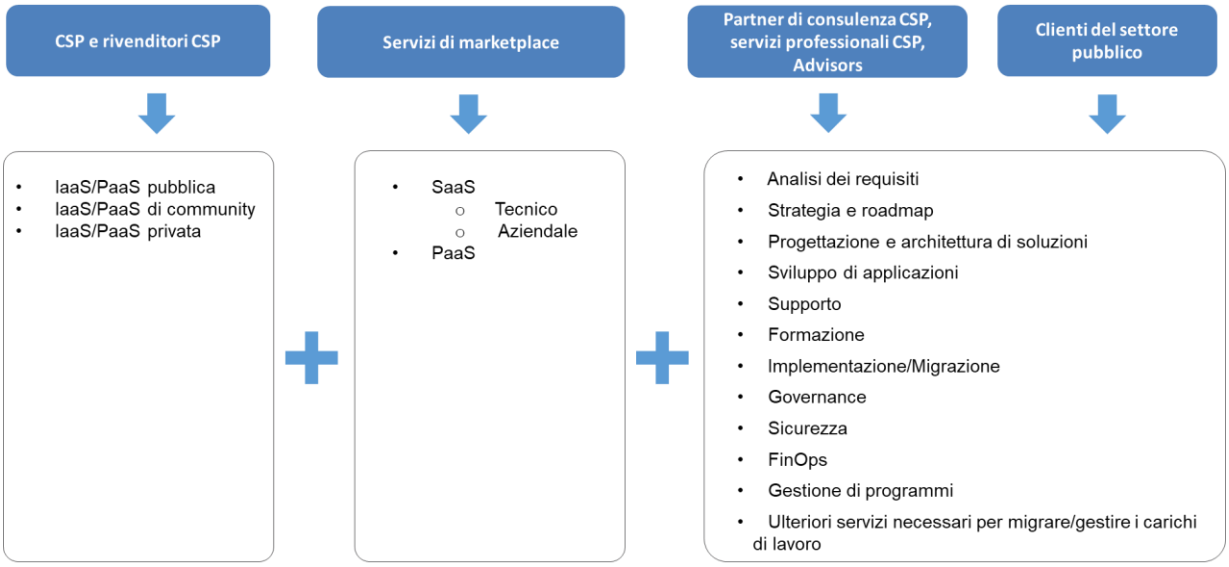

Figura 2. Una RFP per servizi cloud dovrebbe fornire agli utenti finali una selezione completa dei servizi cloud di cui hanno bisogno. I clienti del settore pubblico avranno bisogno di un CISP per le tecnologie cloud e probabilmente di un marketplace per i prodotti PaaS e SaaS. Il cliente potrà quindi decidere in quale misura partecipare all'erogazione dei servizi cloud e quante attività esternalizzare a una società di consulenza/un SI/un MSP ecc.

Il testo di esempio riportato sotto dipende dai ruoli e dalle responsabilità descritti nella Figura 2. Un Contratto quadro per il cloud e la RFP per servizi cloud associata devono consentire ai responsabili degli acquisti di valutare adeguatamente le offerte di ogni fornitore e di selezionare i servizi necessari per il carico di lavoro/progetto specifico. Questo traguardo può essere raggiunto suddividendo i servizi in lotti, come già accennato, e spiegando chiaramente come si devono svolgere gli ordini a chiamata e le mini-gare nell'ambito del Contratto quadro.

Testo di esempio di una RFP: modello di acquisto

Il presente contratto fungerà da veicolo di acquisto ***quadro****. Il presente Contratto quadro per il cloud conterrà molteplici* ***lotti*** *definiti dall'<****ENTE>*** *per le tecnologie cloud e i servizi/prodotti correlati per il marketplace, i servizi di consulenza, i servizi professionali per integrazione di sistema/servizi gestiti/migrazione, il training e il supporto definiti dall'<****ENTE>*** *e potrà essere utilizzato da più responsabili degli acquisti autorizzati e affiliati all'<****ENTE****>. Ciò consente di semplificare la procedura della gara d'appalto e, al tempo stesso, di ottimizzare le economie di scala.*

Una volta sottoscritto, il presente Contratto quadro consente a un ente di acquistare le specifiche tecnologie cloud e i servizi correlati di cui ha bisogno, nel momento in cui ne ha bisogno, diversamente da quanto accade con le gare d'appalto singole. Questo approccio riduce i requisiti amministrativi e semplifica enormemente la gara d'appalto dal punto di vista della complessità e dei tempi.

La durata del Contratto quadro sarà al massimo di ***<X>*** *anni, compresi eventuali rinnovi. La durata massima di un ordine a chiamata nell'ambito di un Contratto quadro è normalmente di* ***<x>*** *mesi, prorogabili per* ***<x>*** *mesi e successivamente per ulteriori* ***<x>*** *mesi, con le eventuali approvazioni interne richieste per la concessione della proroga. La durata deve essere sempre indicata in ogni* ***ordine a chiamata.***

Il Contratto Quadro è suddiviso in ***3 (tre) lotti****.*

1. *1° LOTTO - TECNOLOGIE CLOUD. Fornitura completa di tecnologie cloud (servizi/prodotti venduti direttamente dal CISP, dal rivenditore o dal rivenditore con servizi a valore aggiunto):*
    i. ***Servizi IaaS e PaaS****: ampia scelta di tecnologie cloud per calcolo, storage, reti, database, analisi, servizi applicativi, distribuzione, gestione, sviluppo, Internet of Things (IoT) ecc. Include pacchetti di soluzioni basate sulla tecnologia cloud, come DR/COOP, Archive, Big Data & Analytics, DevOps ecc.*
2. *2° LOTTO - MARKETPLACE. Fornitura completa di servizi/prodotti PaaS e SaaS, ad esempio contabilità, CRM, progettazione, HR, mappatura GIS, HPC, BI, gestione contenuti, analisi dei registri ecc.*
3. *3° LOTTO - CONSULENZA CLOUD. Fornitura completa di servizi di consulenza (servizi gestiti, servizi professionali, servizi di consulenza/promozionali, servizi a valore aggiunto, operazioni finanziarie, supporto tecnico) correlati alla migrazione e all'utilizzo del cloud. Questi servizi possono includere: pianificazione, progettazione, migrazione, gestione, supporto, controllo della qualità, sicurezza, formazione ecc.*

I fornitori possono presentare offerte per più lotti.

I fornitori potranno presentare offerte corredate di prezzi in un formato a loro scelta.

CONCORRENZA NELL'AMBITO DEL CONTRATTO QUADRO E AGGIUDICAZIONE DEGLI APPALTI

ORDINI A CHIAMATA

Gli enti pubblici che sottoscrivono il Contratto quadro possono ricorrere agli "ordini a chiamata" per i servizi di cui hanno bisogno, nel momento in cui ne hanno bisogno. Inserendo un ordine a chiamata nell'ambito del Contratto quadro, i responsabili degli acquisti possono correggere o aggiungere dei requisiti tecnici per l'ordine a chiamata specifico, senza dover rinunciare ai vantaggi offerti dal Contratto quadro.

Gli appalti aggiudicati tramite il Contratto quadro avranno un audit trail molto chiaro per quanto riguarda i requisiti applicati alla selezione del fornitore per ogni lotto. Gli acquirenti finali conserveranno tutte le comunicazioni avvenute

con i fornitori, compreso l'eventuale dialogo iniziale con il mercato, le richieste di precisazioni, le e-mail e le discussioni faccia a faccia.

1. DEFINIZIONE DEI REQUISITI DI UN ORDINE A CHIAMATA E APPROVAZIONE INTERNA DELL'ACQUISTO

Tutti gli acquirenti finali che hanno diritto ad utilizzare il Contratto quadro creeranno dei gruppi (costituiti da utenti finali aziendali, esperti di acquisti e tecnici) per redigere un elenco dei prodotti/servizi indispensabili e di quelli desiderati. Questi requisiti semplificheranno la scelta del lotto/dei lotti pertinenti e del fornitore/fornitori più qualificati. Nel definire i requisiti, i responsabili degli acquisti dovranno considerare:

- *I fondi disponibili per l'uso del servizio*
- *I requisiti tecnici e la procedura d'appalto per il progetto*
- *I criteri su cui si dovrà basare la scelta*

2. RICERCA DEI SERVIZI

Nell'ambito del Contratto quadro, i responsabili degli acquisti potranno consultare un catalogo online (un portale sul quale saranno elencati tutti gli aggiudicatari qualificati in base al Contratto quadro, con i rispettivi servizi) per trovare prodotti/servizi rispondenti alle esigenze da loro identificate. Dovranno selezionare i lotti pertinenti e quindi cercare i servizi.

3. ESAME E VALUTAZIONE DEI SERVIZI

Nell'ambito del Contratto quadro, i responsabili degli acquisti potranno esaminare le descrizioni e identificare i servizi rispondenti alle loro esigenze sulla base dei requisiti e del budget. Tutte le descrizioni dei servizi devono includere:

- *Un documento con le definizioni dei servizi o i link alle definizioni dei servizi*
- *Un documento con i termini e le condizioni*
- *Un documento con i prezzi (i link ai prezzi pubblici sono ammessi a condizione che, su richiesta, sia disponibile un documento/listino prezzi completo)*

Il prezzo corrisponderà al costo della configurazione più comune del servizio. Tuttavia il prezzo viene normalmente fissato in base al volume, pertanto i responsabili degli acquisti devono consultare sempre il documento con i prezzi del fornitore o un suo listino pubblico e, con l'aiuto degli strumenti idonei, calcolare il prezzo effettivo di ciò che acquistano più il valore globale per l'acquirente (ad esempio, servizi di ottimizzazione con conseguente taglio dei costi).

Nell'ambito del Contratto quadro, i responsabili degli acquisti possono interagire con i fornitori per ricevere chiarimenti circa la descrizione di un servizio, i termini e le condizioni applicati, i prezzi o il modello/documento che definisce il servizio. È necessario conservare le registrazioni di tutte le interazioni con i fornitori.

4. SCELTA DI UN SERVIZIO E AGGIUDICAZIONE DI UN APPALTO

Unico fornitore

Se c'è un solo fornitore che soddisfa tutti i requisiti, sarà lui l'aggiudicatario dell'appalto.

Fornitori multipli

Se l'elenco viene ristretto a un determinato numero di servizi, la scelta del responsabile degli acquisti dovrà ricadere sull'offerta economicamente più vantaggiosa (MEAT, Most Economically Advantageous Tender). Per conoscere i criteri della valutazione basata sul principio MEAT, vedere la tabella seguente. I responsabili degli acquisti possono decidere il livello di dettaglio e il peso di ogni caratteristica.

Tenere presente che il responsabile degli acquisti potrebbe dover:

- *Considerare combinazioni di più fornitori*
- *Chiedere informazioni specifiche su sconti per impresa o per volume e su costo fornitore-servizi di ottimizzazione*

La valutazione dei fornitori deve essere sempre onesta e trasparente. La scelta deve ricadere sul più idoneo e i fornitori/servizi non dovranno essere esclusi senza tenere conto dei requisiti del progetto.

Tabella 2. Valutazione basata sul principio MEAT

Criteri di aggiudicazione
Costo dell'intero ciclo di vita: *rapporto costi/benefici, prezzo e costi di esercizio*
Valore tecnico e idoneità funzionale: *copertura, capacità di rete e prestazioni, come specificato nei livelli di servizio pertinenti*
Gestione post-vendita dei servizi: *help desk, documentazione, funzione di gestione degli account e continuità del rifornimento per una serie di servizi*
Caratteristiche non funzionali

MINI-GARE

Se necessario, è possibile indire una mini-gara per individuare il fornitore migliore per un determinato carico di lavoro o progetto. Si parla di mini-gara quando un cliente aumenta il livello della concorrenza nell'ambito del Contratto quadro e chiede a tutti i fornitori di un determinato lotto di rispondere a una serie di requisiti. Il cliente inviterà tutti i fornitori del lotto che sono idonei a fare un'offerta. Più avanti sono riportate ulteriori informazioni comparative riguardanti aspetti tecnici, sicurezza e prezzo/valore.

CONTRATTO

Sia l'acquirente che il fornitore devono sottoscrivere una copia del contratto prima dell'uso del servizio. La durata massima di un Contratto quadro è normalmente di <x> mesi, prorogabili per <x> mesi e successivamente per ulteriori <x> mesi, con le eventuali approvazioni interne richieste per la concessione della proroga.

Una copia del contratto dovrà essere sottoscritta da tutti i contraenti (l'acquirente e il fornitore) prima dell'uso del servizio.

2.1.5 Requisiti minimi del candidato - Amministrativi

L'uso di un linguaggio semplice e chiaro per definire i criteri di qualificazione per il Contratto quadro garantirà che non arriveranno offerte dai tradizionali fornitori di hardware o data center che offrono una soluzione classica facendola passare per "cloud". Chi parteciperà alla RFP dovrà dimostrare di soddisfare i requisiti amministrativi minimi degli offerenti.

Come già sottolineato, questo documento si sofferma in modo specifico sul 1° LOTTO - TECNOLOGIE CLOUD. Tuttavia sono state aggiunte informazioni anche sul 2° LOTTO - MARKETPLACE e sul 3° LOTTO - CONSULENZA CLOUD quando sono utili a chiarire il contesto generale dal punto di vista dei requisiti e dell'ambito di applicazione della RFP. È ad esempio importante includere i criteri di qualificazione minimi per un Rivenditore CISP/MSP/SI/consulente ecc. per garantire che il soggetto (1) è direttamente affiliato al CISP in qualità di rivenditore o partner commerciale; (2) è autorizzato dal CISP a rivendere l'accesso diretto alle offerte del CISP a terzi; ed (3) è in possesso di una certificazione rilasciata dai CISP che ne attesta competenze ed esperienza

Testo di esempio di una RFP: requisiti amministrativi minimi dell'offerente

Il presente Contratto quadro consentirà di aggiudicare appalti a fornitori multipli per le categorie seguenti. Il fornitore deve essere un CISP commerciale, un rivenditore di un CISP, un distributore di servizi marketplace e/o un fornitore di servizi per l'utilizzo di un CISP (ad esempio consulenze, servizi di migrazione, servizi gestiti, operazioni finanziarie ecc.). Identificare i ruoli per i quali si presenta l'offerta:

1° LOTTO

____ - Fornitore diretto (CISP) di servizio cloud pubblico (IaaS + PaaS)

____ - Fornitore diretto (CISP) di servizio cloud di community (IaaS + PaaS)

____ - Fornitore diretto (CISP) di servizio cloud privato (IaaS + PaaS)

____ - Rivenditore di CISP (in grado di garantire l'accesso diretto alle offerte cloud online dei CISP).

- *Indicare l'offerta del CISP per la quale l'offerente rivende l'accesso diretto al servizio: _____*
- *Allegare una lettera in cui il CISP attesta che l'offerente è autorizzato a rivendere le sue offerte: _____*

2° LOTTO

____ - Fornitore diretto di servizi marketplace eseguiti su infrastrutture di un CISP (PaaS e/o SaaS)

____ - Distributore di servizi marketplace eseguiti su infrastrutture di un CISP (PaaS e/o SaaS)

3° LOTTO

____ - CISP che offre servizi professionali

____ - Fornitore di supporto tecnico per il CISP

____- Partner del CISP che offre servizi per l'utilizzo o l'operatività sulle infrastrutture di un CISP

____- Influencer/consulente che offre servizi per l'utilizzo o l'operatività sulle infrastrutture di un CISP

Indicare il tipo di offerta:

- *Servizi gestiti di carichi di lavoro sulle infrastrutture di un CISP (S/N): _____*
  - *Indicare le aree di specializzazione, se pertinenti: _____*
- *Servizi professionali (S/N): _____*
- *Consulenza - Formazione (S/N): _____*
- *Consulenza - Strategia (S/N): _____*
- *Consulenza - Migrazione (S/N): _____*
- *Consulenza - Governance del cloud (S/N): _____*
- *Consulenza - FinOps (S/N): _____*
- *Consulenza - Altro (specificare): _____*

Indicare il CISP o i CISP per conto dei quali si forniscono i servizi: _____
Allegare una lettera del CISP in cui viene confermato il vosro ruolo di partner in conformità al modellodel CISP: _____

REQUISITI AMMINISTRATIVI MINIMI PER IL 1° LOTTO

Fornitore di servizi cloud (CISP)
Per potersi qualificare come CISP, il soggetto offerente deve rispettare i requisiti seguenti.

Criteri di qualificazione proposti per un CISP	*Motivazione*
Informazioni sull'ente (ad esempio, ragione sociale, struttura giuridica, n° di immatricolazione/codice DUNS, n° di partita IVA ecc.)	
Dimensioni dell'azienda, capacità economica e finanziaria[3]	*Il cliente può stabilire che il CISP sarà in grado di onorare il contratto d'appalto.*
Motivi che determinano l'esclusione (ad esempio, attività criminali e fraudolente ecc.)	
Casi di studio/Referenze dei clienti (specificare il numero/tipo richiesto)	*Il cliente ha la possibilità di valutare se l'esperienza del CISP garantisce l'erogazione dei servizi richiesti.*
Responsabilità sociali d'impresa	*Queste dovrebbero essere informazioni di pubblico dominio che vengono fornite dal CISP.*
Impegni e pratiche per la sostenibilità di pubblico dominio.	*Il cliente può verificare se il CISP si è impegnato a gestire la propria azienda nel rispetto dell'ambiente*
Il CISP deve dimostrare di avere investito in innovazione e di avere sviluppato nuovi servizi utili negli ultimi 5 anni, in particolare nei campi dei servizi PaaS, machine learning e analisi, big data, servizi gestiti e funzioni di ottimizzazione dell'utilizzo del cloud. Per dimostrare questo punto, è possibile presentare dei changelog o dei feed di aggiornamento di pubblico dominio.	*In questo modo, il CISP può dimostrare il proprio impegno nella realizzazione di nuovi prodotti per i clienti e nel costante aggiornamento/miglioramento dei propri prodotti. Ciò consente ai clienti di mantenere un'infrastruttura IT sempre all'avanguardia, senza ricorrere a nuovi investimenti.*

Rapporto del rivenditore/partner con il CISP
*L'**<ENTE>** richiede che il primo contraente sia affiliato al CISP in qualità di rivenditore o partner commerciale; sia autorizzato dal CISP a rivendere a soggetti terzi l'accesso diretto alle offerte del CISP; sia in possesso di una certificazione rilasciata dai CISP che ne attesti competenze ed esperienza. In questo modo, l'**<ENTE>** è esonerato dal dover verificare i termini e i servizi associati all'ulteriore livello di subfornitura tra il primo contraente del **Contratto quadro** e il CISP. Inoltre tale requisito riduce la complessità generata da ulteriori livelli di rivendita quando (1) l'**<ENTE>** esegue la propria "due diligence" per garantire che le responsabilità rispetto ai servizi forniti siano ripartite chiaramente e (2) l'**<ENTE>** svolge quotidianamente attività che comportano il consumo dei servizi cloud.*

2.2 Requisiti tecnici

Una RFP per servizi cloud deve aumentare il livello delle aspettative, costringendo i CISP a fornire le tecnologie cloud standardizzate che consentono al cliente di crearsi una soluzione personalizzata. Come accennato in precedenza, la distinzione tra ciò che è standardizzato e ciò che è personalizzato è importante in una RFP per servizi cloud. I CISP offrono servizi standardizzati a milioni di clienti, pertanto le personalizzazioni in una RFP per servizi cloud devono incentrarsi su soluzioni e risultati generali e non sui

[3] Nota: nelle RFP per servizi cloud sono richieste le informazioni societarie generali, non il numero di dipendenti o l'organigramma dell'azienda. Dal punto di vista della tecnologia cloud, non c'è correlazione tra garanzia delle prestazioni del servizio e numero di dipendenti. Al contrario, nelle RFP per servizi cloud, in un'ottica di rispetto dei requisiti contano di più le dimensioni complessive dell'azienda ed esperienza/prestazioni dimostrate.

metodi, sulle infrastrutture o sui componenti hardware sottostanti con cui vengono offerti i servizi cloud utili per la realizzazione delle soluzioni.

2.2.1 Requisiti minimi

Le tradizionali procedure di appalto per il settore IT si basano spesso su requisiti commerciali sviluppati dopo una lunga serie di sessioni di lavoro, che documentano il modo in cui l'ente lavora. Definire questi requisiti con esattezza è, nella migliore delle ipotesi, un'impresa complicata. Se questa impresa riesce, tutte le sessioni dedicate alla definizione dei requisiti documenteranno il processo aziendale storico che, di per sé, potrebbe essere già antiquato e inefficiente. Se poi questi requisiti entrano a far parte di una RFP che il CISP deve rispettare, l'unica possibilità è una soluzione personalizzata. Questo modello non è compatibile con gli appalti per il cloud.

Gli enti pubblici devono identificare chiaramente i loro obiettivi aziendali e le loro esigenze dal punto di vista delle prestazioni, ma non devono utilizzare un linguaggio prescrittivo in una RFP, cioè devono evitare di dettare la progettazione e la funzionalità del sistema. Al contrario, l'ente dovrebbe ambire a concludere l'affare migliore sul mercato. Anziché valutare offerte per centinaia o migliaia di requisiti prescrittivi, che comunque non garantirebbero l'efficienza dei servizi, gli enti dovrebbero fissare dei criteri in base ai quali valutare in che misura le tecnologie e i servizi correlati consentiranno di raggiungere o superare gli obiettivi aziendali, soddisfare le aspettative in fatto di prestazioni e correggere le regole commerciali attraverso la configurazione.

Nelle RFP per i servizi cloud devono esserci le domande giuste per trovare le soluzioni migliori. Dal momento che in un modello cloud non si acquistano beni fisici, molti dei requisiti previsti per i tradizionali appalti dei data center non sono pertinenti. ***Riciclando domande valide per i data center si otterranno inevitabilmente risposte valide per i data center****, impedendo di fatto ai CISP di presentare un'offerta, oppure generando appalti strutturati talmente male che i clienti del settore pubblico non potranno usufruire pienamente di tutti i vantaggi offerti dal cloud.*

Una RFP per servizi cloud deve concentrarsi sui requisiti di base di un CISP e dei servizi cloud, garantendo così fornitori altamente qualificati per il 1° LOTTO. I requisiti non devono essere troppo prescrittivi, per non limitare l'accesso dell'ente pubblico a un'ampia gamma di CISP qualificati.

