CIPA | Convenzione Interbancaria per l'Automazione

ABI Associazione Bancaria Italiana

Rilevazione sull'IT nel settore bancario italiano

Profili tecnologici e di sicurezza

Il cloud computing e le banche

Questionario

2022

Sommario

Premessa

La “Rilevazione sull’IT nel settore bancario italiano”, curata annualmente da CIPA e ABI, ha l’obiettivo di fornire una visione d’insieme dell’utilizzo dell’Information and Communication Technology nelle banche, analizzandone i diversi aspetti organizzativi, economici, tecnologici e di sicurezza.

La Rilevazione si articola in due distinte indagini: la prima è dedicata all’esame dei profili economici e organizzativi dell’IT; la seconda, cui si riferisce il presente questionario, è riservata ai profili tecnologici e di sicurezza ed è centrata di volta in volta su uno specifico argomento.

L’indagine, dedicata in questa edizione a **“Il cloud computing e le banche”**, analizza i principali aspetti strategici, organizzativi e tecnologici connessi con l’adozione e la migrazione degli assetti infrastrutturali e applicativi al cloud.

Il fenomeno della migrazione dei sistemi informatici delle aziende bancarie verso questo nuovo paradigma è in costante aumento in relazione a molteplici fattori tra cui, in particolare, l’esigenza di maggiore flessibilità e scalabilità delle architetture e il ricorso a nuove metodologie di sviluppo delle applicazioni.

I risultati delle analisi vengono illustrati in un rapporto pubblicato sui siti internet della CIPA (www.cipa.it) e dell’ABI (www.abi.it).

Le informazioni, raccolte da CIPA e ABI e fornite su base volontaria, sono utilizzate esclusivamente ai fini dell’indagine e diffuse all’esterno soltanto in forma aggregata o anonima. Il trattamento dei dati si svolge, senza intervento di terze parti, con modalità atte a garantirne la sicurezza e la riservatezza.

Glossario

Con l'obiettivo di utilizzare una terminologia comune sulle tematiche del cloud, si riportano di seguito le definizioni principali adottate nel questionario, tratte da "Orientamenti in materia di esternalizzazione dell'EBA"[1].

Cloud computing

Modello computazionale che consente l'accesso in rete diffuso, conveniente e su richiesta dell'utente a un gruppo condiviso di risorse elettroniche configurabili (es. reti, server, memorie, applicazioni e servizi), che possono essere messe a disposizione rapidamente con un minimo impegno gestionale o con interazione con il fornitore.

Deployment model

Cloud pubblico: infrastruttura cloud disponibile per l'utilizzo da parte della generalità degli utenti. Tipicamente dislocata presso un cloud provider.

Cloud privato: infrastruttura cloud disponibile per l'utilizzo esclusivo da parte di un solo soggetto. Può essere gestita dall'organizzazione stessa o da un fornitore; può essere all'interno delle strutture dell'organizzazione stessa (on-premises) o presso il fornitore (off-premises).

Community Cloud: infrastruttura cloud disponibile per l'utilizzo esclusivo da parte di una specifica comunità di enti, compresa una pluralità di enti appartenenti a un unico gruppo. Può essere gestita dalle stesse organizzazioni o da terzi e può essere on-premises o off-premises.

Hybrid Cloud: infrastruttura cloud composta da due o più infrastrutture cloud distinte.

Service model

I servizi di cloud computing si distinguono in tre modelli, a seconda di quanta parte dello stack tecnologico è offerta e controllata dal fornitore (es. la sola infrastruttura, i servizi di piattaforma software di base, l'intero software, altri componenti o combinazioni): "IaaS (Infrastructure as a Service)", "PaaS (Platform as a Service)" e "Saas (Software as a Service)".

In particolare:

Infrastructure as a Service (IaaS*):* il provider fornisce le risorse elaborative infrastrutturali (capacità elaborativa, storage, networking, difese perimetrali e sistemi di gestione della sicurezza). Il cliente può installare ed eseguire software in autonomia, mantenendo il controllo dello *storage*, delle applicazioni e, nella generalità dei casi, dei sistemi operativi; relativamente all'infrastruttura sottostante può avere un limitato controllo delle componenti di rete.

[1] https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2761380/1c9aaefc-e10d-45a6-8a51-1fb450814a29/EBA revised Guidelines on outsourcing_IT.pdf?retry=1

Platform as a Service (PaaS): il provider offre l'ambiente necessario (piattaforme elaborative, linguaggi di programmazione - API, ambienti di sviluppo e testing, tools e librerie) per lo sviluppo e il deploy di applicazioni del cliente o di una terza parte.

Software as a Service (SaaS): il cliente utilizza i servizi forniti dal provider intesi come applicazioni software che possono essere utilizzate su richiesta. L'infrastruttura rimane sotto il pieno controllo del provider.

Cloud Service Provider (CSP): fornitore di servizi in cloud.