Testo di esempio di una RFP: caratteristiche del fornitore di servizi cloud

Vedere anche i requisiti amministrativi minimi per un CISP con riferimento al 1° LOTTO

Criteri di qualificazione proposti per un CISP	*Motivazione*
Infrastruttura	
L'infrastruttura del CISP deve prevedere almeno 2 cluster di data center. Ogni cluster deve essere costituito da almeno 2 data center con connessione a bassa latenza, per garantire le distribuzioni e le implementazioni attiva-attiva a disponibilità elevata degli scenari DR-BC. I data center in ogni cluster devono essere fisicamente isolati l'uno dall'altro e indipendenti in caso di guasto.	*Il CISP deve mettere a disposizione un'infrastruttura idonea alla costruzione di applicazioni ad elevata disponibilità, dove siano evitabili singoli punti di guasto.*

Il CISP deve mettere a disposizione regioni isolate logicamente e geograficamente. I dati del cliente non devono essere replicati dal CISP al di fuori di suddette regioni.	*I requisiti di residenza dei dati prevedono che il cliente eserciti pieno controllo sul luogo in cui si trovano i suoi dati.*
Il CISP deve assicurare la connettività diretta, dedicata e privata tra i propri data center.	*La connettività privata è un requisito essenziale per poter costruire un'infrastruttura ibrida sicura.*
Il CISP deve mettere a disposizione un numero sufficiente di meccanismi, tra i quali la crittografia dei dati in transito.	*Il cliente può esigere che nessun dato transiti in forma non crittografata.*
Certificazioni minime del CISP	
Il CISP deve avere la certificazione ISO 27001.	*La revisione, la certificazione e l'accreditamento da parte di un soggetto terzo confermano che il cliente è in grado di offrire un livello benchmark di servizi (e in particolare la piattaforma) in termini di qualità, sicurezza e affidabilità. È richiesto un numero minimo di certificazioni.*
Il CISP deve offrire servizi certificati in base al regolamento GDPR nel quadro del Codice di Condotta CISPE sulla protezione dei dati, per consentire al cliente di sviluppare applicazioni conformi al regolamento GDPR.	*Il cliente deve essere in grado di costruire o eseguire applicazioni conformi al regolamento GDPR, pertanto l'offerta di servizi e strumenti conformi al regolamento GDPR deve essere un prerequisito.*
Il CISP deve presentare le relazioni degli audit condotti da soggetti terzi, come SOC 1 e 2 (che coprono i luoghi e i servizi utilizzati da EC), per una questione di trasparenza dei controlli e delle procedure del CISP.	*Il CISP deve garantire trasparenza circa il modo in cui l'applicazione viene utilizzata e gestita. I report SOC sono funzionali all'ottenimento della fiducia e della trasparenza.*
Caratteristiche del servizio	
L'infrastruttura del CISP deve essere accessibile tramite le interfacce API e una console di gestione basata sul web.	*L'accesso autonomo e le interfacce API sono uno standard obbligatorio per i fornitori CISP, i quali devono disintermediare il più possibile l'accesso dell'utente e del fornitore stesso.*
Il CISP deve offrire una serie basilare di Servizi, tra i quali: storage di oggetti, database relazionale gestito, database non relazionale gestito, bilanciatori di carico gestiti, monitoraggio e dimensionamento automatico integrato.	*Il semplice fatto di offrire macchine virtuali non è sufficiente per qualificarsi come fornitore di servizi cloud. I fornitori di servizi cloud devono offrire un insieme di servizi PaaS e IaaS che possono migliorare e velocizzare le applicazioni del cliente.*
Il CISP deve consentire al cliente di cambiare liberamente l'utilizzo e la configurazione dei suoi servizi o di spostare i dati nel/dal CISP (offerta self-service).	*L'accesso ai servizi e ai dati in modalità self-service è un requisito imprescindibile per garantire la totale indipendenza del cliente.*
Il CISP è obbligato a fornire la fatturazione "a consumo" dei propri servizi.	*La fatturazione a consumo consente al cliente di ottimizzare i costi dei carichi di lavoro, riducendo i rischi e sfruttando al meglio le applicazioni di breve durata e i PoC del CISP.*
Sicurezza dei dati e del sistema	
Il CISP deve lasciare al cliente il pieno controllo dei suoi dati, assicurandogli la libertà di scegliere dove conservare i dati (area urbana), oltre a dover garantire che nessun dato del cliente verrà spostato, salvo su iniziativa del cliente stesso.	*Il cliente deve poter controllare: dove vengono conservati i suoi dati, come viene gestito l'accesso ai contenuti; l'accesso degli utenti ai servizi e alle risorse.*

Le caratteristiche del servizio del CISP devono lasciare al cliente il pieno controllo delle sue policy di sicurezza, incluse riservatezza, integrità e disponibilità dei dati e dei sistemi.	*Il cliente deve essere in grado di definire e applicare i propri standard di sicurezza per tutti i carichi di lavoro. Non basta fidarsi che il fornitore "farà ciò che è giusto" con i dati del cliente.*
Controllo dei costi	
Il CISP deve approntare meccanismi e strumenti tali da consentire al cliente di monitorare le spese nel corso del tempo. Tali strumenti devono prevedere la segmentazione basilare dei costi per carico di lavoro, servizio e account.	
Il CISP deve offrire strumenti in grado di avvisare il cliente ogni volta che la soglia dei costi viene superata.	
Il CISP deve inviare al cliente delle fatture dettagliate. La fattura deve avere una struttura tale per cui i costi possono essere segmentati in base a carico di lavoro, ambiente e account.	

Il CISP è inoltre tenuto a rispondere alle domande seguenti riguardanti i requisiti tecnici.

SOLUZIONI

Il CISP deve dimostrare in che modo potrà fornire modelli predefiniti e soluzioni software in hosting o integrate nel CISP stesso per le soluzioni seguenti:

- *Storage*
- *DevOps*
- *Sicurezza/Conformità*
- *Big Data e strumenti di analisi*
- *Applicazioni aziendali*
- *Telecomunicazioni e reti*
- *Applicazioni geospaziali*
- *IoT*
- *[Altro]*

Dare un'idea di come è stato utilizzato il CISP per i carichi di lavoro seguenti:

- *Ripristino di emergenza*
- *Sviluppo e collaudo*
- *Archiviazione*
- *Backup e ripristino*
- *Big Data*
- *High Performance Computing (HPC)*
- *Internet of Things (IoT)*
- *Siti web*
- *Serverless Computing*
- *DevOps*
- *Distribuzione di contenuti*
- *[Altro]*

2.2.2 Confronto tra fornitori

Oltre ai requisiti minimi, in una RFP per servizi cloud è importante indicare anche in base a quali criteri saranno messe a confronto le tecnologie del CISP in caso di valutazione competitiva.

Le RFP per servizi cloud devono richiedere le funzionalità cloud necessarie per un ente, con l'intesa che il cliente è titolare dell'uso di suddette funzionalità con lo scopo di costruire la sua soluzione. Le funzionalità che non rientrano tra gli standard forniti da un CISP (ad esempio soluzioni già sviluppate attraverso i sistemi del CISP o funzioni di automazione) possono essere utilizzate per un'analisi più significativa delle "opzioni a valore aggiunto" o del "miglior rapporto qualità-prezzo" in una RFP per servizi cloud.

Gli enti pubblici spesso sollecitano la competizione tra i candidati applicando criteri di valutazione quali miglior rapporto qualità-prezzo, offerta economicamente più vantaggiosa (MEAT, Most Economically Advantageous Tender) o prezzo più basso. Nella fase di pianificazione di questa parte della RFP per servizi cloud, gli enti pubblici devono assumere un approccio che tenga conto delle peculiarità del cloud. È ad esempio importante comprendere che un semplice confronto tra le voci incluse nelle proposte dei fornitori di servizi cloud (ad esempio, calcolo o storage) non è un metodo efficace per confrontare le offerte. Piuttosto è consigliabile focalizzare l'attenzione sulle soluzioni generali, come quelle illustrate nel capitolo*2.2.1*. Gli enti pubblici potranno quindi prendere in esame requisiti specifici del cloud, come quelli elencati nell'*Appendice A - Requisiti tecnici per il confronto tra* offerenti**.**

Nella RFP devono essere indicate le caratteristiche essenziali del cloud che sono necessarie per costruire la soluzione cloud. A questo scopo, gli enti pubblici possono fare riferimento alle caratteristiche essenziali del cloud descritte dal National Institute of Standards and Technology (NIST) e anche alle relazioni di analisti di terza parte, per avere la certezza che il CISP abbia l'offerta per il cloud "più idonea" e che sia in grado di operare su grande scala.

Testo di esempio di una RFP: confronto tra fornitori

*I CISP sono tenuti a rispondere a TUTTE le domande sui requisiti tecnici nell'**Appendice A**.*

I candidati devono essere in possesso degli attributi descritti di seguito e devono spiegare in che modo la loro offerta di servizi cloud soddisfa le cinque caratteristiche essenziali del cloud computing[4].

1) ***Self-Service a richiesta**: il candidato deve garantire di poter provvedere unilateralmente alla fornitura delle risorse informatiche (ad esempio, tempo del server e storage in rete) secondo necessità e in modo automatico, senza richiedere l'interazione umana con ogni fornitore di servizi. Il candidato deve garantire che le commesse siano in grado di provvedere unilateralmente (cioè senza la verifica o l'approvazione del fornitore) alla fornitura dei servizi. Spiegare in che modo la propria offerta è compatibile con questi requisiti.*

2) ***Accesso alla rete ininterrotto**: il candidato deve offrire opzioni multiple di connettività alla rete e una di queste deve essere obbligatoriamente basata su Internet. Spiegare in che modo la propria offerta è compatibile con questi requisiti.*

3) ***Pool di risorse:** il CISP del candidato deve fornire le risorse informatiche in un pool, in modo da servire più consumatori tramite un modello multi-tenant con risorse virtuali diverse che vengono assegnate e riassegnate in modo dinamico, in base alla domanda del consumatore. L'utente può specificare la posizione a un livello di superiore di astrazione (ad esempio, Paese, regione o data center). Il candidato deve supportare la scalabilità di queste risorse entro pochi minuti, o ore, dalla richiesta di fornitura. Spiegare in che modo la propria offerta è compatibile con questi requisiti.*

4) ***Elasticità rapida**: il CISP del candidato deve supportare il provisioning e il de-provisioning del servizio (scalabilità verso l'alto o il basso), rendendo il servizio disponibile nei tempi minimi prescritti (massimo "x"*

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

ore) dalla richiesta di fornitura. Il candidato deve supportare le rettifiche della fatturazione causate da queste richieste di provisioning che arrivano giornalmente e deve farlo con frequenza oraria o giornaliera.

5) ***Servizio misurato**: il candidato deve dare visibilità all'utilizzo del servizio tramite un dashboard online o uno strumento elettronico analogo.*

In più il CISP deve:

- *Essere un leader affermato nella fornitura di servizi cloud, secondo la definizione del Quadrante magico di Gartner per i servizi IaaS*[5]
- *Fornire le relazioni svolte da analisti di terza parte, riconosciuti nel settore, in cui si attestino le capacità e l'affidabilità dei CISP.*

Infine i CISP verranno confrontati tra di loro con riferimento agli scenari previsti nell'Appendice B.

2.2.2.1 Accordi sul Livello di Servizio (Service Level Agreements - SLA)

I CISP forniscono degli accordi sul livello di servizio commerciali e standardizzati a milioni di clienti, pertanto non sono in grado di offrire accordi SLA personalizzati, come accade con un modello di data center on-premises. Tuttavia, i clienti dei CISP (spesso assistiti dai partner dei CISP) possono utilizzare il cloud sfruttando al meglio gli accordi SLA commerciali di un CISP e così soddisfare, se non addirittura superare, i propri requisiti specifici.

Le RFP per servizi cloud devono garantire che i CISP offrano le funzionalità e le istruzioni necessarie per sfruttare al meglio i loro servizi e accordi SLA commerciali, di modo che i singoli utenti finali possano soddisfare i requisiti di prestazioni e disponibilità.

Testo di esempio di una RFP: accordi SLA

Fornire informazioni, e i link corrispondenti, circa l'approccio dei CISP agli accordi SLA.

*L'**<ENTE>** dovrà tenere presenti gli accordi SLA del CISP e distribuirà i carichi di lavoro e le applicazioni più importanti in modo tale da non interrompere l'operatività nel caso uno SLA non sia rispettato.*

*L'**<ENTE>** è tenuto a mantenere associati gli accordi SLA opportuni con tutte le apparecchiature di proprietà dell'**<ENTE>** o con i servizi gestiti dell'**<ENTE>** utilizzati con il CISP.*

*Il CISP deve mettere a disposizione dell'**<ENTE>** funzionalità che forniscano a quest'ultimo visibilità costante e report sulle prestazioni operative degli accordi SLA, nonché best practice documentate che gli consentano di sfruttare al meglio l'infrastruttura esistente del CISP per strutturare i servizi in modo che siano prestazionali, duraturi e affidabili.*

2.2.3 Appalto

I termini e le condizioni del CISP devono riflettere il modo in cui funziona il modello di servizi cloud (non si tratta di acquistare beni fisici, inoltre i CISP operano su grande scala offrendo servizi standardizzati). Di conseguenza è importante che i termini e le condizioni del CISP siano incorporati e applicati nella misura più ampia possibile. Per ulteriori informazioni sui termini e sulle condizioni dell'appalto, vedere il paragrafo *2.5*.

[5] https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb

2.2.3.1 Servizi nuovi e migliorati

I CISP offrono delle prestazioni attraverso un servizio. A differenza delle tradizionali soluzioni locali, che comportano aggiornamenti e contratti di manutenzione a scadenza, i fornitori di servizi cloud forniscono semplicemente il servizio standardizzato. Per fare in modo che il modello cloud raggiunga economie di scala, le modifiche e gli aggiornamenti e dell'infrastruttura sottostante vengono distribuiti a tutti gli utenti, non solo ad alcuni, dopodiché sono i clienti stessi a dover selezionare i servizi che effettivamente utilizzano. La continuità del servizio è più alta rispetto ai sistemi locali del passato, in più i fornitori di servizi cloud aggiungono costantemente servizi nuovi o migliorati, che i clienti possono utilizzare a loro piacimento.

Se al CISP viene impedito di aggiungere servizi nuovi o migliorati dopo la data di scadenza per la presentazione di una RFP, gli enti pubblici non avranno la possibilità di usufruire delle nuove funzionalità finché non verrà rilasciata una nuova versione del Contratto quadro. Pertanto consigliamo vivamente che la fornitura dei servizi descritti nel Contratto quadro sia il più possibile ampia, così da permettere al CISP di aggiungere eventuali nuovi servizi anche dopo la data di scadenza per la presentazione. È possibile che la legislazione UE in materia di appalti pubblici ponga dei limiti all'aggiunta di nuovi servizi del CISP che implichino modifiche materiali al Contratto quadro, tuttavia eventuali aggiornamenti e nuove versioni dei servizi che non implichino modifiche materiali potrebbero essere ammessi senza causare ricorsi contro l'appalto pubblico.

Testo di esempio di una RFP: servizi nuovi e migliorati

*Il CISP deve fornire una soluzione economicamente vantaggiosa, che sfrutti da un lato le tecnologie di virtualizzazione già consolidate, dall'altro le tecnologie di nuova generazione che vengono costantemente aggiornate. L'**<ENTE>** riconosce e accetta che le tecnologie cloud potrebbero essere fornite come servizio condiviso all'**<ENTE>** ed altri clienti del CISP tramite un codice base condiviso e/o un ambiente comune e che il CISP potrebbe, di tanto in tanto, cambiare, aggiungere/eliminare funzioni, caratteristiche, prestazioni o altri aspetti dei servizi cloud e che, nel caso dette modifiche/aggiunte/eliminazioni abbiano effettivamente luogo, le specifiche tecniche del servizio cloud saranno emendate di conseguenza.*

*Questo ordine di consegna copre tutti i servizi del CISP esistenti, nuovi o migliorati, **CHE RIENTRANO NELL'AMBITO DEL CONTRATTO QUADRO**. I servizi cloud forniti dal CISP ai clienti commerciali saranno messi a disposizione dell'**<ENTE>**.*

2.2.3.2 Vendor lock-in/Reversibilità

La tecnologia cloud riduce il "vendor lock-in" (la dipendenza da un singolo fornitore) poiché non vengono acquistati beni fisici e i clienti possono decidere di spostare i loro dati da un fornitore di servizi cloud a un altro in qualsiasi momento.

Eppure è inevitabile che, anche quando si acquistano servizi cloud, persista un certo grado di "vendor lock-in": infatti non tutti i cloud sono uguali e quindi un CISP potrebbe offrire servizi e funzionalità che un altro semplicemente non è in grado di offrire, riducendo di conseguenza la capacità di usufruire di quei servizi con un altro fornitore. Un approccio prudente consiste nel richiedere ai CISP di fornire le funzionalità e i servizi necessari per uscire dai loro cloud, allegando la documentazione necessaria per utilizzare tali servizi, come una ragionevole "strategia di uscita". È infatti impossibile che un CISP conosca la configurazione specifica con cui un cliente utilizza i suoi servizi standardizzati e, per questa ragione, non può offrire un piano di uscita personalizzato.

Per affrontare questioni come la "portabilità dei dati" e il "cambio di fornitore di servizi cloud" in conformità ai requisiti dell'Articolo 6 del regolamento UE sulla libera circolazione dei dati non personali, sono in fase

di sviluppo i codici di condotta del settore che, non appena saranno pubblicati, serviranno per dimostrare tale reversibilità. I riferimenti a questi argomenti saranno disponibili sul sito web del CISPE.

Testo di esempio di una RFP: on-boarding e off-boarding

*L'**<ENTE>** è alla ricerca di offerte che forniscano una strategia di uscita ragionevole ed evitino il lock-in. L'**<ENTE>** non sta acquistando beni fisici e il CISP dovrà consentire la possibilità di innalzamento e abbassamento dello stack IT. Il CISP fornirà gli strumenti e i servizi per la portabilità in modo tale da agevolare la migrazione da/verso la piattaforma del CISP e ridurre al minimo il lock-in. La documentazione che descrive l'uso degli strumenti e dei servizi di portabilità fornita dal CISP fungerà da piano di uscita ragionevole.*

*Il CISP non può esigere impegni minimi **obbligatori** o contratti a lungo termine **obbligatori**.*

*I dati archiviati presso un fornitore di servizi possono essere esportati dal cliente in qualsiasi momento. Il CISP deve consentire all'**<ENTE>** di spostare i dati, secondo necessità, da/verso lo storage del CISP. Il CISP deve inoltre consentire il download delle immagini della macchina virtuale e la loro portabilità verso un nuovo fornitore di servizi cloud. L'**<ENTE>** può esportare le immagini della propria macchina e utilizzarle localmente o presso un altro fornitore (nel rispetto delle limitazioni di licenza del software).*

2.3 Sicurezza

Le responsabilità relative a sicurezza e conformità sono condivise tra un CISP e i suoi clienti. In questo modello, i clienti controllano l'architettura e la protezione delle applicazioni e dei dati che vengono messi nell'infrastruttura, mentre i CISP hanno la responsabilità di fornire i servizi su un'infrastruttura estremamente sicura e controllata e di offrire una gamma di funzioni di sicurezza supplementari molto ampia. In questo modello, il livello delle responsabilità del CISP e del cliente dipende dal modello di distribuzione cloud (IaaS/PaaS/SaaS) e i clienti devono sapere con chiarezza quali sono le loro responsabilità in ogni modello.

È cruciale comprendere questo modello di responsabilità condivise per poter predisporre una buona RFP per servizi cloud. Gli enti pubblici devono sapere quali sono le proprie responsabilità, quali quelle del CISP e in quali casi possono risultare utili i consulenti/gli ISV partner e le soluzioni da loro offerte.

2.3.1 Requisiti minimi

In tema di sicurezza del cloud, la parola chiave è **funzionalità**. Gli enti pubblici devono essere esigenti con i CISP e pretendere che forniscano funzionalità di sicurezza tali da garantire ai clienti che potranno assolvere ai compiti loro assegnati dal modello di responsabilità condivise. Come mostra l'elenco dei requisiti più avanti, il CISP è chiamato a fornire una funzionalità standardizzata, cosicché il cliente possa usufruirne per rendere sicuro il proprio ambiente cloud specifico.

- ***Fornire** firewall di rete e **funzionalità** firewall delle applicazioni web per creare reti private e per controllare l'accesso a istanze e applicazioni.*
- ***Fornire opzioni** di connettività che supportino le connessioni private, o dedicate, dall'ufficio del cliente o dall'ambiente locale.*
- ***Fornire** le **funzionalità** per implementare una strategia di difesa profonda e contrastare gli attacchi DDoS.*
- *Fornire **funzionalità** di crittografia dei dati per i servizi di storage e database.*
- ***Fornire opzioni** per la gestione flessibile delle chiavi, in modo da consentire al cliente di scegliere se affidare al CISP la gestione delle chiavi di crittografia o assumere direttamente il controllo completo delle proprie chiavi.*
- ***Fornire API** che consentano ai clienti di integrare la crittografia e la protezione dei dati con eventuali servizi sviluppati o distribuiti in un ambiente CISP.*

- ***Fornire*** *gli* ***strumenti*** *di distribuzione che consentono di gestire la creazione e la disattivazione delle risorse CISP in base agli standard dell'ente.*
- ***Fornire strumenti*** *di gestione della configurazione e dell'inventario per individuare le risorse del CISP e quindi monitorare e gestire le eventuali modifiche di queste risorse nel corso del tempo.*
- ***Fornire strumenti e funzionalità*** *che consentano ai clienti di vedere con esattezza cosa accade nel loro ambiente CISP.*
- ***Supportare*** *la* ***visibilità*** *avanzata delle chiamate API, inclusi dati su autore, tipo di chiamata, data, ora e origine.*
- ***Fornire opzioni*** *di aggregazione dei registri per razionalizzare le indagini e il reporting di conformità.*
- *Fornire le funzionalità per configurare le notifiche di avviso quando si verificano determinati eventi o vengono superate determinate soglie.*
- ***Fornire le funzionalità*** *per definire, applicare e gestire le policy di accesso utente di tutti i servizi del CISP.*
- ***Fornire*** *le* ***funzionalità*** *per definire i singoli account utente con autorizzazioni per tutte le risorse del CISP.*
- ***Fornire*** *le* ***funzionalità*** *per l'integrazione e l'unione con le directory aziendali, al fine di ridurre il carico amministrativo e migliorare l'esperienza dell'utente finale.*

Molti di questi requisiti sono descritti nell'*Appendice A - Requisiti tecnici per il confronto tra* offerenti.

È possibile utilizzarefunzionalità oltre lo standard minimo di sicurezza per avere un'analisi più significativa delle "opzioni a valore aggiunto" o del "miglior rapporto qualità-prezzo" in una RFP. E in tema di sicurezza, maggiore è l'integrazione e l'automazione dell'operatività, tanto meglio. Per i requisiti per il confronto tra gli offerenti, vedere ancora l'*Appendice A - Requisiti tecnici per il confronto tra* offerenti.

Gli enti pubblici devono prestare attenzione alle certificazioni e alle valutazioni per l'accreditamento del cloud, per avere la certezza che i controlli di sicurezza del CISP siano applicati. Consideriamo, ad esempio, un CISP che ha ottenuto la convalida e la certificazione da parte di un revisore indipendente, a conferma della sua conformità con lo standard di certificazione ISO 27001. Nell'Annesso A, dominio 14, dello standard ISO 27001 vengono approfonditi i controlli specifici ai quali aderisce un CISP in conformità con i requisiti ISO riguardanti acquisizione, sviluppo e manutenzione del sistema. È probabile che questi controlli coprano gran parte o tutti i controlli riguardanti acquisizione, sviluppo e manutenzione del sistema che normalmente vengono richiesti da un ente in una RFP per le risorse IT. Ha dunque senso che l'ente chieda semplicemente la certificazione ISO 27001 del CISP, anziché duplicare l'elenco dei requisiti di controllo riguardanti acquisizione, sviluppo e manutenzione del sistema in una RFP per servizi cloud.

Questo metodo di fare riferimento alle certificazioni di conformità rilasciate da terze parti può essere applicato alla maggior parte dei controlli di sicurezza e conformità, ad esempio GDPR, ISO, SOC ecc.

Testo di esempio di una RFP: sicurezza

*Il CISP deve rivelare all'***<ENTE>** *eventuali processi di sicurezza non proprietari e limitazioni tecniche, in modo da consentire che vengano raggiunti livelli soddisfacenti di protezione e flessibilità tra l'***<ENTE>** *e il fornitore di servizi.*

Il CISP deve dichiarare i ruoli e le responsabilità che gli competono in materia di sicurezza e conformità:

- *Nella proposta è necessario descrivere i ruoli e le responsabilità sia del CISP che dell'***<ENTE>** *in materia di sicurezza. È necessario dichiarare con precisione le responsabilità e descrivere i servizi del CISP che possono aiutare l'***<ENTE>** *a costruire e automatizzare le funzioni di sicurezza nel suo ambiente cloud.*
- *Occorre rispondere alle specifiche tecniche riportate nell'***APPENDICE A** *riguardo ai requisiti di sicurezza dell'***<ENTE>***.*

PROPRIETÀ E CONTROLLO DEI CONTENUTI DELL'<ENTE>

*Descrivere in che modo le funzionalità del CISP possono proteggere la privacy dei dati dell'**<ENTE>**. Includere i controlli posti in essere per la protezione dei contenuti dell'**<ENTE>**. Il CISP deve fornire un forte isolamento regionale, in modo tale che gli oggetti archiviati in una regione non escano mai da quella regione, a meno che non sia l'**<ENTE>** a trasferirli esplicitamente altrove.*

- *L'**<ENTE>** gestirà l'accesso ai propri contenuti, servizi e risorse. Il CISP deve fornire una serie di funzionalità avanzate per accesso, crittografia e registrazione, in modo da aiutare l'**<ENTE>** a raggiungere questi obiettivi. Il CISP non dovrà accedere ai contenuti dell'**<ENTE>** o utilizzarli per nessuna finalità, tranne nei casi previsti dalla legge e nella misura in cui ciò sia necessario per la gestione dei servizi del CISP e l'erogazione degli stessi all'**<ENTE>** e ai rispettivi utenti finali.*

- *L'**<ENTE>** potrà scegliere in quale regione (o regioni) archiviare i propri contenuti. Il CISP non potrà trasferire o replicare i contenuti dell'**<ENTE>** al di fuori della regione (o delle regioni) scelte, tranne nei casi previsti dalla legge e nella misura in cui ciò sia necessario per la gestione dei servizi del CISP e per l'erogazione degli stessi all'**<ENTE>** e ai rispettivi utenti finali.*

- *L'**<ENTE>** sceglierà come rendere sicuri i propri contenuti. Il CISP deve mettere a disposizione una crittografia forte per i contenuti dell'**<ENTE>**, sia in transito che in sosta, concedendo all'**<ENTE>** la possibilità di gestire le proprie chiavi di crittografia.*

- *Il CISP è tenuto ad avere un programma di controlli di sicurezza fondato su Best Practice universalmente riconosciute in materia di privacy e protezione dei dati, per consentire all'**<ENTE>** di definire, gestire e sfruttare al meglio l'ambiente di controllo sicuro del CISP. Queste procedure di controllo e di protezione devono essere convalidate in modo indipendente con valutazioni condotte da terze parti.*

Per gli enti pubblici, le certificazioni e le valutazioni di accreditamento del cloud rappresentano la garanzia che i CISP hanno predisposto controlli di sicurezza fisica e logica efficaci. Facendo riferimento a questi accreditamenti nelle RFP, è possibile semplificare le procedure di appalto ed evitare attività ripetitive e gravose o flussi di lavoro di approvazione non strettamente necessari per un ambiente cloud.

Le RFP per il cloud devono concedere ai CISP la possibilità di dimostrare la loro conformità con gli accreditamenti e le valutazioni. Come accennato in precedenza, c'è una certa sovrapposizione degli scenari di rischio e delle pratiche di gestione dei rischi tra i diversi sistemi di accreditamento esistenti. Poiché i controlli e i requisiti formano un tutt'uno in questi accreditamenti, per risolvere la questione della conformità in una RFP è più veloce richiedere ai CISP di dichiarare di essere conformi agli accreditamenti anziché duplicare l'elenco dei controlli uno a uno (molti dei quali potrebbero essere presi da una RFP precedente per i data center locali e, in quanto tali, potrebbero non essere pertinenti per il cloud computing).

NOTA: è inoltre molto importante comprendere come fare per consultare i report elencati di seguito. Ad esempio, i report SOC 1 e SOC 2 sono generalmente documenti sensibili. Occorre capire quali accordi sono necessari per poterli consultare (ad esempio, accordi di non divulgazione o NDA), invece di richiedere semplicemente che detti documenti siano allegati alla risposta a una RFP (si tratta di documenti che potrebbero essere resi pubblici attraverso atti giuridici o legislativi, compromettendo la sicurezza del cloud).

Testo di esempio di una RFP: conformità

L'uso di standard di sicurezza, conformità e operatività consolidati e derivanti dalle Best Practice nelle attività dei servizi cloud (tra cui gestione dei dati, sicurezza dei dati, riservatezza, disponibilità ecc.) semplifica la procedura di appalto delle tecnologie cloud.

*L'**<ENTE>** dovrà valutare le offerte specifiche rispetto agli standard di sicurezza, conformità e operatività accettati, come spiegato più avanti e nell'**Appendice A**. Basandosi sulla certificazione di conformità dichiarata dal fornitore per ogni standard, l'**<ENTE>** può fare riferimento alla conformità minima rispetto a tale standard nella sua valutazione dell'offerta.*

Richiedendo al CISP di garantire che la conformità allo standard minimo sarà mantenuta per tutta la durata del contratto, si otterrà il vantaggio di avere un servizio sempre conforme.

*Il CISP che presenta l'offerta (direttamente o per il tramite di un suo rivenditore) deve dimostrare di essere in possesso dei seguenti attestati, report e certificazioni rilasciati da soggetti terzi indipendenti (Nota: qualora sussistano delle limitazioni alla divulgazione di alcuni di questi attestati, report e certificazioni per motivi di sicurezza, l'**<ENTE>** si impegna a collaborare con il CISP per ottenere l'accesso con azioni concordate):*

Certificazioni/attestati	***Leggi, normative e privacy***	***Allineamenti/quadri***
☐ *C5 [Germania]*		☐ *CDSA*
☐ *Codice di condotta CISPE sulla protezione dei dati (GDPR)*		
☐ *DIACAP*	☐ *Direttiva dell'UE sulla protezione dei dati*	☐ *CIS*
☐ *DoD SRG – Livelli 2 & 4*	☐ *Clausole modello per l'UE*	☐ *Criminal Justice Info. Service (CJIS)*
☐ *HDS (Francia, Sanità)*		
☐ *FedRAMP*	☐ *FERPA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *GDPR*	☐ *Scudo UE-USA per la privacy*
☐ *ISO 9001*	☐ *GLBA*	☐ *Approdo sicuro UE*
☐ *ISO 27001*	☐ *HIPAA*	☐ *FISC*
☐ *ISO 27017*	☐ *HITECH*	☐ *FISMA*
☐ *ISO 27018*	☐ *IRS 1075*	☐ *G-Cloud [Regno Unito]*
☐ *IRAP [Australia]*	☐ *ITAR*	☐ *GxP (FDA CFR 21 Part 11)*
☐ *MTCS Tier 3 [Singapore]*	☐ *PDPA – 2010 [Malesia]*	☐ *ICREA*
☐ *PCI DSS livello 1*	☐ *PDPA – 2012 [Singapore]*	☐ *IT Grundschutz [Germania]*
☐ *Rule 17-a-4(f) della SEC*	☐ *PIPEDA [Canada]*	☐ *MARS – E*
☐ *SecNumCloud (Francia)*		
☐ *SOC1 / ISAE 3402*	☐ *Privacy Act [Australia]*	☐ *MITA 3.0*
☐ *SOC2 / SOC3*	☐ *Privacy Act [Nuova Zelanda]*	☐ *MPAA*
	☐ *Autorizzazione DPA (Spagna)*	☐ *NIST*
	☐ *U.K. DPA – 1988*	☐ *Livelli di certificazione Uptime Institute*

☐ *VPAT/articolo 508* ☐ *UK Cloud Security Principles*

Questo elenco viene fornito a puro scopo illustrativo e non intende essere esaustivo delle certificazioni e degli standard che potrebbero applicarsi ai servizi cloud.

2.3.2 Confronto tra fornitori

Come spiegato nei paragrafi precedenti con riferimento ai criteri tecnici, in una RFP per servizi cloud è importante indicare, oltre ai requisiti di sicurezza minimi, anche i criteri in base ai quali le funzionalità e i servizi offerti dal CISP saranno messi a confronto in caso di valutazione competitiva.

Per un esempio dei requisiti minimi di sicurezza per un CISP, vedere l'*Appendice A - Requisiti tecnici per il confronto tra* offerenti. Si consiglia vivamente agli enti pubblici di svolgere una valutazione dei CISP tenendo conto delle funzionalità di sicurezza elencate di seguito:

Testo di esempio di una RFP: considerazioni importanti per la sicurezza

- *Conoscenza del modello di responsabilità condivisa e relativa documentazione del CISP, per aiutare i clienti a comprendere come si delineano le responsabilità in tema di sicurezza per le funzionalità e i servizi del CISP (ad esempio, nel contesto del regolamento GDPR).*
- *Sicurezza dimostrata dell'infrastruttura del CISP, con i documenti non proprietari e di pubblico dominio che attestano il livello di sicurezza e i controlli fisici/logici posti in essere dal CISP.*
- *Supporto specifico del CISP alla sicurezza del cloud.*
- *Servizi che consentono ai clienti di formalizzare la progettazione degli account, automatizzare i controlli di sicurezza e governance del cloud, semplificare l'auditing.*
- *Funzionalità per creare, fornire e gestire un insieme di risorse sotto forma di modello (inclusi i modelli di sicurezza "gold-standard"costruiti da CISP/CISP-Partner)*
- *Funzionalità per definire operazioni di controllo affidabili e ripetibili.*
- *Funzionalità per svolgere audit continui e in tempo reale.*
- *Funzionalità per la redazione tecnica delle policy di governance del cloud.*
- *Funzionalità per creare funzioni forzate, che non possono essere annullate dagli utenti senza le autorizzazioni necessarie per la modifica.*
- *Capacità di implementare in modo affidabile quanto precedentemente scritto nelle policy, negli standard e nelle norme, nonché di creare procedure esecutive di sicurezza e conformità; tutto ciò, di rimando, crea un modello di governance del cloud funzionale e affidabile per gli ambienti IT.*
- *Servizi per la protezione dagli attacchi DDoS (Distributed Denial of Service) più comuni e frequenti nei confronti della rete e del livello di trasporto, con la capacità di scrivere regole personalizzate per attenuare gli attacchi sofisticati al livello delle applicazioni.*
- *Servizio gestito di rilevamento delle minacce*

2.3.3 Contrattualizzazione

Come accennato in precedenza, i termini e le condizioni del CISP devono riflettere il modo in cui funziona il modello di servizi cloud (non si tratta di acquistare beni fisici, inoltre i CISP operano su grande scala offrendo servizi standardizzati). Di conseguenza è importante che i termini e le condizioni del CISP siano incorporati e applicati nella misura più ampia possibile. Per ulteriori informazioni sui termini e sulle condizioni dell'appalto, vedere il paragrafo *2.5*.

Quando in ballo c'è la sicurezza, è importante che i CISP aggiornino costantemente le loro offerte o, almeno, che sia data la possibilità ai fornitori di aggiungere prodotti dopo la data di scadenza della presentazione dell'offerta, purché conformi ai parametri originali della RFP. In questo modo si tiene conto del fatto che le

funzionalità e i servizi correlati alla sicurezza si evolvono rapidamente e i CISP rilasciano spesso servizi orientati alla sicurezza che, in molti casi, sono gratuiti. È importante che venga fissato un livello di sicurezza minimo di riferimento (vedere i requisiti minimi descritti in precedenza), per garantire che le modifiche alle offerte per la sicurezza non siano peggiorative.

Il modello di responsabilità condivisa è, ovviamente, al centro della sicurezza in una RFP per servizi cloud. Ogni contraente deve sapere chiaramente quali sono le sue responsabilità in materia di sicurezza e i CISP dovrebbero essere tenuti a documentare le responsabilità del CISP/del cliente in materia di sicurezza nei confronti delle tecnologie cloud fornite dal CISP, nonché a fornire la documentazione necessaria per aiutare i clienti a integrare e automatizzare le Best Practice per la sicurezza.

Un Contratto quadro per il cloud deve offrire la flessibilità necessaria per poter rimuovere un fornitore qualora non soddisfi più i requisiti minimi di sicurezza e conformità previsti nella RFP per servizi cloud.

2.4 Prezzi

Per appaltare tecnologie cloud che tengano conto della fluttuazione della domanda, gli enti pubblici hanno bisogno di un contratto che consenta loro di pagare per i servizi in base al consumo effettivo (con la governance del cloud e la visibilità richieste per quanto riguarda utilizzo e spesa).

È importante che le RFP per servizi cloud tengano in considerazione il valore e il TCO (Total Cost Of Ownership), anziché fare semplicemente un confronto diretto dei prezzi unitari, articolo per articolo. Il criterio del prezzo unitario più basso non è compatibile con il modello cloud e pertanto non necessariamente l'appalto viene aggiudicato all'offerta economicamente più vantaggiosa o al prezzo complessivamente più basso.

Per agevolare la valutazione del prezzo del CISP, è d'aiuto provvedere alla pre-qualificazione o alla selezione dei CISP con ***requisiti minimi correlati ai prezzi****, in modo da permettere ai CISP con funzionalità simili di qualificarsi per il Contratto quadro. Nella procedura di valutazione degli ordini a chiamata e delle mini-gare, è possibile consultare una selezione di architetture cloud tipiche e gli* ***scenari di prezzo*** *che riflettono i carichi di lavoro dell'ente pubblico, chiedendo ai CISP di specificare i prezzi. Anche i test dimostrativi (Live Test Demos) sono utili per mettere a confronto le prestazioni e l'elasticità dei servizi delle tecnologie cloud fornite dai CISP. Per esaminare un test dimostrativo di esempio per le tecnologie cloud, vedere l'Appendice B.*

2.4.1 Requisiti minimi

Il capitolo dei prezzi in una RFP per servizi cloud ha quattro elementi chiave:

1. **Prezzo a consumo**: i clienti di servizi cloud stanno incorporando il modello di pagamento a consumo, in base al quale alla fine del mese si paga solo per ciò che si è utilizzato effettivamente. Questo metodo è ottimale per conoscere i parametri di utilizzo e risorse.
2. **Prezzi trasparenti**: i prezzi del CISP devono essere pubblici e trasparenti.
3. **Prezzi dinamici**: serve la flessibilità necessaria per consentire la fluttuazione dei prezzi del cloud in base ai prezzi di mercato. Questo approccio consente di beneficiare del dinamismo e della competitività dei prezzi del cloud, oltre a sostenere l'innovazione e la riduzione dei prezzi.

4. **Spesa controllata**: i CISP devono offrire strumenti per il reporting, il monitoraggio e le previsioni con cui i clienti possono (1) monitorare l'utilizzo e la spesa sia a livelli granulari che di riepilogo, (2) ricevere avvisi quando l'utilizzo e la spesa superano soglie personalizzate e (3) stimare l'utilizzo e la spesa per pianificare i futuri budget destinati al cloud.

Testo di esempio di una RFP: prezzi

*L'**<ENTE>** richiede ai CISP candidati di specificare la loro proposta in relazione al metodo e al modello di determinazione dei prezzi per la fornitura di ognuno dei servizi offerti agli utenti finali sotto forma di funzionalità cloud commerciale.*

Il CISP deve fornire:

- *Un documento contenente le definizioni dei servizi o i link alle definizioni dei servizi*
- *Un documento contenente i termini e le condizioni*
- *Un documento contenente i prezzi (i link ai prezzi al pubblico sono ammessi a condizione che, su richiesta, sia disponibile un documento completo di listino/prezzi)*

Il prezzo corrisponderà al costo della configurazione più comune del servizio. I CISP devono offrire delle opzioni di sconto in base al volume e strumenti di calcolo adeguati per determinare il prezzo effettivo di ciò che viene acquistato, più il valore complessivo a vantaggio dell'acquirente (ad esempio, servizi di ottimizzazione con conseguente abbattimento dei costi).

Nell'ambito del Contratto quadro, i responsabili degli acquisti possono interagire con i fornitori per chiedere chiarimenti circa la descrizione di un servizio, i termini e le condizioni applicati, i prezzi o il modello/documento che definisce il servizio. È necessario conservare le registrazioni di tutte le interazioni con i fornitori.

Ulteriori requisiti per i prezzi

- *Le tecnologie cloud devono essere fornite con un modello dinamico di determinazione dei prezzi, che assicuri la massima flessibilità commerciale e supporti scalabilità e crescita.*
- *Gli attributi dei prezzi devono includere quanto segue:*
  - *I prezzi sono forniti per un servizio al consumo su richiesta,? Spiegare il proprio modello per la determinazione dei prezzi.*
  - *È possibile ottenere ulteriori sconti impegnandosi a utilizzare/acquistare grandi volumi? Spiegare come, in modo dettagliato.*
  - *I prezzi sono di dominio pubblico e trasparenti? Includere i link dei prezzi al pubblico.*
  - *I prezzi sono dinamici e si adattano in modo rapido ed efficiente alla concorrenza sul mercato?*
  - *Vengono fornite best practice e risorse per monitorare la spesa?*
  - *Vengono fornite best practice e risorse per ottimizzare i costi?*

Trasparenza dei prezzi

*Data la tendenza dei prezzi delle tecnologie cloud ad abbassarsi costantemente, grazie all'innovazione e alla concorrenza, il costo unitario a consumo del servizio del CISP che viene sostenuto dall'**<ENTE>** nell'ambito del Contratto quadro non potrà mai essere superiore al prezzo unitario pubblicato sul sito web del fornitore del servizio cloud, che è valido nel momento in cui il servizio viene consumato dal cliente.*

Avvisi/report per budget e fatturazione

*Per dimostrare la fornitura e l'utilizzo delle tecnologie cloud, i CISP devono fornire all'**<ENTE>** gli strumenti necessari per generare i report di fatturazione con il dettaglio dei costi per ora, giorno o mese, per ogni account in un'ente, per prodotto o risorsa del prodotto, o per tag definiti dal cliente. L'**<ENTE>** riconosce che, nell'ambito del modello di*

*responsabilità condivisa del cloud, l'**<ENTE>** sarà responsabile dell'uso di funzionalità e strumenti per il budget e la fatturazione forniti dal CISP al fine di soddisfare i requisiti unici di previsione e reporting.*

- *Fornire informazioni sul modo in cui l'**<ENTE>** può visualizzare i dati sulla fatturazione e sull'utilizzo a livello dettagliato o sintetico, evidenziando i modelli di spesa per le risorse del CISP nel tempo, oltre a una previsione di spesa futura.*
- *Fornire informazioni su come l'**<ENTE>** può filtrare i dati di utilizzo e fatturazione in base al servizio, all'account collegato o ai tag personalizzati applicati alle risorse e creare avvisi per ricevere notifiche quando l'utilizzo dei servizi si avvicina o supera il budget/le soglie impostate dall'<**ENTE**>.*
- *Fornire informazioni su come l'**<ENTE>** può prevedere quanti servizi cloud utilizzerà in un determinato periodo di tempo, in base all'utilizzo passato. Il CISP deve fornire una **stima** di quanto fatturerà all'**<ENTE>** e consentire all'**<ENTE>** di utilizzare allarmi e budget per gli importi che si prevede utilizzerà, al fine di avere una maggiore governance sui costi e sulla spesa.*

2.4.2 Confronto tra fornitori

Gli enti pubblici spesso sollecitano la competizione tra i candidati applicando criteri di valutazione quali miglior rapporto qualità-prezzo, offerta economicamente più vantaggiosa (MEAT, Most Economically Advantageous Tender) o prezzo più basso. Quando si definiscono i prezzi degli ordini a chiamata o delle mini-gare nell'ambito di un Contratto quadro, è importante utilizzare un approccio che tenga conto delle caratteristiche uniche del cloud. È ad esempio importante comprendere che un semplice confronto tra le voci incluse nelle proposte dei fornitori di servizi cloud (ad esempio, calcolo o storage) non è un metodo efficace per confrontare le offerte, in quanto non vengono considerati aspetti importanti come le prestazioni, l'ottimizzazione dei costi tramite l'uso di servizi nativi del cloud e degli strumenti di monitoraggio del CISP, o la differenziazione dei servizi che i CISP potrebbero offrire gratuitamente. Inoltre, il prezzo di catalogo di un CISP può comprendere decine di migliaia di voci/articoli e i modelli di prezzi possono variare da un servizio all'altro e da un fornitore all'altro.

Analisi del TCO

È consigliabile concentrarsi sul costo totale di proprietà (TCO) dei casi di utilizzo definiti, che tengono conto di tutti gli aspetti di una soluzione cloud (compresi i servizi dei partner, gli sconti standardizzati del CISP, le caratteristiche tecniche in grado di aumentare le performance, ridurre/ottimizzare i costi ecc.).

Confronto in base allo scenario

Il processo di valutazione può considerare anche gli scenari tipici che corrispondono a sistemi o applicazioni comuni. Tali scenari (come il web hosting o l'implementazione di un sistema di risorse umane con un numero x di utenti ecc.) possono includere variabili come la velocità e la scala delle risorse, le prestazioni dell'applicazione o della soluzione, i tempi di accesso allo storage, dati complessi a basso volume rispetto a semplici attività di elaborazione ad alto volume e così via. Gli scenari tipici delle applicazioni o dei sistemi possono andare dall'elaborazione di volumi elevati in concomitanza con le dichiarazioni dei redditi alle notifiche di emergenza per l'allerta alluvione. Gli scenari dovranno essere esaustivi, in modo da comprendere tutte le tecnologie e i servizi che il cliente potrebbe utilizzare durante il progetto. In questo modo il cliente riuscirà a confrontare il costo complessivo stimato del progetto.

Confronto finanziario e tecnico tra scenari

È altrettanto importante tener conto dei vantaggi tecnici quando si confrontano i prezzi delle offerte dei CISP. Ad esempio, un CISP può permettere ai clienti di realizzare una topologia di ripristino di emergenza (Disaster Recovery, DR) attiva-attiva grazie al suo modello che prevede la presenza dei cluster di data center

entro una regione geografica. Un CISP che non dispone di questo tipo di ridondanza e di configurazione dei data center potrebbe costare un x% in più, a causa dei costi imputabili al ripristino di emergenza. Per capire come mai un approccio olistico ai prezzi, che includa caratteristiche tecniche aggiuntive, sia cruciale per la valutazione dei CISP, consideriamo il seguente esempio di confronto diretto, articolo per articolo.

Esempio: un cliente vuole confrontare il prezzo del servizio di storage di oggetti offerto da CISP qualificati nell'ambito di un Contratto quadro. Il CISP 1 propone un prezzo di € 0,023/GB per la voce "unità" storage. Il CISP 2 propone un prezzo di € 0,01/GB per la stessa voce. Se si facesse un semplice confronto tra unità, il cliente non farebbe domande cruciali come:

1. Quante copie ridondanti dell'oggetto sono disponibili in caso di guasto? Nell'esempio precedente, il CISP 1 è progettato per sostenere la perdita simultanea di dati in due strutture diverse e conserva copie multiple dei dati. Nel caso del CISP 2, non vengono create copie ridondanti.
2. Qual è il livello di sostenibilità degli oggetti archiviati? Per il CISP 1 è del 99,999999999%, per il CISP 2 è del 99%.
3. Considerare qual è il costo dell'intero ciclo di vita della proprietà per il progetto o il carico di lavoro totale e in che modo le funzioni di ottimizzazione possono ridurre i costi dal punto di vista dello storage e dell'utilizzo dei dati (ad esempio, aumentando l'uso delle funzioni Serverless di un CISP è possibile ridurre i costi di un x%).

Queste sono solo alcune delle tante considerazioni tecniche che incidono sui prezzi, in particolare per quanto riguarda la sicurezza e la conformità.

Le considerazioni sugli scenari per la determinazione dei prezzi includono

Tariffe base: in pratica, i prezzi pubblici dei CISP. I CISP devono rendere pubblici questi prezzi. Tuttavia, come indicato in precedenza, per confrontare in modo efficace i CISP tra di loro, i clienti possono richiedere a tutti i fornitori di determinare i prezzi in base a 3-5 scenari specifici (o un numero significativo per il cliente). Gli scenari dovranno essere esaustivi, in modo da comprendere tutte le tecnologie e i servizi che il cliente potrebbe utilizzare durante il progetto. In questo modo il cliente riuscirà a confrontare il costo complessivo stimato del progetto. I confronti effettuati a livello di singole voci/SKU tendono ad essere più problematici che utili per clienti e fornitori: i clienti dovrebbero confrontare decine di migliaia di voci di tutti i CISP, mentre i fornitori dovrebbero fornire questo livello di dettaglio e gestirlo, quando il prezzo effettivo è determinato solo dal consumo del servizio.

La valutazione delle capacità globali di un CISP è un requisito indispensabile per i clienti di servizi cloud che puntano al miglior rapporto qualità-prezzo. Ad esempio, alcuni CISP potrebbero offrire una serie di servizi gratuiti, o praticamente gratuiti, di cui una valutazione dei prezzi dovrebbe tener conto, mentre altri CISP potrebbero addebitare un costo per funzionalità analoghe.

I criteri di valutazione possono essere scritti in modo tale da consentire ai CISP di indicare le funzionalità "incluse di default" e quanto tali servizi incidono sul costo complessivo. I criteri di valutazione possono anche prendere in considerazione i prezzi del CISP a volume/a scaglioni e gli sconti commerciali disponibili, come Istanze Riservate/Istanze Spot. Ad esempio:

- x% di risparmio se i clienti acquistano capacità di calcolo riservate (1 anno, 3 anni ecc.)

- x% di sconto sui prezzi a volume/a scaglioni
- x% di risparmio sulla base di verifiche dell'architettura e ottimizzazioni dell'infrastruttura, come il passaggio all'opzione di *calcolo* più adeguata
- Come osservato in precedenza, occorre considerare qual è il costo dell'intero ciclo di vita e in che modo le funzioni di ottimizzazione possono ridurre i costi.

SCENARIO PER LA DETERMINAZIONE DEI PREZZI
Gli offerenti devono specificare i prezzi per il seguente scenario solo per le finalità di valutazione. Il prezzo effettivo si baserà sul consumo dei servizi secondo un modello di pagamento in base all'uso.

I requisiti riportati sotto sono solo indicativi ai fini della determinazione dei prezzi e vengono forniti con l'esplicita consapevolezza che, durante la durata dell'appalto, tali requisiti nominali cambieranno. Specificare i prezzi sia per 12 e 36 mesi per consumo a richiesta, sia per 12 e 36 mesi per consumo riservato.

Indicare:

- *Nome delle soluzioni proposte:*
- *Miglior prezzo dell'offerente:*

- *Ore di servizio: 24x7x365*
- *Disponibilità del servizio: 99,95%*

Gli scenari per la determinazione dei prezzi possono anche includere esempi di clienti esistenti con carichi di lavoro simili, che hanno ottimizzato la loro spesa in 1/2/3 anni, anche se utilizzano strumenti di monitoraggio e ottimizzazione del CISP, se adottano soluzioni native ottimizzate per il cloud e se godono di riduzioni dei prezzi da parte del CISP.

2.5 Impostazione/Termini e condizioni per l'esecuzione dell'appalto

Le tecnologie e le operazioni cloud fornite dal CISP sono standardizzate dal punto di vista della progettazione, pertanto anche le condizioni contrattuali sono standardizzate. Tuttavia, vi è la possibilità di modificare marginalmente questi contratti per adeguarli ai contesti legislativi e normativi locali.

Spesso le tradizionali procedure di appalto del settore IT prevedono regole rigorose che impongono ai candidati di rispettare molti o tutti i requisiti dell'appalto per non essere respinti. In alternativa, prevedono un sottoinsieme vincolante di requisiti obbligatori. Quando si utilizza questo tipo di metodo di approvvigionamento con le tecnologie cloud, che sono in realtà un insieme di componenti e strumenti standardizzati per la progettazione di una soluzione personalizzata, gli appalti tendono a non andare a buon fine.

2.5.1 Termini e condizioni

Quando si esegue un appalto con una RFP per servizi cloud, il primo passaggio consiste nell'esaminare e comprendere le condizioni commerciali esistenti del CISP che, in molti casi, sono pubblicate nel sito web del CISP in questione. Gli enti pubblici sono sempre più orientati ad accettare le condizioni commerciali dei CISP. Rientra in questo sforzo di comprensione delle condizioni commerciali anche un incontro con i CISP e con i loro partner, per approfondire i rispettivi orientamenti. La domanda chiave da porre è "perché" i CISP operano con determinate condizioni. Alcune di queste condizioni possono sembrare diverse da quelle classiche del settore IT, tuttavia sussistono ragioni molto precise per cui tali condizioni vengono inserite in un appalto per servizi cloud. Se le condizioni di pubblico dominio non sono accettabili, i CISP hanno spesso accordi leggermente modificabili per i clienti aziendali che è possibile visionare.

Oltre a esaminare i termini e le condizioni del CISP, è importante comprendere anche le policy, le normative e/o le leggi esistenti (ad esempio, in materia di tecnologie, classificazione dei dati, privacy, risorse umane ecc.). Spesso esistono policy, normative e leggi che sono concepite per l'acquisto e l'utilizzo delle offerte IT classiche, ma che possono essere in contrasto con il modello del CISP. Ad esempio, consentire solo l'uso delle tecnologie cloud incluse nel Contratto quadro originale tramite la RFP per servizi cloud. I CISP aggiungono in continuazione nuovi servizi e funzionalità. Impedire l'accesso a questi nuovi servizi semplicemente per seguire un approccio tradizionale di aggiornamento dei prodotti IT non ha senso per il cliente finale. In tale eventualità, è importante avere colloqui approfonditi con i CISP, con una seria riflessione su queste policy, normative e/o leggi.

Vantaggi dei colloqui preliminari alla RFP

Come detto in precedenza, prima di redigere una RFP è necessario dedicare del tempo a incontrare i CISP e i rispettivi fornitori, al fine di comprendere i termini e le condizioni e sensibilizzarli circa l'approccio dell'ente, le policy, le normative e le leggi vigenti. La cosa più importante di questi colloqui è assicurarsi che entrambe le parti comprendano "perché" le condizioni funzionano nel modo in cui vengono applicate. Ad esempio, i termini e le condizioni per i servizi cloud sono diversi da quelli per i tradizionali data center, servizi gestiti, hardware, software preconfezionati e sistemi integrati. Poiché si tratta di modelli unici, che comportano un'innovazione costante, i rispettivi modelli aziendali richiedono una procedura della RFP sufficientemente flessibile da consentire trattative o colloqui di chiarimento.

Grazie alla possibilità di chiarire i termini e le condizioni nel corso di colloqui o trattative, gli enti pubblici acquisiscono una maggiore conoscenza dei modelli cloud ed evitano il problema di dover rifiutare fornitori che, di fatto, potrebbero essere in grado di soddisfare i loro bisogni. Un modo di procedere tipico per l'ente è quello di identificare in anticipo determinate condizioni che è disposto a discutere e negoziare prima dell'aggiudicazione. Negoziando in anticipo con gli offerenti, l'ente avrà la certezza di ricevere le condizioni di aggiudicazione più idonee e potrà dirimere le eventuali difformità che altrimenti potrebbero portare al rifiuto di una proposta valida. Gli enti pubblici possono anche rivedere le loro policy, normative e leggi, ed entrambe le parti possono rendersi conto di come l'uso del cloud si adatterà a questi modelli. Spesso si trova il modo di lavorare con le clausole esistenti. Se tuttavia c'è un'area particolarmente problematica, i due team possono collaborare per trovare una soluzione (è meglio tenere questi colloqui molto prima di qualsiasi RFP o negoziato contrattuale successivo).

Flessibilità nelle trattative

Per poter firmare i contratti in conformità con la legislazione locale, pur basandosi sulle condizioni contrattuali standard del CISP, è consigliabile (1) richiedere ai candidati il loro contratto standard, (2) non applicare condizioni contrattuali inadeguate al momento della preparazione del contratto quadro per la RFP per servizi cloud e (3) prevedere un'opzione di negoziazione su tutte le disposizioni della procedura di consultazione e sulle proposte che daranno luogo al contratto quadro (ad eccezione, ovviamente, delle clausole obbligatorie previste dalla legge).

Nota: la portata della responsabilità condivisa è insita nel modello cloud e deve riflettersi nelle condizioni del contratto: ad esempio, il CISP conferma che i clienti sono proprietari dei loro dati e del luogo in cui

È importante che vi sia un ***insieme distinto di termini e condizioni*** *del contratto per ognuno dei LOTTI indicati in un Contratto quadro per il cloud. L'adozione di un unico approccio indifferenziato per appaltare tutti i LOTTI potrebbe causare problemi di fattibilità e compatibilità tecnica.*

risiedono, mette a disposizione gli strumenti per garantire che la scelta delle ubicazioni dei dati sia limitata, MA l'uso di tali strumenti è responsabilità del cliente o partner.

Come già osservato, le RFP che contemplano condizioni vincolanti non negoziabili sono essenzialmente una proposta "prendere o lasciare" per i fornitori, che può determinare il rigetto di una proposta altrimenti accettabile. Gli enti pubblici devono riflettere attentamente se sia il caso di utilizzare delle condizioni vincolanti, a meno che non si tratti di un obbligo di legge. Gli enti devono essere certi della reale necessità di applicare un requisito o una condizione vincolante, dal momento che le trattative future saranno vincolate a questa classificazione. L'uso di requisiti o condizioni vincolanti deve essere ridotto al minimo, in modo che l'ente possa godere della flessibilità necessaria per acquisire la tecnologia migliore e la soluzione più idonea.

Le tecnologie cloud del CISP sono peraltro completamente standardizzate e vengono erogate in modo completamente automatizzato. Un CISP non è dunque in grado di apportare nessuna modifica ai termini e alle condizioni, nel caso questa implichi una personalizzazione del servizio sottostante. Inoltre i prezzi dei servizi sono generalmente pubblici e standardizzati per tutti gli utenti, di conseguenza il CISP non è in condizione di adeguarli per poter assorbire il maggiore rischio per conto di un particolare cliente.

Acquisti indiretti

Un'alternativa all'acquisto delle tecnologie cloud direttamente da un CISP consiste nell'acquisto tramite un rivenditore del CISP. Per ulteriori informazioni sui rivenditori del CISP, vedere il paragrafo *2.1.3* precedente.

Testo di esempio di una RFP: termini e condizioni

I CISP o i rivenditori autorizzati devono dichiarare le condizioni i termini e le condizioni applicate al pubblico e devono fornire un riscontro sui termini e sulle condizioni applicate dall'<ENTE>.

L'<ENTE> intende stipulare un contratto scritto con l'aggiudicatario in base alle condizioni contrattuali offerte dallo stesso. L'offerente deve sottoporre alla valutazione dell'<ENTE> una serie di condizioni contrattuali, che rappresentano la migliore offerta commerciale e legale. Gli offerenti e l'<ENTE> possono discutere entrambe le proposte (termini e condizioni) durante la fase di <DISCUSSIONE/NEGOZIAZIONE>.

- *Le condizioni principali del Contratto quadro a livello generale dovrebbero consistere, al massimo, nei seguenti elementi:*
  - *Durata del contratto quadro*
  - *Governance del contratto quadro*
  - *Prestazioni del contratto quadro*
  - *Risoluzione del contratto quadro*
  - *Ambito di applicazione del contratto quadro*
  - *Procedura di ordinazione*
  - *Disposizioni riguardanti la privacy*
  - *IP e informazioni specifiche per categoria*
  - *Requisiti tecnici minimi che i CISP devono soddisfare, ad esempio standard di qualità, accreditamento, sicurezza e protezione dei dati.*
- *Le condizioni saranno diverse per ogni lotto del contratto quadro*
- *Le specifiche dei servizi del CISP possono essere prese in considerazione e saranno trattate al momento dell'ordine a chiamata.*

- *Consentire modifiche contrattuali: le condizioni non devono costringere i clienti e i fornitori a concordare modifiche contrattuali per aggiungere nuovi servizi o miglioramenti. I servizi cloud si evolvono così rapidamente che vengono costantemente apportati miglioramenti ai servizi, con vantaggi per l'efficienza dei clienti.*
- *Gli accordi sul livello di servizio (SLA) non dovrebbero essere definiti dal cliente. Le condizioni del cliente non dovrebbero definire accordi SLA specifici e personalizzati, che differiscano dai modelli standard di fornitura dei servizi del CISP. Grazie agli accordi SLA standard dei CISP, i CISP potranno mantenere bassi i costi, trasferirli ai clienti e, al tempo stesso, rassicurare i clienti perché i CISP potranno onorare l'accordo SLA.*
- *I massimali di responsabilità devono essere proporzionati. La responsabilità deve essere proporzionata ai servizi acquistati e i massimali di responsabilità non devono essere eccessivamente elevati. Un massimale eccessivamente elevato costituirebbe un disincentivo per i CISP ad accettare progetti di valore modesto. Questi progetti sono spesso utili per avviare una collaborazione e rappresentano una specie di "test" con cui i clienti valutano se determinate soluzioni cloud sono valide per il loro ente.*
- *I clienti devono essere proprietari dei loro dati personali. I clienti devono controllare e possedere i propri dati e avere la possibilità di determinare il luogo geografico in cui sono conservati. In questo modo, i clienti potranno evitare il "vendor lock-in" e potranno trasferire liberamente i dati a nuovi fornitori.*

2.5.2 Come scegliere l'assegnatario migliore per un progetto

Gli enti pubblici che sottoscrivono il contratto quadro possono ricorrere a un "ordine a chiamata" per i servizi di cui hanno bisogno al momento opportuno. Inserendo un ordine a chiamata nell'ambito del contratto quadro, i responsabili degli acquisti possono correggere o aggiungere dei requisiti tecnici per l'ordine a chiamata specifico, senza dover rinunciare ai vantaggi offerti dal contratto quadro.

È eventualmente possibile indire una mini-gara per individuare il fornitore migliore per un determinato carico di lavoro o progetto. Si parla di mini-gara quando un cliente aumenta il livello della concorrenza nell'ambito del contratto quadro e chiede a tutti i fornitori di un determinato lotto di rispondere a una serie di requisiti. Il cliente invita tutti i fornitori qualificati per il lotto a fare un'offerta, per questo è importante che gli aggiudicatari di una RFP per servizi cloud siano in possesso dei requisiti minimi, così da garantire uno standard elevato delle opzioni per ciascun lotto.

Come già detto, è importante che vi siano serie distinte di termini e condizioni del contratto per ogni categoria di lotto e tipo di offerta (ad esempio, soluzione IaaS/PaaS pubblica, comunitaria o privata), in quanto l'adozione di un unico approccio indifferenziato per appaltare tutti i lotti potrebbe causare problemi di fattibilità e compatibilità tecnica.

Per la selezione degli aggiudicatari, vedere il testo di esempio di una RFP nel paragrafo *2.1.4*.

2.5.3 Onboarding e offboarding

Una considerazione da tenere a mente quando si imposta un contratto quadro per il cloud è la possibilità di adottare un sistema dinamico di acquisto (Dynamic Purchasing System, DPS). Con un modello DPS, tutti i fornitori che soddisfano i requisiti minimi del contratto quadro aderiranno al contratto quadro. Non c'è un limite al numero di fornitori che possono aderire al contratto quadro e, a differenza del modello tradizionale, i fornitori possono anche richiedere di aderire al contratto quadro DPS in qualsiasi fase del suo ciclo di vita.

Suggeriamo vivamente agli enti pubblici di fissare standard elevati per assicurarsi la qualità e la garanzia del servizio da parte di fornitori qualificati, ma di non utilizzare termini troppo specifici che potrebbero escludere eventuali CISP senza consentire una concorrenza leale. In ultima analisi, l'obiettivo è quello di

evitare di saturare l'utente finale con un numero eccessivo di opzioni, mantenendo al contempo alto lo standard delle tecnologie cloud offerte.

3.0 Best Practice/Lezioni apprese

Qui di seguito sono riportate alcune lezioni apprese su come riuscire a realizzare un Contratto quadro per il cloud con una RFP per servizi cloud ben strutturata.

3.1 Governance del cloud

La governance del cloud è una responsabilità condivisa. I CISP forniscono funzionalità e servizi per l'integrazione della governance del cloud in ogni aspetto di un ambiente cloud, mentre i clienti portano i propri standard di governance esistenti e apprendono in che modo il cloud favorisce la governance del cloud.

Nel cloud i clienti hanno la possibilità di creare l'ambiente IT desiderato, anziché limitarsi alla gestione dell'ambiente esistente. Il cloud permette ai clienti di: (1) iniziare con un inventario completo di tutti i beni IT; (2) gestire tutti questi beni centralmente; e (3) predisporre un meccanismo di avvisi su utilizzo/fatturazione/sicurezza ecc. Tutti questi importanti vantaggi del cloud permettono ai clienti di avere un'architettura ottimizzata e quanto più automatizzata possibile, senza dover acquistare e installare continuamente nuovo hardware. Ciò è reso possibile dal CISP, che consente ai clienti di spostare l'attenzione dalla gestione di un'infrastruttura indifferenziata al livello operativo mission critical.

Il cloud del CISP può essere considerato un'API di dimensioni molto grandi. Sia quando viene lanciato un nuovo server che quando viene modificata un'impostazione di sicurezza, in realtà vengono effettuate delle chiamate API. Ogni modifica nell'ambiente viene registrata, ovvero vengono registrati il "chi", "cosa", "dove" e "quando" di ogni modifica. Si ottengono così la governance, il controllo e la visibilità del cloud che solo un ambiente cloud può offrire. Ciò consente ai clienti di ripensare ai modelli di governance IT esistenti e di decidere come migliorarli o snellirli sfruttando i vantaggi offerti dal cloud.

Governance del cloud significa anche comunicare e incorporare i cambiamenti positivi dei processi e le nuove competenze che derivano dal cloud. Ad esempio, i project manager sono abituati al fatto che occorrono mesi per la realizzazione di un ambiente IT, pertanto potrebbero essere indotti a sovrastimare i tempi necessari per realizzare un ambiente di sviluppo e test nel cloud (operazione che nel cloud richiede letteralmente pochi minuti). L'adattamento a questa ritrovata agilità richiederà tempo e si evolverà programma dopo programma. È importante condividere le lezioni apprese per favorire l'evoluzione costante del Contratto quadro per il cloud, rendendo i requisiti compatibili con i nuovi processi e la ritrovata agilità.

3.2 Budget per il cloud

Quando si tratta di strutturare i prezzi dei servizi cloud in base al modello al consumo e di adattarli ai requisiti di acquisto e budget del settore pubblico, ci siamo resi conto che è utile raggruppare i servizi del CISP sotto un'unica voce (calcolo, storage, reti, database, IoT ecc.), tutti all'interno della categoria Tecnologie cloud. Questo approccio assicura la flessibilità necessaria per proporre in tempo reale agli utenti tutte le tecnologie dei CISP nuove ed esistenti, oltre che per assicurare agli utenti l'accesso rapido alle risorse necessarie nel momento esatto in cui ne hanno bisogno. Risponde inoltre alle fluttuazioni della domanda e assicura un utilizzo ottimizzato e costi bassi.

Gli enti pubblici possono aggiungere eventuali voci aggiuntive agli ordini di altri lotti in un contratto quadro per il cloud, nel caso in cui abbiano bisogno di servizi gestiti o servizi di consulenza/professionali, software da un marketplace, supporto su cloud e training sulle offerte del CISP.

È possibile offrire ulteriore flessibilità contrattuale inserendo voci opzionali nel contratto, all'interno delle categorie di risorse appropriate, per essere pronti per un'eventuale crescita futura. In alternativa, se un ente volesse raggruppare le tecnologie cloud con i servizi gestiti/di consulenza/professionali sotto un'unica voce, potrebbe farlo aggiungendo una voce e chiamandola, ad esempio, "Tecnologie cloud e servizi aggiuntivi".

Di seguito è riportato un esempio di questo approccio. Nell'esempio che segue, ogni unità nella voce n° 1001 - Tecnologie cloud corrisponde a €1,00 di "Tecnologie cloud" utilizzate. Ogni mese è possibile finanziare gli incrementi degli ordini sulla base delle proiezioni di utilizzo correnti e previste.

Tabella 3. Esempio di struttura dei prezzi a voci singole.

N° VOCE	FORNITURE/SERVIZI	QUANTITÀ	UNITÀ	PREZZO UNITARIO	IMPORTO
1001	Tecnologie cloud	1.000	Cad.	€1	€1.000
1002	Servizi di consulenza	1	A settimana	€3.000	€3.000
1003	Supporto per cloud	1	Al mese	€1.000	€1.000
1004	Formazione sul cloud	1	Al giorno	€3,00	€3.000
1005	Marketplace per cloud	10	Cad.	€10	€100

Esempio di come funziona questa struttura: un ente pubblico coinvolge un CISP nella stima della quantità di servizi di tecnologia cloud che l'ente utilizzerà. L'ente concorda con il fornitore dei termini per un totale di €10 milioni su 5 anni, ovvero €2 milioni all'anno. L'ente stanzia l'importo annuale iniziale di €2 milioni. Ogni mese viene emessa una fattura e il denaro viene prelevato dal fondo per effettuare il pagamento. Viene eseguito un prelievo da quel conto. L'assorbimento di liquidità dei fondi rimanenti viene tenuto sotto controllo tramite gli strumenti di monitoraggio e previsione del CISP. Se il livello dei fondi rimanenti cala troppo, l'ente richiede al CFO fondi addizionali che possono essere impegnati per garantire i servizi.

Testo di esempio di una RFP: determinazione del prezzo - appalti

TERMINI DI PAGAMENTO
*I termini di pagamento devono essere strutturati in modo tale da pagare solo per le risorse effettivamente utilizzate dall'**<ENTE>**, come illustrato di seguito:*

1. *Pagamento mensile basato sull'effettivo uso/consumo dei servizi e secondo i prezzi al pubblico dei CISP.*

GARANZIA MINIMA E SPESA MASSIMA
*Poiché sarà impossibile per l'**<ENTE>** determinare esattamente il volume di risorse di un fornitore di servizi cloud specifico che sarà consumato in un dato periodo di tempo, gli ordini dovranno indicare le quantità unitarie a prezzo fisso per una singola voce denominata "Tecnologie cloud".*

*Ogni unità della voce che verrà ordinata equivarrà a **<€1,00>** del valore delle Tecnologie cloud ordinate. Gli ordini incrementali saranno inseriti periodicamente tramite la modifica di questo ordine in svariate quantità, in modo da offrire all'**<ENTE>** la flessibilità necessaria per pre-ordinare svariati "importi in euro" di Tecnologie cloud del CISP sulla base dell'utilizzo stimato per fabbisogni di diversa durata. L'**<ENTE>** effettuerà pre-ordini periodici delle quantità per*

importi sufficienti a coprire il costo stimato delle Tecnologie cloud che saranno utilizzate per soddisfare una varietà di fabbisogni.

N° voce	Descrizione	Quantità	Unità	Prezzo
01	Tecnologie cloud del CISP	1.000	EA	€1.000,00

ORDINE MINIMO/ORDINE INCREMENTALE
*Gli ordini saranno inviati periodicamente per svariate quantità di <10.000> unità per voce, in base all'utilizzo stimato delle Tecnologie cloud da parte dell'**<ENTE>**. Questo accordo offrirà all'**<ENTE>** la flessibilità di effettuare pre-ordini per **<10.000>** unità di "Tecnologie cloud", in base alla necessità di supportare le operazioni e di portare avanti le pratiche commerciali del cloud computing basate sul pagamento a consumo.*

*Un incremento iniziale di **<100.000>** unità al costo di **<€100.000>** verrà commissionato al momento dell'ordine a chiamata. **<x>** è il numero minimo di unità totali di voci che è possibile inserire in un singolo ordine incrementale comprendente una o più voci. **<x>** è il numero massimo di unità che è possibile ordinare nell'ambito dell'ordine di consegna, ma questo numero non può mai superare il valore dell'ordine a chiamata sommato a tutte le unità ordinate in precedenza. L'**<ENTE>** ha la responsabilità di assicurare che tutti gli ordini rientrino nei limiti specificati in questo paragrafo.*

ORDINE MASSIMO
*Il valore massimo totale dell'ordine è **<x>**, comprese **< x>** unità di una singola voce al prezzo di **<x>** per unità. Il valore si basa su una stima del fabbisogno dell'**<ENTE>** nel periodo di esecuzione, ma non è garantito.*

3.3 Comprendere il modello di business dei partner

Gli enti pubblici dovrebbero cercare di comprendere i modelli sulla base dei quali i CISP erogano le loro offerte, nonché riconoscere il ruolo fondamentale svolto dai partner che forniscono consulenza, servizi gestiti, rivendita e molto altro. Molti clienti necessitano di un fornitore di servizi cloud per la propria infrastruttura e di un integratore di sistemi (SI) o un fornitore di servizi gestiti (MSP) a cui esternalizzare le attività di pianificazione, migrazione e gestione. Vista la varietà di servizi offerti, alcuni requisiti potrebbero non essere applicabili ai fornitori di servizi cloud, ad esempio le clausole a cascata per i subappaltatori.

Queste clausole sono esemplificative per illustrare quanto sia importante capire il modo in cui i partner e i rivenditori operano rispetto ai CISP. In alcuni tipi di appalti, infatti, sono previste clausole che impongono al primo contraente di predisporre a cascata determinate clausole vincolanti per tutti i suoi partner o subappaltatori. Di norma i CISP non forniscono né fanno offerte in qualità di partner subappaltatori formali, in quanto offrono un servizio standardizzato su vasta scala che non è concepito per soddisfare le esigenze specifiche di un particolare cliente finale (inclusi i clienti del settore pubblico ai sensi di un contratto pubblico). In un modello di appalto indiretto (acquisizione di servizi cloud tramite un un rivenditore del CISP), un CISP potrebbe rifiutare queste clausole dai propri rivenditori, in quanto non applicabili a un fornitore di servizi commerciali di "2° livello". In questo caso, l'attività oggetto del contratto non viene svolta in prima persona dal CISP, ma piuttosto da un partner che utilizza l'infrastruttura CISP a tale scopo. Il CISP è quindi un fornitore commerciale (non un subappaltatore) per le attività di un partner. In un modello di appalto diretto (acquisto di servizi cloud direttamente da un CISP), un CISP di norma rifiuterebbe queste clausole "vincolanti" che sono appropriate per un subappaltatore di beni, a causa della natura commerciale dei servizi in appalto e del fatto che la maggior parte dei CISP non si serve di subappaltatori per fornire i propri servizi commerciali.

3.4 Cloud broker

Il concetto di Cloud Broker come strumento per ridurre la possibilità di "vendor lock-in" può essere problematico. Sebbene in teoria un cloud broker possa sembrare un'idea valida, nella pratica probabilmente aggiungerebbe più complessità e confusione che non valore effettivo.

Il tentativo di fare funzionare le applicazioni tra più servizi cloud contemporaneamente o in modo intercambiabile porta inevitabilmente a compromessi sul piano della capacità (**non esiste una stele di Rosetta per il cloud**). In ultima analisi, questo approccio può aggiungere un livello di complessità inutile tra i clienti del settore pubblico e i loro servizi cloud, tale da compromettere l'efficienza e i benefici perseguiti sul piano della sicurezza, con la conseguente perdita di scalabilità e agilità, l'aumento dei costi e il rallentamento dell'innovazione.

3.5 *Sourcing*/consultazione di mercato pre-RFP

Quando un ente pubblico pianifica una RFP per i servizi cloud, dovrebbe cercare di coinvolgere tutti i soggetti interessati all'interno dell'ente (dirigenti di alto livello, interlocutori commerciali, tecnologia, finanza, appalti, ufficio legale e contrattuale) fin dall'inizio del processo. In questo modo tutti i soggetti interessati possono farsi un'idea del modello cloud e, di conseguenza, avere un approccio consapevole nel rivedere i tradizionali metodi di gestione degli acquisti IT.

Per quanto riguarda il dialogo con il settore industriale, raccomandiamo vivamente agli enti pubblici di prendersi il tempo necessario per fissare colloqui e raccogliere feedback da CISP, partner dei CISP, fornitori di marketplace PaaS/SaaS ed esperti del settore. Un esempio di dialogo potrebbero essere le conferenze di settore o i seminari sulla sicurezza e sugli appalti. Un altro modo efficace per comprendere bene gli appalti per il cloud consiste nel rilasciare una richiesta di informazioni (RDI o RFI – *Request for Information*) o idealmente una bozza della richiesta di offerta (RFP). Spesso questi documenti contengono potenziali problemi che possono essere identificati, discussi e corretti prima della pubblicazione della RFP per servizi cloud definitiva.

Appendice A - Requisiti tecnici per il confronto tra offerenti

Di seguito sono elencati alcuni requisiti generici della tecnologia cloud che potrebbero essere utilizzati per confrontare i CISP in occasione degli ordini a chiamata o delle mini-gare nell'ambito di un Contratto quadro per il cloud.

1. Profilo del fornitore di servizi cloud

	Requisito
1.	***ESPERIENZA SUL MERCATO:*** *Da quanti anni il fornitore di servizi cloud opera nel segmento di mercato dei servizi cloud?*
2.	***DIVULGAZIONE E PROTEZIONE DEI DATI:*** *Il fornitore di servizi cloud aderisce ai codici di condotta riguardanti la protezione dei dati e la reversibilità? Il fornitore di servizi cloud aderisce ai principi di sviluppo open source e open API?*

2. Infrastruttura globale

	Requisito
1.	***PORTATA GLOBALE:*** *Il fornitore di servizi cloud offre un'infrastruttura globale per fornire agli utenti minore latenza e throughput elevato?*
2.	***REGIONI:*** *Il fornitore di servizi cloud è presente nelle regioni delle aree geografiche richieste?*
3.	***DOMINI/ZONE:*** *Il fornitore di servizi cloud adotta il principio di domini o zone, in base al quale più data center sono raggruppati attraverso una rete a bassa latenza per fornire un grado più elevato di alta disponibilità e tolleranza ai guasti?* • *Se sì, elencare il numero di domini e zone e il numero di data center all'interno delle aree geografiche richieste*
4.	***DISTANZA DOMINI/ZONE:*** *Il fornitore di servizi cloud crea i suoi domini o zone con data center fisicamente distanti per supportare ridondanza, alta disponibilità e latenza ridotta?*
5.	***DATA CENTER CREATI:*** *Il fornitore di servizi cloud offre data center progettati in modo che siano isolati dai guasti che si verificano in altri data enter, con alimentazione, raffreddamento e reti ridondanti?*
6.	***REPLICA DEI DATA CENTER:*** *Il fornitore di servizi cloud fornisce repliche dei dati nei data center all'interno di un dominio o zona con failover automatico?*
7.	***REPLICA DI DOMINIO/ZONA:*** *Il fornitore di servizi cloud offre repliche dei dati nei domini o zone all'interno di una regione?*

3. Infrastruttura

3.1 Calcolo

	Requisito
1.	***CALCOLO - ISTANZA ORDINARIA - SCOPO GENERALE:*** *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *Scopo generale: ottimizzata per applicazioni generiche, con un giusto equilibrio tra capacità di calcolo, memoria e risorse di rete.* o *Se sì, qual è l'istanza di maggiori dimensioni?*
2.	***CALCOLO - ISTANZA ORDINARIA - OTTIMIZZATA PER LA MEMORIA:*** *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *Con ottimizzazione per la memoria - Ottimizzazione per le applicazioni a uso intensivo della memoria* o *Se sì, qual è l'istanza di maggiori dimensioni?*
3.	***CALCOLO - ISTANZA ORDINARIA - OTTIMIZZATA PER IL CALCOLO:*** *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *Con ottimizzazione per il calcolo – Ottimizzazione per le applicazioni a calcolo intensivo* o *Se sì, qual è l'istanza di maggiori dimensioni?*
4.	***CALCOLO - ISTANZA ORDINARIA - OTTIMIZZATA PER LO STORAGE:*** *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *Con ottimizzazione per lo storage - Offre una grande quantità di capacità di storage locale* o *Se sì, qual è la capacità di storage massima (ovvero 5, 10, 20, 50 TB) e il numero massimo di dischi (HDD/SSD) di cui è possibile effettuare il provisioning e che è possibile aggiungere a un'istanza?*
5.	***CALCOLO - ISTANZA ORDINARIA - OTTIMIZZATA PER LA GRAFICA:*** *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *Grafica a basso costo - Offre accelerazione grafica a basso costo per le istanze di calcolo?* o *Se sì, qual è l'istanza di maggiori dimensioni?*
6.	***CALCOLO - ISTANZA ORDINARIA - OTTIMIZZATA PER GPU:*** *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *GPU - Offre delle GPU (Graphics Processing Unit) hardware per le applicazioni a uso intensivo della grafica* o *Se sì, quali modelli e quante GPU il fornitore di servizi cloud è in grado di offrire per istanza?*
7.	***CALCOLO - ISTANZA ORDINARIA - OTTIMIZZATA PER FPGA:*** *Il fornitore di servizi cloud offre i seguenti tipi di istanza?* • *FPGA - Fornisce i Field Programmable Gate Array (FPGA) per lo sviluppo e la distribuzione dell'accelerazione hardware personalizzata per le applicazioni.* o *Se sì, quanti FPGA il fornitore di servizi cloud è in grado di offrire per ciascuna istanza?*
8.	***CALCOLO - ISTANZE "BURSTABLE":*** *Il fornitore di servizi cloud offre istanze "bursstable" in grado di fornire una prestazione di riferimento dell'unità di elaborazione centrale (CPU) con la possibilità di raggiungere un livello superiore?*

	• *Se sì, qual è l'istanza ottimizzabile di maggiori dimensioni?*
9.	*CALCOLO - ISTANZE A USO INTENSIVO DI IO:* *Il fornitore di servizi cloud offre istanze che utilizzano unità a stato solido (SSD) Non-Volatile Memory Express (NVMe) ottimizzate per latenza ridotta, prestazioni I/O random molto elevate e throughput di lettura sequenziale elevato?* • *Se sì, qual è la capacità IOPS (numero di operazioni di input/output al secondo) massima dell'istanza di maggiori dimensioni?*
10.	*CALCOLO - STORAGE LOCALE TEMPORANEO:* *Il fornitore di servizi cloud supporta lo storage locale per le istanze di calcolo da utilizzare per lo storage temporaneo delle informazioni modificate di frequente?*
11.	*CALCOLO - SUPPORTO DI PIÙ NIC:* *Il fornitore di servizi cloud supporta più schede di interfaccia di rete (NIC), principali e aggiuntive, da allocare per un'istanza specifica?* • *Se sì, qual è il numero massimo di NIC per istanza?*
12.	*CALCOLO - AFFINITÀ ISTANZA:* *Il fornitore di servizi cloud offre agli utenti la possibilità di raggruppare in maniera logica le istanze all'interno dello stesso data center?*
13.	*CALCOLO - ANTI-AFFINITÀ DELLE ISTANZE:* *Il fornitore di servizi cloud offre agli utenti la possibilità di raggruppare in maniera logica le istanze e collocarle in data center diversi all'interno di una regione?*
14.	*CALCOLO - PROVISIONING SELF-SERVICE:* *Il fornitore di servizi cloud offre il provisioning self-service di più istanze contemporaneamente tramite un'interfaccia programmatica, una console di gestione o un portale web?*
15.	*CALCOLO - PERSONALIZZAZIONE:* *Il fornitore di servizi cloud offre delle istanze personalizzabili, ovvero la possibilità di modificare impostazioni di configurazione quali le unità centrali di elaborazione virtuali (vCPU) e la memoria RAM?*
16.	*CALCOLO - TENANCY:* *Il fornitore di servizi cloud offre istanze a tenant singolo in esecuzione su hardware dedicato a un unico utente?* • *Se sì, qual è l'istanza a tenant singolo più grande disponibile?*
17.	*CALCOLO - AFFINITÀ HOST:* *Il fornitore di servizi cloud offre la possibilità di avviare un'istanza e specificare che venga sempre riavviata sullo stesso host fisico?*
18.	*CALCOLO - ANTI-AFFINITÀ HOST:* *Il fornitore di servizi cloud offre la possibilità di suddividere e ospitare specifiche istanze su diversi host fisici?*
19.	*CALCOLO - SCALABILITÀ AUTOMATICA:* *Il fornitore di servizi cloud offre la possibilità di aumentare automaticamente il numero di istanze durante i picchi di domanda per mantenere le prestazioni (ovvero "scalabilità orizzontale")?*
20.	*CALCOLO - MECCANISMO DI IMPORTAZIONE DELLE IMMAGINI:* *Il fornitore di servizi cloud offre agli utenti la possibilità di importare le immagini esistenti e salvarle come immagini nuove e privatamente disponibili, utilizzabili per effettuare il provisioning delle istanze in futuro?* • *Se sì, quali sono i formati supportati?*
21.	*CALCOLO - MECCANISMO DI ESPORTAZIONE DELLE IMMAGINI:*

	Il fornitore di servizi cloud dà la possibilità di prendere un'istanza esistente in esecuzione o una copia di un'istanza e di esportarla in un formato di macchina virtuale? • *Se sì, quali sono i formati supportati?*
22.	*CALCOLO - INTERRUZIONE DEL SERVIZIO:* *Il fornitore di servizi cloud offre meccanismi per evitare interruzioni di istanze o tempi di fermo durante le attività di manutenzione dell'hardware o del servizio a livello di host?*
23.	*CALCOLO - RIAVVIO DI ISTANZE:* *Il fornitore di servizi cloud offre meccanismi per riavviare automaticamente le istanze su un host integro se l'host fisico originale smette di funzionare?*
24.	*CALCOLO - NOTIFICHE:* *Qualora dovesse verificarsi un evento di resilienza di calcolo, il fornitore di servizi cloud ha la capacità di notificare tale evento all'utente e l'utente può scegliere di ricevere o meno tale notifica tramite un'opzione self-service?*
25.	*CALCOLO - PIANIFICAZIONE EVENTI:* *Il fornitore di servizi cloud offre la capacità di pianificare eventi per le istanze dell'utente, come riavvio, interruzione, avvio o ritiro dell'istanza?*
26.	*CALCOLO - MECCANISMO DI BACKUP E RIPRISTINO:* *Il fornitore di servizi cloud offre un meccanismo di backup e ripristino integrato?*
27.	*CALCOLO - MECCANISMO DI SNAPSHOT:* *Il fornitore di servizi cloud offre un meccanismo di snapshot on demand manuale?*
28.	*CALCOLO - METADATI:* *Il fornitore di servizi cloud offre un servizio per i metadati dell'istanza che consente agli utenti di impostare coppie chiave-valore arbitrarie per l'istanza?*
29.	*CALCOLO - CHIAMATA DEI METADATI:* *Il fornitore di servizi cloud offre un servizio per i metadati dell'istanza che fornisce un'API utilizzabile dall'istanza per avere informazioni su se stessa?*
30.	*CALCOLO - MECCANISMO DI OFFERTA:* *Il fornitore di servizi cloud offre un meccanismo di offerta per fare un'offerta per le istanze più economiche e di cui sia possibile avviare le istanze immediatamente per ospitare carichi di lavoro non mission critical?*
31.	*CALCOLO - MECCANISMO DI PIANIFICAZIONE:* *Il fornitore di servizi cloud offre un modo per pianificare e prenotare capacità di elaborazione aggiuntive su base periodica, ovvero piano giornaliero, settimanale, mensile?*
32.	*CALCOLO - MECCANISMO DI PRENOTAZIONE:* *Il fornitore di servizi cloud offre un modo per prenotare capacità di elaborazione aggiuntive per il futuro (ad esempio, 1 anno, 2 anni, 3 anni e così via)?*
33.	*CALCOLO - SISTEMA OPERATIVO LINUX:* *Il fornitore di servizi cloud supporta le ultime due versioni supportate da più tempo di almeno una distribuzione Linux aziendale (come Red Hat, SUSE) e una distribuzione gratuita e ampiamente diffusa di Linux (come Ubuntu, CentOS e Debian)?*
34.	*CALCOLO - SISTEMA OPERATIVO WINDOWS:* *Il fornitore di servizi cloud supporta le ultime due versioni principali di Windows Server (Windows Server 2017 e Windows Server 2016)?*

35.	***CALCOLO - PORTABILITÀ DELLE LICENZE*** *Il fornitore di servizi cloud offre e supporta la portabilità delle licenze?* • *Se sì, indica il produttore del software e i nomi delle applicazioni software con edizioni e versioni.*
36.	***CALCOLO - RESTRIZIONI DEI SERVIZI:*** *Il fornitore di servizi cloud applica delle limitazioni (ovvero restrizioni dei servizi) relativamente alla sezione calcolo precedente?* *Esempio:* *Numero massimo di istanze per account* *Numero massimo di host dedicati per account* *Numero massimo di indirizzi IP riservati*

3.2 Reti

	Requisito
1.	***RETI - RETI VIRTUALI:*** *Il fornitore di servizi cloud offre la possibilità di creare una rete virtuale logica isolata che rappresenta la rete aziendale nel cloud?*
2.	***RETI - CONNETTIVITÀ NELLA STESSA REGIONE:*** *Il fornitore di servizi cloud supporta la connessione di due reti virtuali all'interno della stessa regione per instradare il traffico tra di esse utilizzando indirizzi IP privati?*
3.	***RETI - CONNETTIVITÀ IN REGIONI DIVERSE:*** *Il fornitore di servizi cloud supporta la connessione di due reti virtuali in regioni diverse per instradare il traffico tra di esse utilizzando indirizzi IP privati?*
4.	***RETI - SOTTORETE PRIVATA:*** *Il fornitore di servizi cloud offre la possibilità di creare reti e sottoreti virtuali completamente isolate (private) in cui è possibile effettuare il provisioning di istanze senza un indirizzo IP pubblico o instradamento a Internet?*
5.	***RETI - INTERVALLO DI INDIRIZZI PER LE RETI VIRTUALI:*** *Il fornitore di servizi cloud supporta gli intervalli di indirizzi IP specificati nella RFC 1918, nonché i blocchi Classless Inter-Domain Routing (CIDR) instradabili pubblicamente?*
6.	***RETI - PIÙ PROTOCOLLI:*** *Il fornitore di servizi cloud supporta più protocolli inclusi TCP (Transmission Control Protocol), UDP (User Datagram Protocol) e ICMP (Internet control message Protocol)?*
7.	***RETI - ASSEGNAZIONE AUTOMATICA DEGLI INDIRIZZI IP:*** *Il fornitore di servizi cloud supporta la funzionalità di assegnazione automatica di indirizzi IP pubblici a istanze?*
8.	***RETI - INDIRIZZI IP STATICI PRENOTATI:*** *Il fornitore di servizi cloud supporta gli indirizzi IP associati a un account utente, non a un'istanza specifica? L'indirizzo IP dovrebbe rimanere associato all'account fino a quando non viene rilasciato esplicitamente.*
9.	***RETI - SUPPORTO DI IPV6:*** *Il fornitore di servizi cloud supporta il protocollo IP versione 6 (IPv6) a livello di gateway o di istanza e mostra questa funzionalità agli utenti?*

10.	***RETI - PIÙ INDIRIZZI IP PER CIASCUNA NIC:*** *Il fornitore di servizi cloud offre la possibilità di assegnare un indirizzo IP primario e un indirizzo IP secondario a una scheda di interfaccia di rete (NIC) associata a un'istanza specifica?*
11.	***RETI - PIÙ NIC:*** *Il fornitore di servizi cloud supporta la capacità di assegnare più schede di interfaccia di rete (NIC) a un'istanza specifica?*
12.	***RETI - MOBILITÀ IP E NIC:*** *Il fornitore di servizi cloud supporta la capacità di spostare sia le schede di interfaccia di rete (NIC) sia gli indirizzi IP tra istanze?*
13.	***RETI - SUPPORTO PER SR-IOV:*** *Il fornitore di servizi cloud supporta funzionalità come Single Root Input/Output Virtualization (SR-IOV) per prestazioni più elevate (come pacchetti al secondo - PPS) e latenza e jitter ridotti?*
14.	***RETI - FILTRO DI INGRESSO:*** *Il fornitore di servizi cloud supporta l'aggiunta o la rimozione di regole applicabili al traffico in ingresso a istanze?*
15.	***RETI - FILTRO DI USCITA:*** *Il fornitore di servizi cloud supporta l'aggiunta o la rimozione di regole applicabili al traffico in uscita da istanze?*
16.	***RETI - ACL:*** *Il fornitore di servizi cloud fornisce liste di controllo accessi (Access Control Lists - ACLs) per controllare il traffico in entrata e in uscita dalle subnet?*
17.	***RETI - SUPPORTO PER LOG DI FLUSSO:*** *Il fornitore di servizi cloud offre la funzionalità di acquisizione di log dei flussi di traffico della rete?*
18.	***RETI - NAT:*** *Il fornitore di servizi cloud offre un servizio gestito per il gateway NAT (Network Address Translation) per abilitare istanze in una rete privata per la connessione a Internet o ad altri servizi cloud, ma impedisce che Internet avvii una connessione a tali istanze?*
19.	***RETI - CONTROLLO DELL'ORIGINE/DELLA DESTINAZIONE:*** *Il fornitore di servizi cloud è in grado di disabilitare il controllo dell'origine/della destinazione sulle schede di interfaccia di rete (NIC)?*
20.	***RETI — SUPPORTO DI VPN:*** *Il fornitore di servizi cloud supporta la connettività VPN (Virtual Private Network) tra il fornitore di servizi cloud e il data center dell'utente?*
21.	***RETI - TUNNEL VPN:*** *Il fornitore di servizi cloud supporta più connessioni VPN (Virtual Private Network) per rete virtuale?*
22.	***RETI - SUPPORTO PER VPN IPSEC:*** *Il fornitore di servizi cloud consente agli utenti di accedere ai servizi cloud tramite un tunnel VPN IPsec (Internet protocol security) o un tunnel VPN SSL (Secure Sockets Layer) sulla rete Internet pubblica?*
23.	***RETI - SUPPORTO DI BGP:*** *Il fornitore di servizi cloud adotta il protocollo BGP (Border Gateway Protocol) per migliorare il failover su tunnel VPN (Virtual Private Network) IPsec (Internet Protocol Security)?*
24.	***RETI - CONNETTIVITÀ DEDICATA PRIVATA:***

	Il fornitore di servizi cloud offre un servizio di connettività privata e diretta tra le sedi del fornitore di servizi cloud e un ufficio o ambiente di co-location per il trasferimento di dati rapido e di volumi elevati?
25.	***RETI - SISTEMA DI BILANCIAMENTO DEL CARICO FRONT-END:*** *Il fornitore di servizi cloud offre un servizio di sistema di bilanciamento del carico front-end (connesso a Internet) che riceve richieste dai client su Internet e le distribuisce tra istanze registrate con il sistema di bilanciamento del carico?*
26.	***RETI - SISTEMA DI BILANCIAMENTO DEL CARICO BACK-END:*** *Il fornitore di servizi cloud offre un servizio di sistema di bilanciamento del carico back-end (privato) che instrada il traffico a istanze ospitate in subnet private?*
27.	***RETI - SISTEMA DI BILANCIAMENTO DEL CARICO DI LIVELLO 7:*** *Il fornitore di servizi cloud offre un servizio sistema di bilanciamento del carico di livello 7 (Hypertext Transfer Protocol – HTTP) in grado di effettuare il bilanciamento di carico del traffico di rete tra più istanze?*
28.	***RETI - SISTEMA DI BILANCIAMENTO DEL CARICO DI LIVELLO 4:*** *Il fornitore di servizi cloud offre un servizio sistema di bilanciamento del carico di livello 4 (Transmission Control Protocol - TCP) in grado di effettuare il bilanciamento del carico del traffico di rete tra più istanze?*
29.	***RETI - AFFINITÀ DI SESSIONE PER I SISTEMI DI BILANCIAMENTO DEL CARICO:*** *Il fornitore di servizi cloud offre un servizio di bilanciamento del carico che supporta l'affinità di sessione?*
30.	***RETI - BILANCIAMENTO DEL CARICO BASATO SU DNS:*** *Il fornitore di servizi cloud offre un servizio di bilanciamento del carico in grado di effettuare il bilanciamento del traffico per istanze ospitate in più host che appartengono a un singolo dominio?*
31.	***RETI - LOG DEL SISTEMA DI BILANCIAMENTO DEL CARICO:*** *Il fornitore di servizi cloud offre log che acquisiscono informazioni dettagliate su tutte le richieste inviate a un sistema di bilanciamento del carico?*
32.	***RETI - DNS:*** *Il fornitore di servizi cloud offre un servizio Domain Name System (DNS) altamente disponibile e scalabile?*
33.	***RETI - INSTRADAMENTO DNS BASATO SULLA LATENZA:*** *Il fornitore di servizi cloud offre un servizio Domain Name System (DNS) che supporta l'instradamento basato su latenza (ossia, il servizio DNS risponde a query DNS con le risorse che forniscono la migliore latenza)?*
34.	***RETI - INSTRADAMENTO DNS BASATO SU AREE GEOGRAFICHE:*** *Il fornitore di servizi cloud offre un servizio Domain Name System (DNS) che supporta l'instradamento basato su aree geografiche (ovvero il servizio DNS risponde alle query DNS in base alla posizione geografica degli utenti)?*
35.	***RETI - INSTRADAMENTO DNS BASATO SU FAILOVER:*** *Il fornitore di servizi cloud offre un servizio Domain Name System (DNS) che supporta l'instradamento basato su failover (ovvero il servizio DNS instrada le query DNS a una risorsa attualmente attiva, mentre una seconda risorsa attende e diventa attiva solo in caso di problemi con la risorsa principale)?*
36.	***RETI - SERVIZIO DI REGISTRAZIONE DEI DOMINI:*** *Il fornitore di servizi cloud offre servizi di registrazione dei nomi dei domini (ovvero gli utenti possono cercare e registrare i nomi di dominio disponibili)?*
37.	***RETI - CONTROLLI DELLO STATO DNS:*** *Il fornitore di servizi cloud offre un servizio Domain Name System (DNS) che utilizza i controlli dello stato per monitorare lo stato e le prestazioni delle risorse?*
38.	***RETI - INTEGRAZIONE DI DNS E SISTEMA DI BILANCIAMENTO DEL CARICO:***

	Il fornitore di servizi cloud offre un servizio Domain Name System (DNS) che si integra con il sistema di bilanciamento del carico del fornitore stesso?
39.	***RETI - VISUAL EDITOR:*** *Il fornitore di servizi cloud offre uno strumento che consente agli utenti di creare policy per la gestione del traffico?*
40.	***RETE DI DISTRIBUZIONE DI CONTENUTI (CDN):*** *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) per distribuire contenuti a bassa latenza ed elevate velocità di trasferimento dei dati?*
41.	***RETI - SCADENZA DELLA CACHE CDN:*** *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) che consente di rimuovere un oggetto dalle edge cache prima della scadenza e che include caratteristiche come l'invalidamento di oggetti e la funzione Versioni multiple?*
42.	***RETI - ORIGINI CDN ESTERNE:*** *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) che supporta un'origine personalizzata, ovvero un server HTTP (Hypertext Transfer Protocol)?*
43.	***RETI - OTTIMIZZAZIONE CDN:*** *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) con controllo granulare per la configurazione di più server di origine e proprietà di caching per URL diversi?*
44.	***RETI - CDN CON LIMITAZIONE GEOGRAFICA:*** *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) che supporta la limitazione geografica, ossia, evitare che gli utenti in specifiche aree geografiche accedano ai contenuti?*
45.	***RETI - TOKEN CDN:*** *Il fornitore di servizi cloud fornisce un servizio di rete di distribuzione di contenuti (CDN) che supporta gli URL firmati, che solitamente includono informazioni aggiuntive come l'ora/la data di scadenza per offrire agli utenti maggiore controllo sull'accesso ai loro contenuti?*
46.	***RETI - CERTIFICATI CDN:*** *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) che supporta i certificati Secure Sockets Layer (SSL) personalizzati per la distribuzione sicura dei contenuti su HTTPS (Hypertext Transfer Protocol Secure) dalle edge location?*
47.	***RETI - CACHE MULTI-TIER CDN:*** *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) che adotta un approccio cache multi-tier con l'uso di edge cache regionali per ridurre la latenza?*
48.	***RETI - COMPRESSIONE CDN:*** *Il fornitore di servizi cloud offre un servizio di rete di distribuzione di contenuti (CDN) che supporta la compressione dei file?*
49.	***RETI - CARICAMENTI CRITTOGRAFATI CDN:*** *Il fornitore di servizi cloud offre una rete di distribuzione di contenuti (CDN) che consente agli utenti di caricare in modo sicuro i propri dati sensibili in modo che tali informazioni possano essere visualizzate solo da componenti e servizi specifici nell'infrastruttura di origine dell'utente?*
50.	***RETI - ENDPOINT:*** *Il servizio di rete del fornitore di servizi cloud offre agli utenti endpoint in grado di instradare il traffico tramite la connettività di rete interna del fornitore (ovvero tramite connettività privata) per ridurre i costi di comunicazione e migliorare la sicurezza del traffico?*
51.	***RETI - RESTRIZIONI DEI SERVIZI:***

	Il fornitore di servizi cloud applica delle limitazioni (ovvero restrizioni dei servizi) relativamente alla sezione reti precedente? *Esempio:* *Numero massimo di reti virtuali per account* *Dimensione massima di una rete virtuale* *Numero massimo di subnet per account* *Numero massimo di sistemi di bilanciamento del carico per account* *Numero massimo di voci della lista di controllo accessi (ACL)* *Numero massimo di tunnel VPN (Virtual Private Network)* *Numero massimo di origini per distribuzione* *Numero massimo di certificati per sistema di bilanciamento del carico*

3.3 Storage

	Requisito
1.	***SERVIZIO DI STORAGE A BLOCCHI:*** *Il fornitore di servizi cloud offre volumi di storage a livello di blocchi da utilizzare per le istanze di calcolo?*
2.	***STORAGE A BLOCCHI - IOPS:*** *Il fornitore di servizi cloud offre la possibilità di acquistare un target di prestazioni o un livello di prestazioni esplicito su volumi di storage a blocchi, ad esempio un determinato numero di operazioni di input/output per secondo (IOPS) o megabyte per secondo (MB/S) di throughput?*
3.	***STORAGE A BLOCCHI - UNITÀ A STATO SOLIDO:*** *Il fornitore di servizi cloud supporta supporti di storage basati su unità a stato solido (SSD) che offrono latenze di millisecondi a una cifra?* • *Se sì, qual è il numero massimo di SSD che è possibile collegare per istanza?*
4.	***STORAGE A BLOCCHI - DIMENSIONAMENTO:*** *Il fornitore di servizi cloud offre agli utenti la possibilità di aumentare le dimensioni di un volume di storage a blocchi esistente senza dover effettuare il provisioning di un nuovo volume e copiare/spostare i dati?*
5.	***STORAGE A BLOCCHI - SNAPSHOT:*** *Il fornitore di servizi cloud dispone di funzionalità di snapshot per il servizio di storage a blocchi?*
6.	***STORAGE A BLOCCHI - ELIMINAZIONE DATI:*** *Il fornitore di servizi cloud supporta l'eliminazione completa dei dati così che non siano più leggibili o accessibili da utenti e/o terze parti non autorizzati?*
7.	***STORAGE A BLOCCHI - CRITTOGRAFIA DEI DATI INATTIVI:*** *Il fornitore di servizi cloud offre la crittografia lato server dei dati inattivi per dati archiviati su volumi e relativi snapshot?* • *Se sì, qual è l'algoritmo di crittografia utilizzato?*
8.	***SERVIZIO DI STORAGE DI OGGETTI:*** *Il fornitore di servizi cloud offre lo storage di oggetti protetto, duraturo e altamente scalabile per l'archiviazione e il recupero di qualsiasi quantità di dati dal Web?*

9.	***STORAGE DI OGGETTI - ACCESSO NON FREQUENTE:*** *Il fornitore di servizi cloud offre un livello di servizio storage a costi inferiori per l'archiviazione di oggetti e file ai quali si accede meno frequentemente?*
10.	***STORAGE DI OGGETTI - DURABILITÀ INFERIORE*** *Il fornitore di servizi cloud offre un livello di ridondanza ridotta a un prezzo inferiore, in cui un utente può archiviare oggetti non critici e facilmente riproducibili?*
11.	***STORAGE DI OGGETTI - ACCESSO MENO FREQUENTE:*** *Il fornitore di servizi cloud offre un livello per dati cui si accede meno frequentemente, ma che richiedono accesso rapido?*
12.	***STORAGE DI OGGETTI - TIERING DEGLI OGGETTI:*** *Il fornitore di servizi cloud offre una funzionalità di tiering per lo storage degli oggetti, ossia la possibilità di consigliare il trasferimento di un oggetto tra classi o livelli di storage di oggetti in base alla relativa frequenza di accesso?*
13.	***STORAGE DI OGGETTI - GESTIONE DEL CICLO DI VITA:*** *Il fornitore di servizi cloud supporta la gestione del ciclo di vita degli oggetti utilizzando una configurazione del ciclo di vita che definisce il modo in cui gli oggetti vengono gestiti durante la loro vita, dalla creazione all'eliminazione?*
14.	***STORAGE DI OGGETTI - GESTIONE BASATA SU POLICY:*** *Il fornitore di servizi cloud offre la possibilità di creare e utilizzare policy per la gestione dei dati archiviati, dei relativi cicli di vita e impostazioni di tiering?*
15.	***STORAGE DI OGGETTI - POLICY BASATE SU POSIZIONE E ORA:*** *Il fornitore di servizi cloud offre agli utenti la possibilità di creare policy per limitare l'accesso ai dati in base alla posizione dell'utente e all'ora della richiesta?*
16.	***STORAGE DI OGGETTI - HOSTING DI SITI WEB:*** *Il fornitore di servizi cloud supporta l'hosting di siti web statici oltre al servizio di storage degli oggetti?*
17.	***STORAGE DI OGGETTI - CRITTOGRAFIA DEI DATI INATTIVI:*** *Il fornitore di servizi cloud supporta la crittografia lato server (SSE) dei dati inattivi in cui il fornitore stesso gestisce le chiavi di crittografia?* • *Se sì, qual è l'algoritmo di crittografia utilizzato?*
18.	***STORAGE DI OGGETTI - CRITTOGRAFIA CON CHIAVI UTENTE:*** *Il fornitore di servizi cloud offre funzionalità di crittografia lato server (SSE) utilizzando chiavi crittografiche fornite dal cliente?*
19.	***STORAGE DI OGGETTI - SERVIZIO GESTITO PER LE CHIAVI:*** *Il fornitore di servizi cloud supporta la crittografia lato server (SSE) utilizzando un servizio di gestione delle chiavi che crea le chiavi di crittografia, definisce le policy che controllano le modalità di utilizzo consentito delle chiavi e controlla le chiavi per verificare che vengano utilizzate correttamente?*
20.	***STORAGE DI OGGETTI - CHIAVE MASTER LATO CLIENT:*** *Il fornitore di servizi cloud offre agli utenti la possibilità di mantenere il controllo delle chiavi di crittografia e completare la crittografia/decrittografia di oggetti lato client?*
21.	***STORAGE DI OGGETTI - COERENZA ASSOLUTA:*** *Il fornitore di servizi cloud supporta la coerenza lettura dopo scrittura per le operazioni PUT dei nuovi oggetti?*
22.	***STORAGE DI OGGETTI - UBICAZIONE DEI DATI:*** *Il fornitore di servizi cloud offre un solido isolamento regionale affinché gli oggetti archiviati in una regione non la lascino mai a meno che l'utente non li trasferisca esplicitamente in un'altra regione?*

23.	***STORAGE DI OGGETTI - REPLICA:*** *Il fornitore di servizi cloud offre una caratteristica di replica tra regioni che consente di replicare automaticamente gli oggetti tra regioni selezionate dall'utente?*
24.	***STORAGE DI OGGETTI - FUNZIONE VERSIONI MULTIPLE:*** *Il fornitore di servizi cloud supporta la funzione Versioni multiple, ossia la capacità di archiviare e mantenere più versioni di un oggetto?*
25.	***STORAGE DI OGGETTI - CONTRASSEGNO DI NON ELIMINABILITÀ:*** *Il fornitore di servizi cloud consente a un utente la possibilità di contrassegnare una voce come non eliminabile?*
26.	***STORAGE DI OGGETTI - ELIMINAZIONE MFA:*** *Il fornitore di servizi cloud supporta l'autenticazione a più fattori (MFA) per l'eliminazione di operazioni come opzione di sicurezza aggiuntiva?*
27.	***STORAGE DI OGGETTI - CARICAMENTO IN PIÙ PARTI:*** *Il fornitore di servizi cloud consente il caricamento di un oggetto come un insieme di parti, in cui ciascuna parte è una porzione adiacente dei dati dell'oggetto e tali parti degli oggetti possono essere caricate singolarmente e in qualsiasi ordine?*
28.	***STORAGE DI OGGETTI - TAG:*** *Il fornitore di servizi cloud offre la possibilità di creare e associare tag modificabili e dinamici a livello dell'oggetto?*
29.	***STORAGE DI OGGETTI - NOTIFICHE:*** *Il fornitore di servizi cloud offre la possibilità di inviare notifiche in occasione di determinati eventi a livello dell'oggetto (ovvero operazioni di aggiunta/eliminazione)?*
30.	***STORAGE DI OGGETTI - LOG:*** *Il fornitore di servizi cloud offre la possibilità di generare log di controllo che includono dettagli su una singola richiesta di accesso, come il richiedente, l'ora della richiesta, l'operazione della richiesta, lo stato della risposta e il codice di errore?*
31.	***STORAGE DI OGGETTI - INVENTARIO PER OGGETTI:*** *Il fornitore di servizi cloud offre funzionalità di inventario degli oggetti che permette agli utenti di visualizzare rapidamente gli oggetti e il relativo stato, consentendo loro di individuare velocemente gli oggetti con accesso pubblico?*
32.	***STORAGE DI OGGETTI - INVENTARIO PER METADATI:*** *Il fornitore di servizi cloud offre funzionalità di inventario degli oggetti che permette agli utenti di visualizzare rapidamente i metadati degli oggetti?*
33.	***STORAGE DI OGGETTI - OTTIMIZZAZIONE DEI CARICAMENTI:*** *Il fornitore di servizi cloud ha la possibilità di instradare i dati da edge location al servizio di storage utilizzando un percorso di rete ottimizzato?*
34.	***STORAGE DI OGGETTI - FUNZIONALITÀ DI QUERY:*** *Il fornitore di servizi cloud offre agli utenti la possibilità di eseguire query sul servizio di storage degli oggetti utilizzando istruzioni SQL?*
35.	***STORAGE DI OGGETTI - RECUPERO DI SOTTOINSIEMI:***

	Il fornitore di servizi cloud offre agli utenti la possibilità di recuperare solo un sottoinsieme di dati da un oggetto utilizzando semplici espressioni SQL?
36.	*SERVIZIO DI STORAGE DI FILE:* *Il fornitore di servizi cloud offre un servizio di storage di file semplice e scalabile da utilizzare con istanze di calcolo nel cloud?*
37.	*STORAGE FILE - RIDONDANZA:* *Il fornitore di servizi cloud archivia gli oggetti del file system (ovvero directory, file e link) in modo ridondante in più data center o strutture per ottenere livelli di disponibilità e durabilità più elevati?*
38.	*STORAGE DI FILE - ELIMINAZIONE DATI:* *Il fornitore di servizi cloud supporta l'eliminazione dei dati di storage di file in modo che non siano più leggibili o accessibili da utenti o terze parti non autorizzati?*
39.	*STORAGE DI FILE - ALTA DISPONIBILITÀ:* *Il file system gestito del fornitore di servizi cloud fornisce un elevato livello di alta disponibilità?*
40.	*STORAGE DI FILE - NFS:* *Il fornitore di servizi cloud supporta il protocollo NFS (Network File System)?*
41.	*STORAGE FILE - SMB:* *Il fornitore di servizi cloud supporta il protocollo SMB (Server Message Block)?*
42.	*STORAGE DI FILE - CRITTOGRAFIA DEI DATI INATTIVI:* *Il servizio di storage di file del fornitore di servizi cloud supporta la crittografia dei dati inattivi?*
43.	*STORAGE DI FILE - CRITTOGRAFIA DATI IN TRANSITO:* *Il servizio di storage di file del fornitore di servizi cloud supporta la crittografia dei dati in transito?*
44.	*STORAGE DI FILE - STRUMENTO DI MIGRAZIONE DEI DATI:* *Il fornitore di servizi cloud offre uno strumento di migrazione dei dati per consentire agli utenti di spostare dati da sistemi locali nel file system basato su cloud?*
45.	*SERVIZIO DI STORAGE IN ARCHIVI:* *Il fornitore di servizi cloud offre un servizio di storage a costi estremamente bassi per l'archiviazione di file e oggetti ai quali si accede meno di frequente e quasi sempre immutabili?*
46.	*STORAGE IN ARCHIVI - TOLLERANZA AI GUASTI:* *L'architettura del fornitore di servizi cloud offre tolleranza ai guasti per il servizio di storage in archivi?*
47.	*STORAGE IN ARCHIVI - IMMUTABILITÀ:* *Il fornitore di servizi cloud supporta l'immutabilità di oggetti e file archiviati?*
48.	*STORAGE IN ARCHIVI - WORM:* *Il fornitore di servizi cloud offre funzionalità WORM (Write Once Read Many)?*
49.	*STORAGE IN ARCHIVI - RECUPERO DI SOTTOINSIEMI:* *Il fornitore di servizi cloud offre agli utenti la possibilità di recuperare solo un sottoinsieme di dati da un oggetto archiviato utilizzando semplici espressioni SQL?*
50.	*STORAGE IN ARCHIVI - RECUPERO CON VELOCITÀ DIVERSE:* *Il fornitore di servizi cloud offre agli utenti più opzioni di recupero dei dati con costi e tempi di recupero diversi?*

51.	***STORAGE IN ARCHIVI - CRITTOGRAFIA DEI DATI INATTIVI:*** *Il servizio di storage in archivi del fornitore di servizi cloud supporta la crittografia di dati inattivi?*
52.	***STORAGE - RESTRIZIONI DEI SERVIZI:*** *Il fornitore di servizi cloud applica limitazioni (ovvero restrizioni dei servizi) relativamente alla sezione storage precedente?* *Esempio:* *Dimensione massima volume* *Numero massimo di unità collegate a un'istanza* *Numero massimo di operazioni in ingresso/uscita al secondo (IOPS)* *Dimensione massima oggetto* *Numero massimo di oggetti per account storage* *Numero massimo di snapshot*

4. Amministrazione

	Requisito
1.	***AMMINISTRAZIONE - UTENTI E GRUPPI:*** *Il fornitore di servizi cloud offre un servizio per creare e gestire utenti e gruppi di utenti della relativa infrastruttura e delle relative risorse?*
2.	***AMMINISTRAZIONE - REIMPOSTAZIONE PASSWORD:*** *Il fornitore di servizi cloud consente agli utenti di reimpostare la password in modo autonomo?*
3.	***AMMINISTRAZIONE - AUTORIZZAZIONI:*** *Il fornitore di servizi cloud offre la possibilità di aggiungere autorizzazioni a utenti e gruppi a livello di risorsa?*
4.	***AMMINISTRAZIONE - AUTORIZZAZIONI TEMPORANEE:*** *Il fornitore di servizi cloud offre la possibilità di creare autorizzazioni valide per un intervallo di tempo specifico?*
5.	***AMMINISTRAZIONE - CREDENZIALI TEMPORANEE:*** *Il fornitore di servizi cloud offre agli utenti la possibilità di creare e fornire credenziali di sicurezza temporanee a utenti affidabili configurate per durare ovunque da pochi minuti a diverse ore?*
6.	***AMMINISTRAZIONE - CONTROLLO ACCESSI:*** *Il fornitore di servizi cloud offre controlli di accesso granulare alle risorse infrastrutturali?* • *Se sì, quali condizioni possono essere utilizzate da tali controlli (ovvero ora del giorno, indirizzo IP di origine e così via)?*
7.	***AMMINISTRAZIONE - POLICY INTEGRATE:*** *L'infrastruttura del fornitore di servizi cloud contiene policy di controllo degli accessi integrate che possono essere collegate a utenti e gruppi?*
8.	***AMMINISTRAZIONE - POLICY PERSONALIZZATE:*** *L'infrastruttura del fornitore di servizi cloud consente la creazione e la personalizzazione di policy di controllo degli accessi che possono essere collegate a utenti e gruppi?*
9.	***AMMINISTRAZIONE - SIMULATORE POLICY:***

	Il fornitore di servizi cloud offre un meccanismo per testare gli effetti delle policy di controllo degli accessi prima di utilizzare tali policy in ambiente di produzione?
10.	***AMMINISTRAZIONE - MFA CLOUD:*** *Il fornitore di servizi cloud supporta l'utilizzo dell'autenticazione a più fattori (MFA) come ulteriore livello di controllo degli accessi e di autenticazione all'infrastruttura in uso?*
11.	***AMMINISTRAZIONE - RESTRIZIONI DEI SERVIZI:*** *Il fornitore di servizi cloud applica delle limitazioni (ovvero restrizioni dei servizi) relativamente alla sezione amministrazione precedente?* *Esempio:* *Numero massimo di utenti* *Numero massimo di gruppi* *Numero massimo di policy gestite*

5. Sicurezza

	Requisito
1.	***SICUREZZA - CONTROLLI SUI PRECEDENTI PENALI:*** *Tutto il personale del fornitore di servizi cloud che dispone dell'accesso all'infrastruttura del servizio (sia fisico che non fisico) è soggetto ai controlli sui precedenti penali?*
2.	***SICUREZZA - ACCESSO FISICO:*** *Il fornitore di servizi cloud limita l'accesso del personale all'infrastruttura del servizio a meno che non sia presente una richiesta di assistenza o di modifica o un'autorizzazione formale analoga specifica?*
3.	***SICUREZZA - LOG DI ACCESSO:*** *Il fornitore di servizi cloud registra l'accesso del personale all'infrastruttura in uso, registrando sempre l'accesso e conservando i log per un minimo di 90 giorni?*
4.	***SICUREZZA - ACCESSI ALL'HOST:*** *Il fornitore di servizi cloud limita l'accesso del personale agli host di calcolo, automatizzando invece tutte le attività eseguite su tali host, registrando i contenuti dei processi automatizzati e conservando i log per un minimo di 90 giorni?*
5.	***SICUREZZA - CHIAVI CRITTOGRAFICHE:*** *Il fornitore di servizi cloud offre un servizio per creare e controllare le chiavi crittografiche per cifrare i dati degli utenti?*
6.	***SICUREZZA - GESTIONE CHIAVI DI ACCESSO:*** *Il fornitore di servizi cloud offre la possibilità di identificare l'ultimo utilizzo di una chiave di accesso, di ruotare le vecchie chiavi e di rimuovere gli utenti inattivi?*
7.	***SICUREZZA - CHIAVI FORNITE DAL CLIENTE:*** *Il fornitore di servizi cloud consente agli utenti di importare chiavi dalla propria infrastruttura di gestione chiavi nel servizio di gestione chiavi del fornitore di servizi?*
8.	***SICUREZZA - INTEGRAZIONE SERVIZIO CHIAVI CRITTOGRAFICHE:*** *Il servizio di gestione chiavi del fornitore di servizi cloud si integra con altri servizi cloud per fornire funzionalità di crittografia dei dati inattivi?*
9.	***SICUREZZA - HSM:***

	Il fornitore di servizi cloud offre moduli di sicurezza hardware (HSM) dedicati, ad esempio dispositivi hardware, che forniscono operazioni protette di crittografia e storage delle chiavi in un modulo hardware anti-manomissione?
10.	*SICUREZZA - DURABILITÀ CHIAVI CRITTOGRAFICHE:* *Il fornitore di servizi cloud supporta la durabilità delle chiavi, ad esempio l'archiviazione di più copie in modo che le chiavi siano disponibili quando necessario?*
11.	*SICUREZZA - SSO:* *Il fornitore di servizi cloud offre un servizio Single Sign-On (SSO) gestito che consente agli utenti di gestire centralmente l'accesso a più account e applicazioni aziendali?*
12.	*SICUREZZA – CERTIFICATI:* *Il fornitore di servizi cloud offre un servizio gestito per effettuare il provisioning, gestire e distribuire certificati Secure Sockets Layer (SSL)/Transport Layer Security (TLS)?*
13.	*SICUREZZA - RINNOVO CERTIFICATI:* *Il servizio di gestione dei certificati del fornitore di servizi cloud semplifica il rinnovo dei certificati?*
14.	*SICUREZZA - CERTIFICATI JOLLY:* *Il servizio di gestione dei certificati del fornitore di servizi cloud supporta l'uso di certificati jolly?*
15.	*SICUREZZA - AUTORITÀ DI CERTIFICAZIONE:* *Il servizio di gestione dei certificati del fornitore di servizi cloud agisce anche come autorità di certificazione (CA)?*
16.	*SICUREZZA - ACTIVE DIRECTORY:* *Il fornitore di servizi cloud offre un servizio Microsoft Active Directory (AD) gestito nel cloud?*
17.	*SICUREZZA - ACTIVE DIRECTORY LOCALE:* *Il servizio Microsoft Active Directory (AD) gestito del fornitore di servizi cloud supporta l'integrazione con servizi Microsoft Active Directory (AD) locali?*
18.	*SICUREZZA - LADP:* *Il servizio Microsoft Active Directory (AD) gestito del fornitore di servizi cloud supporta il protocollo LDAP (Lightweight Directory Access Protocol)?*
19.	*SICUREZZA - ACTIVE DIRECTORY:* *Il servizio Microsoft Active Directory (AD) gestito del fornitore di servizi cloud supporta il linguaggio SAML (Security Assertion Markup Language)?*
20.	*SICUREZZA - GESTIONE CREDENZIALI:* *Il fornitore di servizi cloud offre un servizio gestito che consente agli utenti di ruotare, gestire e recuperare facilmente credenziali, ad esempio chiavi API, credenziali di database e altre informazioni riservate?*
21.	*SICUREZZA - WAF:* *Il fornitore di servizi cloud offre un firewall per applicazioni Web (WAF) che consenta di proteggere le applicazioni Web da exploit comuni, che potrebbero influire sulla disponibilità delle applicazioni, compromettere la sicurezza e utilizzare un numero eccessivo di risorse?*
22.	*SICUREZZA - DDOS:* *Il fornitore di servizi cloud offre un servizio per la protezione dagli attacchi DDoS (Distributed Denial of Service) più comuni e frequenti verso la rete e il livello trasporto con la possibilità di scrivere regole personalizzate per ridurre attacchi sofisticati a livello delle applicazioni?*
23.	*SICUREZZA - CONSIGLI PER LA SICUREZZA:* *Il fornitore di servizi cloud offre un servizio per accedere automaticamente a potenziali vulnerabilità in applicazioni e risorse?*

24.	***SICUREZZA - RILEVAMENTO DELLE MINACCE:*** *Il fornitore di servizi cloud offre un servizio di rilevamento delle minacce gestito?*
25.	***SICUREZZA - RESTRIZIONI DEI SERVIZI:*** *Il fornitore di servizi cloud applica limitazioni (ovvero restrizioni dei servizi) relativamente alla sezione sicurezza precedente?* *Esempio:* *Numero massimo di chiavi master del cliente* *Numero massimo di moduli di sicurezza hardware (HSM)*

6. Conformità

L'elenco che segue è stato fornito a puro scopo illustrativo e non deve essere considerato esaustivo rispetto alle certificazioni e agli standard che potrebbero applicarsi ai servizi cloud.

Indicare i set di standard di conformità internazionali e specifici del settore rispettati dal fornitore di servizi cloud:

Certificazioni/attestati	***Leggi, normative e privacy***	***Allineamenti/quadri***
☐ C5 [Germania]	*☐ Direttiva dell'UE sulla protezione dei dati*	*☐ CDSA*
☐ Codice di condotta CISPE sulla protezione dei dati	*☐ Clausole modello per l'UE*	
☐ DIACAP	*☐ FERPA*	*☐ CIS*
☐ DoD SRG – Livelli 2 & 4	*☐ GDPR*	*☐ Criminal Justice Info. Service (CJIS)*
☐ FedRAMP	*☐ GLBA*	*☐ CSA*
☐ FIPS 140-2	*☐ HIPAA*	*☐ Scudo UE-USA per la privacy*
☐ HDS (Francia, Sanità)	*☐ HITECH*	*☐ Approdo sicuro UE*
☐ ISO 9001	*☐ IRS 1075*	*☐ FISC*
☐ ISO 27001	*☐ ITAR*	*☐ FISMA*
☐ ISO 27017	*☐ PDPA – 2010 [Malesia]*	*☐ G-Cloud [Regno Unito]*
☐ ISO 27018	*☐ PDPA – 2012 [Singapore]*	*☐ GxP (FDA CFR 21 Part 11)*
☐ IRAP [Australia]	*☐ PIPEDA [Canada]*	*☐ ICREA*
☐ MTCS Tier 3 [Singapore]	*☐ Privacy Act [Australia]*	*☐ IT Grundschutz [Germania]*
☐ PCI DSS livello 1	*☐ Privacy Act [Nuova Zelanda]*	*☐ MARS – E*
☐ Rule 17-a-4(f) della SEC	*☐ Autorizzazione DPA (Spagna)*	*☐ MITA 3.0*

☐ *SOC1 / ISAE 3402*	☐ *U.K. DPA – 1988*	☐ *MPAA*
☐ *SOC2 / SOC3*	☐ *VPAT/articolo 508*	☐ *NIST*
		☐ *Livelli di certificazione Uptime Institute*
		☐ *UK Cloud Security Principles*

Facendo riferimento ai report di conformità qui sopra, gli enti pubblici possono valutare le offerte uniche rispetto agli standard di sicurezza, conformità e operativi accettati. Questi report dimostrano che il CISP, grazie alla conformità dichiarata, soddisfa i controlli operativi dei data center indicati sotto, che sono obbligatori per i fornitore di servizi cloud pubblici. Richiedendo la conformità a questi report, gli enti pubblici hanno la certezza che i controlli riportati di seguito sono stati effettuati.

- *Accesso verificato: il CISP deve limitare l'accesso fisico ai soli soggetti che hanno la necessità di recarsi in un luogo per motivi professionali giustificati. Se l'accesso viene concesso, dovrà essere revocato non appena il lavoro verrà completato.*
- *Ingresso controllato e monitorato: l'ingresso all'interno del perimetro del data center deve essere controllato. Il CISP deve collocare alcuni agenti di sicurezza presso i cancelli d'ingresso del personale e assumere supervisori che controllino gli agenti e i visitatori tramite telecamere di sicurezza. Alle persone autorizzate presenti nel sito verrà consegnato un badge con autenticazione a più fattori, per limitare l'accesso alle sole aree preventivamente approvate.*
- *Addetti ai data center del CISP: i dipendenti del CISP che devono accedere regolarmente a un data center dovranno essere ammessi nelle aree pertinenti dell'edificio a seconda della mansione che svolgono, ma il loro accesso dovrà essere controllato in modo sistematico. Gli elenchi del personale devono essere controllati regolarmente da un responsabile degli accessi all'area, per verificare che l'autorizzazione di ciascun dipendente sia ancora necessaria. Se un dipendente non ha l'esigenza di accedere a un data center costantemente per motivi professionali, sarà sottoposto alla stessa procedura per visitatori.*
- *Monitoraggio degli accessi non autorizzati: i CISP devono monitorare costantemente gli accessi non autorizzati all'edificio in cui si trova il data center tramite sistemi di videosorveglianza, rilevamento delle intrusioni e monitoraggio dei registri degli accessi. Gli ingressi devono essere protetti con dispositivi che emettono allarmi acustici se una porta viene forzata o tenuta aperta.*
- *Monitoraggio della sicurezza globale da parte dei centri operativi per la sicurezza del CISP: i centri operativi per la sicurezza del CISP devono essere dislocati in tutto il mondo; sono responsabili del monitoraggio, della selezione e dell'esecuzione dei programmi di sicurezza per i data center del CISP. Devono vigilare sulla gestione degli accessi fisici e sulla risposta al rilevamento delle intrusioni, nonché offrire un supporto globale 24 ore su 24, 7 giorni su 7 giorni ai team di sicurezza locali dei data center, svolgere attività di monitoraggio continuo (ad esempio, controllo delle attività di accesso, revoca dei permessi di accesso) ed essere disponibili a intervenire e analizzare eventuali incidenti riguardanti la sicurezza.*
- *Analisi degli accessi livello per livello: l'accesso al Livello Infrastruttura deve essere limitato sulla base delle esigenze aziendali. Con l'implementazione di un'analisi degli accessi livello per livello, il diritto di accedere a ogni livello non è garantito di default. L'ingresso a un livello specifico deve essere consentito solo in presenza di una necessità effettiva di accedere a quel livello.*
- *Manutenzione dei dispositivi nell'ambito delle operazioni di routine: i team del CISP devono eseguire test diagnostici su macchine, reti e dispositivi di riserva, per garantire che siano in condizioni perfette per poter funzionare immediatamente in caso di emergenza. I controlli di manutenzione ordinaria dei dispositivi e dei servizi del data center dovrebbero rientrare nelle operazioni di routine del data center del CISP.*
- *Dispositivi di riserva pronti per le emergenze: i meccanismi per l'erogazione di acqua, energia elettrica, telecomunicazioni e connettività Internet devono essere progettati in modo ridondante, affinché il CISP possa garantire la continuità delle operazioni in situazioni di emergenza. I sistemi di alimentazione elettrica devono essere progettati in modo completamente ridondante: in caso di interruzione dell'alimentazione, dovranno essere attivati i gruppi di continuità per specifiche funzioni e i generatori per fornire energia di emergenza all'intera struttura. Sia le persone che i sistemi devono*

monitorare e controllare la temperatura e l'umidità per prevenire il surriscaldamento e ridurre ulteriormente le possibili interruzioni del servizio.

- ***Collaborazione tra tecnologia e persone per una maggiore sicurezza**: è necessario approntare delle procedure obbligatorie per ottenere l'autorizzazione ad entrare nel Livello Dati. Una di queste è la verifica e approvazione della richiesta di accesso di una persona da parte di soggetti autorizzati. Parallelamente, i sistemi di rilevamento delle minacce e delle intrusioni elettroniche devono monitorare e attivare automaticamente gli allarmi in caso di minacce rilevate o di attività sospette. Se ad esempio viene forzata o tenuta aperta una porta, scatterà un allarme. Il CISP deve dislocare le telecamere di sicurezza e conservare i filmati nel rispetto delle disposizioni legali e di conformità.*

- ***Prevenzione delle intrusioni fisiche e tecnologiche**: i punti di accesso alle sale server devono essere rafforzati con dispositivi elettronici di controllo che richiedono un'autorizzazione a più fattori. Il CISP deve anche essere pronto a impedire le intrusioni tecnologiche. I server del CISP devono essere in grado di avvertire i dipendenti di eventuali tentativi di rimozione dei dati. Nel caso improbabile di una violazione, il server deve essere automaticamente disabilitato.*

- ***Particolare attenzione a server e supporti multimediali**: i supporti multimediali utilizzati per lo storage dei dati dei clienti devono essere classificati dal CISP come critici e trattati di conseguenza, in quanto ad alto impatto, per tutto il loro ciclo di vita. Il CISP deve adottare standard rigorosi per l'installazione, la manutenzione e l'eventuale distruzione dei dispositivi quando non sono più utili. Quando un dispositivo di storage raggiunge la fine della sua vita utile, il CISP deve dismetterlo utilizzando le tecniche descritte nella specifica NIST 800-88. I supporti su cui sono archiviati i dati dei clienti non sono esclusi dal controllo del CISP fino a quando non vengono dismessi in modo sicuro.*

- ***Verifica delle procedure e dei sistemi del CISP da parte di revisori esterni**: il CISP deve essere sottoposto ad audit da parte di revisori esterni incaricati di ispezionare i data center e di condurre indagini approfondite, per confermare che vengano rispettate le regole stabilite, necessarie per ottenere le certificazioni di sicurezza pertinenti. A seconda del programma di conformità e dei requisiti che prevede, i revisori esterni possono fare domande ai dipendenti del CISP sulla gestione e sullo smaltimento dei supporti. I revisori possono anche guardare i filmati delle telecamere di sicurezza e controllare gli ingressi e i corridoi di un data center. Inoltre possono esaminare le apparecchiature, ad esempio i dispositivi elettronici per il controllo degli accessi e le telecamere di sicurezza del CISP.*

- ***Preparativi in caso di imprevisti**: il CISP deve preparasi anticipatamente per affrontare potenziali minacce ambientali, come catastrofi naturali e incendi. L'installazione di sensori automatici e di apparecchiature sensibili sono due modi in cui il CISP può proteggere i data center. È necessario installare dispositivi di rilevamento dell'acqua che avvisino i dipendenti di eventuali problemi, quando le pompe automatiche sono impegnate a rimuovere il liquido e a prevenire danni. Allo stesso modo, le attrezzature per rilevare e spegnere automaticamente gli incendi riducono i rischi e, in caso di problemi, possono allertare i dipendenti del CISP e i vigili del fuoco.*

- ***Alta disponibilità grazie a più zone di disponibilità**: il CISP deve prevedere più zone di disponibilità per garantire una maggiore tolleranza ai guasti. Ogni zona di disponibilità deve essere costituita da uno o più data center, deve essere fisicamente separata dalle altre e deve avere un sistema ridondante per l'alimentazione elettrica e le reti. Le zone di disponibilità devono essere collegate tra loro da una rete privata veloce in fibra ottica, in modo da poter realizzare applicazioni in grado di eseguire automaticamente il fail-over tra le varie zone di disponibilità, senza interruzioni.*

- ***Simulazione delle interruzioni e misurazione della nostra risposta**: il CISP deve dotarsi di un piano di continuità aziendale come guida al processo operativo che gli consenta di stabilire come evitare e ridurre le interruzioni dovute a catastrofi naturali, con misure dettagliate da adottare prima, durante e dopo un evento. Per attutire le conseguenze e prepararsi all'imprevisto, il CISP deve testare regolarmente il piano di continuità aziendale con esercitazioni che simulino diversi scenari. Il CISP deve documentare le prestazioni del personale e dei processi e quindi comunicare agli altri le lezioni apprese e le eventuali azioni correttive necessarie per migliorare il tasso di risposta. Il personale del CISP deve essere addestrato e pronto a risolvere rapidamente le interruzioni, con un processo di recupero metodico che riduca al minimo i tempi di fermo macchina dovuti a errori.*

- ***Aiuto per il conseguimento degli obiettivi di efficienza**: oltre ad occuparsi dei rischi ambientali, il CISP dovrebbe anche integrare il concetto di sostenibilità nella progettazione dei data center. Il CISP deve dichiarare in che modo si impegnerà a favore l'uso delle energie rinnovabili per i propri data center e spiegare ai clienti come possono ridurre le emissioni di carbonio rispetto ai loro data center.*

- ***Selezione della sede**: prima di scegliere una sede, il CISP deve condurre una prima valutazione ambientale e geografica. Le ubicazioni dei data center devono essere selezionate con cura per mitigare i rischi ambientali, come inondazioni, condizioni*

meteorologiche estreme e attività sismica. Le zone di disponibilità del CISP devono essere costruite in modo tale da risultare indipendenti e fisicamente separate l'una dall'altra.

- ***Ridondanza**: i data center devono essere progettati in modo da anticipare e sopperire ai problemi, pur mantenendo livelli di servizio adeguati. In caso di problemi, i processi automatizzati devono spostare il traffico dati del cliente dall'area interessata. Le applicazioni strategiche devono essere distribuite seguendo uno standard N+1: in questo modo, in caso di problemi al data center viene garantita una capacità sufficiente per consentire la distribuzione bilanciata del traffico sui siti rimanenti.*

- ***Disponibilità**: il CISP deve individuare i componenti critici del sistema, che sono necessari per assicurare la disponibilità del sistema e ripristinare il servizio in caso di interruzione. I componenti critici del sistema devono essere sottoposti a backup in più siti isolati. Ogni sito o zona di disponibilità deve essere progettato per funzionare in modo indipendente e con un'elevata affidabilità. Le zone di disponibilità dovrebbero essere connesse, di modo che le applicazioni possano eseguire automaticamente il fail-over senza interruzioni. Una caratteristica nella progettazione del sistema deve essere l'estrema resilienza del sistema e quindi la disponibilità del servizio. Una progettazione dei data center che preveda zone di disponibilità e replica dei dati dovrà consentire ai clienti del CISP di raggiungere tempi e obiettivi di recupero estremamente ridotti, nonché i livelli più elevati di disponibilità del servizio.*

- ***Pianificazione della capacità**: il CISP deve monitorare costantemente l'utilizzo dei servizi per distribuire le infrastrutture a sostegno degli impegni e dei requisiti di disponibilità. Il CISP deve mantenere un modello di pianificazione della capacità che valuti l'uso e le richieste di infrastrutture CISP almeno una volta al mese. Questo modello deve supportare la pianificazione della domanda futura e includere considerazioni quali l'elaborazione delle informazioni, le telecomunicazioni e lo storage dei registri di audit.*

CONTINUITÀ AZIENDALE e RIPRISTINO DI EMERGENZA

- ***Piano di continuità aziendale**: il piano di continuità aziendale del CISP deve descrivere le misure per evitare e ridurre le interferenze ambientali. Deve includere i dettagli operativi sulle misure da adottare prima, durante e dopo un evento. Il piano di continuità aziendale deve essere suffragato da test che includano le simulazioni dei diversi scenari. Durante e dopo i test, il CISP deve documentare le prestazioni di persone e processi, le azioni correttive e le lezioni apprese con l'obiettivo del miglioramento continuo.*

- ***Risposta alle pandemie**: il CISP deve integrare policy e procedure di risposta alle pandemie nella propria pianificazione di ripristino di emergenza, preparandosi a reagire rapidamente alle minacce di insorgenza di malattie infettive. Le strategie di mitigazione includono modelli di gestione del personale alternativi, che consentano il trasferimento dei processi critici a risorse al di fuori della regione e l'attivazione di un piano di gestione delle crisi a supporto delle operazioni aziendali critiche. I piani per le pandemie devono fare riferimento agli enti e ai regolamenti sanitari internazionali, compresi i punti di contatto con gli organismi internazionali.*

MONITORAGGIO e REGISTRAZIONE

- ***Revisione dell'accesso al data center**: è opportuno procedere a una revisione periodica dell'accesso ai data center. L'accesso viene revocato automaticamente anche quando il profilo di un dipendente viene eliminato dal sistema delle risorse umane del CISP. Inoltre, quando l'accesso di un dipendente o collaboratore scade in base alla durata della richiesta approvata, è necessario revocarne l'accesso anche se la persona continua a lavorare per il CISP.*

- ***Registri degli accessi al data center**: l'accesso fisico ai data center del CISP deve essere registrato, monitorato e conservato. Il CISP deve mettere in correlazione le informazioni che riceve dai sistemi di monitoraggio logico e fisico, per migliorare la sicurezza in funzione delle esigenze.*

- ***Monitoraggio dell'accesso al data center**: il CISP deve monitorare i data center utilizzando i centri operativi globali per la sicurezza, che si occupano del monitoraggio, della selezione e dell'attuazione dei programmi di sicurezza. Devono fornire supporto globale 24 ore su 24, 7 giorni su 7, gestendo e monitorando le attività di accesso ai data center, mettendo i team locali e gli altri team di supporto in condizione di intervenire in caso di incidenti riguardanti la sicurezza attraverso la selezione, la consulenza, l'analisi e l'invio di risposte.*

SORVEGLIANZA e RILEVAMENTO

- *TELECAMERE A CIRCUITO CHIUSO: i punti di accesso fisico alle sale server devono essere videosorvegliati con telecamere a circuito chiuso (CCTV). Le immagini devono essere conservate in ottemperanza ai requisiti legali e di conformità.*

- *Punti di ingresso al data center: l'accesso fisico presso i punti di ingresso dell'edificio deve essere sorvegliato dal personale di sicurezza utilizzando sistemi di videosorveglianza, sistemi anti-intrusione e altri dispositivi elettronici. Il personale autorizzato deve utilizzare meccanismi di autenticazione a più fattori per accedere ai data center. Gli ingressi alle sale server devono essere protetti con dispositivi che emettono allarmi acustici per innescare la risposta a un incidente se una porta viene forzata o tenuta aperta.*

- *Rilevamento delle intrusioni: è necessario che all'interno del Livello Dati siano installati sistemi elettronici anti-intrusione per monitorare, rilevare e avvisare automaticamente il personale preposto agli incidenti di sicurezza. I punti di ingresso e uscita delle sale server devono essere dotati di dispositivi di protezione che impongano l'autenticazione a più fattori a chiunque debba entrare o uscire. Tali dispositivi emettono allarmi sonori quando l'apertura della porta viene forzata senza autenticazione o quando la porta viene tenuta aperta. I dispositivi di allarme delle porte devono inoltre essere configurati in modo da rilevare i casi in cui qualcuno esca o entri in un Livello Dati senza fornire un'autenticazione a più fattori. Gli allarmi devono essere inoltrati tempestivamente ai centri operativi di sicurezza del CISP (attivi 24 ore su 24, 7 giorni su 7) per la registrazione, l'analisi e la risposta immediata.*

GESTIONE DEI DISPOSITIVI

- *Gestione dei beni: i beni del CISP devono essere gestiti in modo centralizzato, mediante un sistema di gestione dell'inventario che consenta di memorizzare e tenere traccia di proprietario, ubicazione, stato, manutenzione e altre informazioni descrittive dei beni di proprietà del CISP. Dopo l'acquisto, i beni devono essere scansionati e monitorati, mentre i beni in fase di manutenzione devono essere controllati e monitorati per quanto riguarda la proprietà, lo stato e la risoluzione.*

- *Distruzione dei supporti multimediali: i supporti multimediali utilizzati per lo storage dei dati dei clienti devono essere classificati dal CISP come critici e trattati di conseguenza, in quanto ad alto impatto, per tutto il loro ciclo di vita. Il CISP deve adottare standard rigorosi per l'installazione, la manutenzione e l'eventuale distruzione dei dispositivi quando non sono più utili. Quando un dispositivo di storage raggiunge la fine della sua vita utile, il CISP deve dismetterlo utilizzando le tecniche descritte nella specifica NIST 800-88. I supporti su cui sono archiviati i dati dei clienti non sono esclusi dal controllo del CISP fino a quando non vengono dismessi in modo sicuro.*

SISTEMI DI SUPPORTO OPERATIVO

- *Energia elettrica: i sistemi di alimentazione elettrica dei data center del CISP devono essere completamente ridondanti e la loro manutenzione deve poter essere eseguita senza alcun impatto sull'operatività, 24 ore al giorno. Il CISP deve garantire che i data center siano dotati di alimentazione di emergenza, per assicurare la disponibilità di energia e mantenere l'operatività in caso di guasto elettrico per i carichi critici ed essenziali della struttura.*

- *Clima e temperatura: i data center del CISP devono utilizzare meccanismi di controllo della climatizzazione e mantenere una temperatura operativa adeguata per i server e gli altri componenti hardware, in modo da prevenire il surriscaldamento e ridurre la possibilità di interruzioni del servizio. Il personale e i sistemi devono monitorare e verificare che umidità e temperatura rimangano entro i limiti stabiliti.*

- *Rilevamento ed estinzione degli incendi: i data center del CISP devono essere dotati di apparecchiature automatiche per rilevare ed estinguere gli incendi. I sistemi di rilevamento degli incendi devono utilizzare sensori per rilevare il fumo negli spazi meccanici, infrastrutturali e di rete. Queste aree devono essere protette anche da sistemi di estinzione degli incendi.*

- *Rilevamento delle perdite: per rilevare eventuali perdite d'acqua, il CISP deve dotare i propri data center di sistemi di rilevamento dell'acqua. Se viene rilevata acqua, devono essere predisposti i meccanismi necessari per rimuoverla ed evitare danni ulteriori.*

MANUTENZIONE DELL'INFRASTRUTTURA

- *Manutenzione delle apparecchiature: il CISP deve monitorare ed eseguire la manutenzione preventiva delle apparecchiature elettriche e meccaniche, per garantire il funzionamento ininterrotto dei sistemi all'interno dei data center del CISP. Le procedure di manutenzione delle apparecchiature devono essere eseguite da personale qualificato e completate secondo un piano di manutenzione documentato.*

- ***Gestione dell'ambiente**: il CISP deve monitorare i sistemi e le apparecchiature elettriche e meccaniche per consentire il rilevamento immediato di eventuali problemi. A tal fine, è necessario utilizzare gli strumenti di audit continuo e le informazioni fornite dai sistemi di gestione degli edifici e di monitoraggio elettrico del CISP. La manutenzione preventiva viene eseguita per garantire il funzionamento ininterrotto delle apparecchiature.*

GOVERNANCE e RISCHIO

- ***Gestione continua dei rischi del data center**: il centro operativo per la sicurezza del CISP deve effettuare valutazioni periodiche delle minacce e delle vulnerabilità dei data center. La valutazione continua e la mitigazione delle possibili vulnerabilità devono essere svolte attraverso attività di valutazione dei rischi del data center. Questa valutazione va ad aggiungersi al processo di valutazione dei rischi a livello aziendale, utilizzato per identificare e gestire i rischi che riguardano l'impresa nel suo complesso. Questo processo deve tenere conto anche dei rischi normativi e ambientali a livello regionale.*

- ***Attestato di sicurezza rilasciato da terze parti**: i test effettuati da soggetti terzi sui data center del CISP, come documentato nei rispettivi report, devono garantire che il CISP abbia attuato misure di sicurezza adeguate, in sintonia con le disposizioni necessarie per ottenere le certificazioni di sicurezza. A seconda del programma di conformità e dei relativi requisiti, i revisori esterni possono eseguire dei test sullo smaltimento dei supporti, esaminare i filmati di videosorveglianza, controllare gli ingressi e i corridoi di un data center, collaudare i dispositivi elettronici di controllo degli accessi e analizzare le apparecchiature del data center.*

7. Migrazioni

	Requisito
1.	***SERVIZIO MIGRAZIONI:*** *Quanti servizi diversi di migrazione dei dati offre il fornitore di servizi cloud?*
2.	***MIGRAZIONI - MONITORAGGIO CENTRALIZZATO:*** *Il fornitore di servizi cloud offre un servizio centralizzato (ad esempio una singola interfaccia), per consentire agli enti di tenere traccia e monitorare lo stato delle migrazioni di applicazioni e server utilizzati?*
3.	***MIGRAZIONI - PANNELLO DI CONTROLLO:*** *Lo strumento di migrazione del fornitore di servizi cloud offre un pannello di controllo per visualizzare in modo rapido lo stato delle migrazioni, i parametri correlati e la cronologia delle migrazioni?*
4.	***MIGRAZIONI - STRUMENTI DEL FORNITORE DI SERVIZI CLOUD:*** *Lo strumento di migrazione del fornitore di servizi cloud offre l'integrazione con altri strumenti di migrazione del fornitore stesso, che possono eseguire la migrazione di applicazioni e server?*
5.	***MIGRAZIONI - STRUMENTI DI TERZE PARTI:*** *Lo strumento di migrazione del fornitore di servizi cloud consente l'integrazione con strumenti di migrazione di terze parti?* • *Se sì, quali sono gli strumenti di migrazione di terze parti supportati?*
6.	***MIGRAZIONI - MIGRAZIONI TRA PIÙ REGIONI:*** *Lo strumento di migrazione del fornitore di servizi cloud offre funzionalità di tracciamento e di monitoraggio delle migrazioni di applicazioni e server che si verificano in regioni diverse?*
7.	***MIGRAZIONI - MIGRAZIONE DEI SERVER:*** *Lo strumento di migrazione del fornitore di servizi cloud offre un modo per eseguire la migrazione di server virtualizzati locali nel cloud?* • *Se sì, quali ambienti virtualizzati sono attualmente supportati?*
8.	***MIGRAZIONI - INDIVIDUAZIONE DEI SERVER:***

	Lo strumento di migrazione del fornitore di servizi cloud offre una funzionalità di individuazione per il rilevamento automatico dei server virtuali locali da migrare nel cloud?
9.	*MIGRAZIONI - DATI SULLE PRESTAZIONI DEI SERVER:* *Lo strumento di migrazione del fornitore di servizi cloud dispone della funzionalità di raccolta e visualizzazione delle prestazioni relative a server e/o macchine virtuali, come ad esempio l'utilizzo della CPU e della memoria RAM?*
10.	*MIGRAZIONI - DATABASE DI INDIVIDUAZIONE* *Lo strumento di migrazione del fornitore di servizi cloud offre la possibilità di archiviare in un database centralizzato tutti i dati raccolti?* • *Se sì, gli enti hanno la possibilità di esportare i dati? In quali formati?*
11.	*MIGRAZIONI - CRITTOGRAFIA DEI DATI INATTIVI:* *Il fornitore di servizi cloud offre un servizio di crittografia dei dati inattivi per tutte le informazioni raccolte e memorizzate nel database di individuazione?*
12.	*MIGRAZIONI - REPLICA INCREMENTALE DEI SERVER:* *Lo strumento di migrazione del fornitore di servizi cloud offre la replica incrementale automatizzata dei server attivi durante la migrazione di server o macchine virtuali per garantire che tutte le modifiche apportate a essi siano incluse nell'immagine migrata finale?* • *Se sì, qual è il tempo di esecuzione consentito per il servizio?*
13.	*MIGRAZIONI - VMWARE:* *Lo strumento di migrazione del fornitori di servizi cloud supporta migrazioni di macchine virtuali VMWare da server locali nel cloud?*
14.	*MIGRAZIONI - HYPER-V:* *Lo strumento di migrazione del fornitore di servizi cloud supporta migrazioni di macchine virtuali Hyper-V da server locali nel cloud?*
15.	*MIGRAZIONI - INDIVIDUAZIONE DELLE APPLICAZIONI:* *Lo strumento di migrazione del fornitore di servizi cloud consente l'individuazione e il raggruppamento delle applicazioni prima della migrazione?*
16.	*MIGRAZIONI - MAPPATURA DELLE DIPENDENZE:* *Lo strumento di migrazione del fornitore di servizi cloud consente l'individuazione delle dipendenze tra i server e le applicazioni prima della migrazione?*
17.	*MIGRAZIONI - MIGRAZIONE DEI DATABASE:* *Lo strumento di migrazione del fornitore di servizi cloud offre funzionalità di migrazione dei database locali nel cloud?*
18.	*MIGRAZIONI - TEMPI DI INATTIVITÀ DURANTE LA MIGRAZIONE DEI DATABASE:* *Lo strumento di migrazione del fornitore di servizi cloud offre funzionalità di migrazione dei database nel cloud che garantiscono tempi di inattività minimi, ossia che consentono al database di origine di rimanere completamente operativo durante il processo di migrazione?*
19.	*MIGRAZIONI - DATABASE DI ORIGINE:* *Lo strumento di migrazione del fornitore di servizi cloud supporta la migrazione di diverse origini di database, come ad esempio Oracle, SQL Server e così via?* • *Se sì, elencare tutti i database di diverse origini che è possibile migrare nel cloud.*
20.	*MIGRAZIONI - MIGRAZIONI ETEROGENEE:* *Lo strumento di migrazione del fornitore di servizi cloud consente di eseguire migrazioni eterogenee dei database, ad esempio da un database di origine a un diverso database di destinazione, come ad esempio da Oracle a SQL Server?*

	• *Se sì, elencare tutte le possibili combinazioni di migrazione eterogenee dei database.*
21.	***MIGRAZIONI - MIGRAZIONE DEI DATI NELL'ORDINE DI PETABYTE:*** *Il fornitore di servizi cloud offre una soluzione di trasporto dati fino a diversi petabyte che utilizza dispositivi sicuri per trasferire grandi quantità di dati da e verso il cloud?*
22.	***MIGRAZIONI - MIGRAZIONE DEI DATI NELL'ORDINE DI EXABYTE:*** *Il fornitore di servizi cloud offre una soluzione di trasporto dati fino a diversi exabyte per trasferire grandi quantità di dati nel cloud?*
23.	***MIGRAZIONI - BACKUP AZIENDALI:*** *Il fornitore di servizi cloud offre un servizio che consente una perfetta integrazione del data center del cliente con i servizi di storage nel cloud, consentendo il trasferimento e l'archiviazione dei dati nel servizio di storage del fornitore di servizi cloud?*
24.	***MIGRAZIONI - BACKUP AZIENDALI - STORAGE DI OGGETTI:*** *Il servizio di backup aziendale del fornitore di servizi cloud offre l'integrazione con il servizio di storage di oggetti nel cloud del fornitore?*
25.	***MIGRAZIONI - BACKUP AZIENDALI - ACCESSO AI FILE:*** *Il servizio di backup aziendale del fornitore di servizi cloud consente agli utenti di archiviare e recuperare oggetti utilizzando protocolli di file come il protocollo NFS (Network File System)?*
26.	***MIGRAZIONI - BACKUP AZIENDALI - ACCESSO AI BLOCCHI:*** *Il servizio di backup aziendale del fornitore di servizi cloud consente agli utenti di archiviare e recuperare oggetti utilizzando protocolli di blocco come il protocollo iSCSI (Internet Small Computer Systems Interface)?*
27.	***MIGRAZIONI - BACKUP AZIENDALI - ACCESSO AI NASTRI:*** *Il servizio di backup aziendale del fornitore di servizi cloud consente agli utenti di eseguire il backup dei dati tramite una libreria di nastri virtuali e archiviare questi backup di nastri nel cloud del fornitore?*
28.	***MIGRAZIONI - BACKUP AZIENDALI - CRITTOGRAFIA:*** *Il servizio di database aziendale del fornitore di servizi cloud offre la crittografia dei dati inattivi e in transito?*
29.	***MIGRAZIONI - BACKUP AZIENDALI - INTEGRAZIONE SOFTWARE DI TERZE PARTI:*** *Il servizio di backup aziendale del fornitore di servizi cloud si integra con il software di backup di terze parti di uso comune?*
30.	***MIGRAZIONI - RESTRIZIONI DEI SERVIZI:*** *Il fornitore di servizi cloud applica delle limitazioni (ovvero restrizioni dei servizi) relativamente alla sezione migrazioni precedente?* *Esempio:* *Numero massimo di migrazioni simultanee di macchine virtuali* *Numero massimo ordinabile di soluzioni di trasporto dei dati*

8. Fatturazione

	Requisito
1.	***FATTURAZIONE - TRACCIAMENTO E CREAZIONE DI REPORT:*** *Il fornitore di servizi cloud offre un servizio di fatturazione con tracciamento e creazione di report per consentire agli utenti di monitorare l'utilizzo delle offerte cloud attive?*

2.	***FATTURAZIONE - ALLARMI E NOTIFICHE:*** *Il fornitore di servizi cloud offre agli utenti un meccanismo per impostare gli allarmi con notifiche per avvisare gli utenti quando hanno superato una soglia di spesa specifica?*
3.	***FATTURAZIONE - GESTIONE DEI COSTI:*** *Il fornitore di servizi cloud offre un meccanismo per creare e visualizzare un grafico riepilogativo dei costi e delle spese?*
4.	***FATTURAZIONE - BUDGET:*** *Il fornitore di servizi cloud offre un meccanismo per visualizzare e gestire i budget e le previsioni dei costi stimati?*
5.	***FATTURAZIONE - VISTA CONSOLIDATA:*** *Il fornitore di servizi cloud offre un meccanismo per consolidare la fatturazione di più account in un unico account di pagamento principale?*
6.	***FATTURAZIONE - RESTRIZIONI DEI SERVIZI:*** *Il fornitore di servizi cloud applica delle limitazioni (ovvero restrizioni dei servizi) relativamente alla sezione fatturazione precedente?* *Esempio:* *Numero massimo di account che è possibile raggruppare* *Numero massimo di allarmi che è possibile creare* *Numero massimo di budget che è possibile gestire*

9. Gestione

	Requisito
1.	***GESTIONE – SERVIZIO DI MONITORAGGIO:*** *Il fornitore di servizi cloud offre un servizio di monitoraggio per la gestione delle applicazioni e delle risorse cloud, che svolge attività di raccolta, monitoraggio e creazione di report utilizzando i parametri predefiniti?*
2.	***GESTIONE - ALLARMI:*** *Il servizio di monitoraggio del fornitore di servizi cloud consente agli utenti di impostare allarmi?*
3.	***GESTIONE - PARAMETRI PERSONALIZZATI:*** *Il servizio di monitoraggio del fornitore di servizi cloud consente agli utenti di creare e impostare i parametri personalizzati?*
4.	***GESTIONE - GRANULARITÀ DEL MONITORAGGIO:*** *Il servizio di monitoraggio del fornitore di servizi cloud fornisce diversi livelli di granularità del monitoraggio, fino al livello di granularità di 1 minuto?*
5.	***GESTIONE - SERVIZIO DI TRACCIAMENTO DELL'API:*** *Il fornitore di servizi cloud offre un servizio che consente la registrazione, il monitoraggio e l'archiviazione delle attività delle risorse cloud a livello di console e di API per una maggiore visibilità?* • *Se sì, quali sono i servizi offerti dal fornitore di servizi cloud che si integrano con questo servizio di tracciamento?*
6.	***GESTIONE - NOTIFICA:*** *Il fornitore di servizi cloud offre la funzionalità di invio delle notifiche sulla base dei livelli di attività delle API?*

7.	***GESTIONE - COMPRESSIONE:*** *Il fornitore di servizi cloud offre un meccanismo di compressione dei log generati dal sistema di tracciamento dell'API per consentire agli utenti di ridurre i costi di storage associati al servizio?*
8.	***GESTIONE - AGGREGAZIONE DELLE REGIONI:*** *Il fornitore di servizi cloud consente di registrare l'attività dell'API dell'account in tutte le regioni e di distribuire le relative informazioni in maniera aggregata per un utilizzo più semplice?*
9.	***GESTIONE - INVENTARIO DELLE RISORSE:*** *Il fornitore di servizi cloud offre un servizio per la valutazione, l'audit e la verifica delle configurazioni delle risorse distribuite da un utente?*
10.	***GESTIONE - MODIFICHE DI CONFIGURAZIONE:*** *Il fornitore di servizi cloud registra in modo automatico le modifiche di configurazione delle risorse quando vengono effettuate?*
11.	***GESTIONE - CRONOLOGIA DI CONFIGURAZIONE:*** *Il fornitore di servizi cloud offre la possibilità di esaminare la configurazione passata delle risorse in qualsiasi sua fase?*
12.	***GESTIONE - REGOLE DI CONFIGURAZIONE:*** *Il fornitore di servizi cloud offre linee guida e raccomandazioni per il provisioning, la configurazione e il monitoraggio continuo della conformità?*
13.	***GESTIONE - MODELLI DI RISORSE:*** *Il fornitore di servizi cloud offre agli utenti funzionalità di creazione, provisioning e gestione di una raccolta di risorse sulla base di un modello?*
14.	***GESTIONE - REPLICA DEI MODELLI DI RISORSE:*** *Il fornitore di servizi cloud offre la possibilità di replicare in modo semplice questi modelli di risorse in regioni diverse per il potenziale utilizzo in un ripristino di emergenza?*
15.	***GESTIONE - STRUMENTO DI PROGETTAZIONE DEI MODELLI:*** *Il fornitore di servizi cloud offre uno strumento grafico semplice da usare con funzionalità di trascinamento della selezione per accelerare il processo di creazione di modelli di risorse?*
16.	***GESTIONE - CATALOGO DEI SERVIZI:*** *Il fornitore di servizi cloud offre un servizio per la creazione e la gestione di un catalogo dei servizi, ovvero server, macchine virtuali, software, database e così via?*
17.	***GESTIONE - ACCESSO ALLA CONSOLE:*** *Il fornitore di servizi cloud offre un'interfaccia utente basata sul web per facilitare la gestione e il monitoraggio dei servizi cloud?*
18.	***GESTIONE - ACCESSO CLI:*** *Il fornitore di servizi cloud offre uno strumento unificato per gestire e configurare più servizi cloud dall'interfaccia a riga di comando (CLI), nonché per automatizzare le attività di gestione mediante l'uso di script?*
19.	***GESTIONE - ACCESSO DAI DISPOSITIVI MOBILI:*** *Il fornitore di servizi cloud offre un'applicazione per smartphone da cui gli utenti possono connettersi al servizio cloud e gestire le proprie risorse?* • *Se sì, questa applicazione è disponibile sia per iOS che per Android?*
20.	***GESTIONE - BEST PRACTICE:*** *Il fornitore di servizi cloud offre un servizio che consente agli utenti di valutare l'utilizzo del cloud rispetto alle best practice?*

21.	***GESTIONE - RESTRIZIONI DEI SERVIZI:*** *Il fornitore di servizi cloud applica delle limitazioni (ovvero restrizioni dei servizi) relativamente alla sezione gestione precedente?* *Esempio:* *Numero massimo di regole di configurazione per account* *Numero massimo di allarmi che è possibile creare* *Numero massimo di log che è possibile archiviare*

10. Supporto

	Requisito
1.	***SUPPORTO - ASSISTENZA:*** *Il fornitore di servizi cloud offre supporto continuativo, 24 ore al giorno, 7 giorni a settimana, 365 giorni all'anno via email, telefono e chat?*
2.	***SUPPORTO - LIVELLI DI SUPPORTO:*** *Il fornitore di servizi cloud offre diversi livelli di supporto?*
3.	***SUPPORTO - ALLOCAZIONE DEI LIVELLI:*** *Il fornitore di servizi cloud consente agli utenti di assegnare in autonomia a diversi livelli di supporto le risorse/i servizi utilizzati in funzione di una classificazione granulare, senza costringerli a gestire account cloud separati per usufruire di livelli diversi di supporto?*
4.	***SUPPORTO - FORUM:*** *Il fornitore di servizi cloud offre ai clienti forum di supporto pubblici dove discutere dei problemi?*
5.	***SUPPORTO - PANNELLO DI CONTROLLO STATO SERVIZI:*** *Il fornitore di servizi cloud offre un pannello di controllo stato servizi con le informazioni più aggiornate sulla disponibilità del servizio in più regioni?*
6.	***SUPPORTO - PANNELLO DI CONTROLLO PERSONALIZZATO:*** *Il fornitore di servizi cloud offre un pannello di controllo che mostra in modo personalizzato la situazione delle prestazioni e la disponibilità dei servizi evidenziando le risorse specifiche dell'utente?*
7.	***SUPPORTO - CRONOLOGIA DEL PANNELLO DI CONTROLLO:*** *Il fornitore di servizi cloud offre una cronologia di 365 giorni per la cronologia del pannello di controllo stato servizi?*
8.	***SUPPORTO - CONSULENTE CLOUD:*** *Il fornitore di servizi cloud offre un servizio che svolge le funzioni di un esperto di cloud personalizzato e aiuta a valutare l'utilizzo delle risorse rispetto alle best practice?*
9.	***SUPPORTO - TAM:*** *Il fornitore di servizi cloud offre un Technical Account Manager (TAM) che fornisce consulenza tecnica per l'intera gamma dei servizi cloud?*
10.	***SUPPORTO - SUPPORTO PER APPLICAZIONI DI TERZE PARTI:*** *Il fornitore di servizi cloud offre supporto per i sistemi operativi più diffusi e i componenti di stack di applicazioni comuni?*
11.	***SUPPORTO - API PUBBLICA:***

	Il fornitore di servizi cloud offre un'API pubblica per l'interazione programmatica con i casi di supporto per creare, modificare e chiudere tali casi?
12.	*SUPPORTO - DOCUMENTAZIONE DEI SERVIZI:* *Il fornitore di servizi cloud offre documentazioni tecniche di buona qualità e consultabili pubblicamente per tutti i suoi servizi, comprese, a titolo illustrativo ma non esaustivo, guide per l'utente, tutorial, domande frequenti e note di rilascio?*
13.	*SUPPORTO - DOCUMENTAZIONE CLI:* *Il fornitore di servizi cloud offre documentazioni tecniche di buona qualità e consultabili pubblicamente per l'interfaccia a riga di comando (CLI)?*
14.	*SUPPORTO - ARCHITETTURE DI RIFERIMENTO:* *Il fornitore di servizi cloud offre una raccolta online gratuita di documenti sull'architettura di riferimento, che siano utili ai clienti per costruire soluzioni specifiche in grado di coniugare molti dei servizi cloud offerti dal fornitore?*
15.	*SUPPORTO - DISTRIBUZIONI DI RIFERIMENTO:* *Il fornitore di servizi cloud offre una raccolta online gratuita di documenti contenenti procedure guidate dettagliate, testate e convalidate, comprensive di best practice, per l'implementazione di soluzioni comuni (ovvero DevOps, Big Data, data warehouse, carichi di lavoro Microsoft, carichi di lavoro SAP e così via) nelle sue offerte cloud?*

Appendice B - Demo

Le demo possono essere un metodo efficace con cui gli utenti finali possono testare le offerte di servizi cloud e con cui viene decisa l'aggiudicazione in base all'offerta più idonea per le esigenze commerciali dell'ente. Di seguito è riportato un test dimostrativo di esempio per le tecnologie cloud.

1. *Dimostrare, ad alto livello, la console del CISP e le offerte/risorse disponibili pubblicamente:*
    - *Funzionalità di storage*
    - *Funzionalità di calcolo*
    - *Funzionalità e tipi di database*
    - *Reti*
    - *Strumenti gestionali e analitici*
    - *Sicurezza*
    - *Altre funzionalità*
2. *Descrivere come operano le tecnologie cloud utilizzate nella demo.*
3. *Dimostrare come viene eseguita questa demo in tempo reale utilizzando l'offerta di servizi cloud.*
4. *Account:*
    - *Descrivere il sistema delle chiavi degli account (root e utente) usato nella demo.*
    - *Dimostrare come sono gestite e protette le chiavi degli account.*
5. *Dimostrare come selezionare la posizione fisica in cui sono archiviati dati/carichi di lavoro.*
6. *Dimostrare la scala delle offerte impostando soluzioni di calcolo e di storage su larga scala.*
7. *Illustrare come un utente finale richiede vari servizi tra le offerte di servizi cloud. Dimostrare:*
    - *Come configurare gli account*
    - *Come attivare le disposizioni in materia di sicurezza*
    - *Come suddividere gli account principali in account secondari*
    - *Come separare l'accesso alle varie risorse tramite IAM (Identity and Access Management)*
        - *Come proteggere un account*
        - *Creare utenti e gruppi*
        - *Allegare le policy*
        - *Impostare le password*
8. *Dimostrare in che modo gli ambienti virtuali possono essere isolati dal punto di vista della sicurezza e delle reti:*
    - *Creare le subnet*
    - *Routing su Internet*
9. *Dimostrare in che modo è possibile creare un ambiente in due o più ubicazioni isolate.*
    - *Dimostrare il bilanciamento del carico tra gli ambienti.*
10. *Dimostrare la capacità di utilizzare più metodi per interagire con i servizi di cloud computing (ad es., Application Program Interface (API), console web, riga di comando).*
11. *Storage:*
    - *Descrivere le opzioni di storage*
    - *Dimostrare i tipi di storage disponibili (ad es. blocco, oggetto) e i processi del ciclo di vita dei dati*
    - *Impostare un volume di storage e dimostrare in che modo i dati vengono caricati e recuperati*
    - *Creare un volume di storage XGB con e senza un'opzione di calcolo*
    - *Dimostrare e convalidare i permessi per accedere a questi volumi.*
12. *Calcolo:*
    - *Descrivere le opzioni di calcolo: dimensioni e funzionalità delle risorse di calcolo*
    - *Dimostrare l'attivazione e disattivazione di una risorsa di calcolo*

- *Dimostrare le proprietà (capacità di avviare X istanze contemporaneamente, selezione della rete, protezione da interruzioni accidentali, tenancy ecc.)*
- *Dimostrare un'opzione di calcolo con l'equivalente di X core e X GB di RAM*
- *Dimostrare il dimensionamento basato sul carico mediante l'esecuzione di un carico di lavoro*
- *Dimostrare le funzionalità di dimensionamento automatico*
- *Dimostrare come è possibile interrompere e riavviare successivamente il calcolo*
- *Dimostrare come è possibile ridimensionare un'opzione di calcolo e gestire le configurazioni*
- *Dimostrare come è possibile copiare un'opzione di calcolo*
- *Dimostrare come configurare i gruppi di sicurezza*
- *Descrivere quali sistemi operativi sono disponibili nell'offerta dei CISP*
- *Dimostrare un esempio di installazione di sistema operativo Linux*
- *Descrivere la propria capacità di fornire immagini per le offerte di calcolo*
- *Quali sono i formati immagine supportati?*
- *Dimostrare in che modo viene caricata e utilizzata un'immagine*
- *Dimostrare il Serverless Computing*
- *Dimostrare la capacità di avviare un cluster di istanze di calcolo con prezzi diversificati basati sul mercato a pronti*

13. *Database:*
    - *Descrivere le funzionalità del database*
    - *Dimostrare le funzionalità MySQL, MS SQL Server, Oracle e Postgres*
    - *Dimostrare tutte le funzionalità di Data Warehousing*
    - *Dimostrare le funzionalità di backup delle risorse*
14. *Reti: dimostrare le opzioni di rete definite a livello di software e le funzionalità di gestione delle reti*
15. *Gestione e analisi*
    - *Descrivere le funzionalità di gestione e analisi dei servizi cloud*
    - *Dimostrare le opzioni di monitoraggio*
    - *Dimostrare le proprie capacità con i framework Hadoop*
16. *Sicurezza: dimostrare la sicurezza della rete*
    - *Descrivere il proprio approccio alla sicurezza*
    - *Firewall*
    - *Gruppi di sicurezza*
    - *Gateway*
    - *Liste di controllo degli accessi di rete (NACL)*
    - *Registri di sistema*
    - *Crittografia*
    - *Accreditamenti di conformità disponibili*
    - *Storage delle chiavi*
    - *Altre caratteristiche*
17. *Provisioning: dimostrare in che modo è possibile creare una raccolta di risorse cloud correlate e provvedere alla loro fornitura in modo ordinato e prevedibile tramite un modello riutilizzabile*
18. *Software: dimostrare la propria capacità di permettere l'accesso e l'utilizzo delle applicazioni software comunemente utilizzate*
19. *Dimostrare in che modo è possibile eseguire un trasferimento dei dati su larga scala*
20. *Dimostrare le opzioni di fatturazione, tra cui:*
    - *Vista di riepilogo, vista granulare, vista per risorse con tag*
    - *Previsione di spesa/utilizzo sulla base della spesa/utilizzo corrente*
21. *Dimostrare le funzionalità di supporto e consulenza disponibili*
    - *Quali opzioni di supporto sono disponibili?*

- *Sono previste funzionalità di controllo e consulenza sull'utilizzo del servizio?*

Dimostrare qualsiasi altra caratteristica dell'offerta ritenuta determinante