Dati del compilatore e della struttura

Dati identificativi della Banca

Codice ABI[2]	☐☐☐☐☐
Ragione sociale	

Struttura organizzativa che cura la compilazione del questionario

Denominazione[3]			
Indirizzo[4]			
Città		CAP	☐☐☐☐☐
Prov.			
E-mail[5]			

Dati del compilatore[6]

Cognome	
Nome	
Telefono	
E-mail	

[2] Cinque cifre senza CIN di controllo.
[3] Inserire la denominazione aziendale della struttura.
[4] Inserire il recapito aziendale con tutti i dati richiesti, al fine di poter recapitare lettere o plichi.
[5] Casella funzionale (non legata a una persona fisica) di posta elettronica della struttura o, in sua mancanza, indirizzo di posta elettronica di un referente della struttura.
[6] Inserire i recapiti aziendali, compreso l'indirizzo di posta elettronica, per richieste di informazioni e chiarimenti o segnalazioni di anomalie nella compilazione.

1 Strategia di adozione

1.1 Con riferimento alla strategia aziendale, il ricorso al cloud computing è tra le priorità di investimento della banca/gruppo?

	Risposta
1. È tra le prime 10 priorità di investimento 2. È una priorità non tra le prime 10 3. È secondario rispetto ad altre priorità 4. Non sono previsti investimenti sul cloud	☐

1.2 Con riferimento alla strategia di cloud computing, indicare l'approccio prevalente.

	Al 2022	2023-2025
Cloud Only		
Cloud First		
Cloud First ad eccezione di servizi/sistemi di "core banking" o che richiedono bassa latenza		
Approccio tattico su ambiti selezionati	☐	☐
Adozione del cloud non in logica Cloud First (ad hoc)		
Non vi è ricorso al cloud		
Altro, specificare:		

1.3 Indicare quali service model sono adottati dalla banca/gruppo, specificandone il deployment model prevalente.

Service model	Cloud pubblico	Cloud privato[7]	Altri modelli[8]
SaaS per servizi di "core banking"	☐	☐	☐
SaaS per gli altri servizi	☐	☐	☐
IaaS/PaaS per infrastrutture critiche	☐	☐	☐
IaaS/PaaS per infrastrutture non critiche	☐	☐	☐
Altro, specificare:	☐	☐	☐

[7] Nel cloud privato considerare anche eventuali cloud di community della banca/gruppo bancario.
[8] In presenza di cloud ibrido, valorizzare pubblico o privato a seconda della prevalenza. Laddove ciò non fosse possibile valorizzare la colonna 'Altri modelli'.

1.4 **Indicare quali service model saranno adottati in previsione dalla banca/gruppo nel 2023-2025, specificandone il deployment model prevalente.**

Service model	Cloud pubblico	Cloud privato	Altri modelli
SaaS per servizi di "core banking"	☐	☐	☐
SaaS per gli altri servizi	☐	☐	☐
IaaS/PaaS per infrastrutture critiche	☐	☐	☐
IaaS/PaaS per infrastrutture non critiche	☐	☐	☐
Altro, specificare:	☐	☐	☐

1.5 **Indicare se la strategia di ricorso al cloud IaaS/PaaS si concentra in maniera prevalente su un unico CSP (Cloud Service Provider) o ne prevede più di uno.**

	Al 2022	2023-2025
1. Multicloud "platform based" con integrazione		
2. Multicloud senza integrazione		
3. Unico CSP	☐	☐
4. Non vi è ricorso al cloud IaaS/PaaS		
5. Altro, specificare:		

1.6 Assegnare un livello di importanza ai requisiti in elenco presi in considerazione nella selezione di un nuovo CSP.

Livello: da 0 (min) a 5 (max)

Requisiti	Livello
Solidità dell'azienda (dimensione, presenza sul mercato, anni di operatività)	☐
Esperienza nel settore e maturità delle soluzioni offerte	☐
Azienda già utilizzata dalla banca/gruppo come system solution/integrator	☐
CSP operante in Italia (localizzazione dei dati in Italia)	☐
Trasparenza delle policy e dei contratti (anche relativamente a eventuali sub-fornitori)	☐
Chiarezza delle policy e dei contratti per l'attribuzione delle responsabilità	☐
Possibilità di negoziare clausole contrattuali ad hoc	☐
Adozione di certificazioni e best practice riconosciute a livello internazionale	☐
Solidità e sicurezza dei meccanismi di incident, problem, change management	☐
Attenzione agli aspetti di sostenibilità ambientale (Green IT, carbon neutral)	☐
Garanzie aggiuntive offerte per la tutela della privacy e della sicurezza dei dati	☐
Offerta di soluzioni technology neutral (open)	☐
Rilascio di funzionalità aggiuntive per il monitoraggio (di sicurezza, dei costi, etc.)	☐
Garanzie sulla disponibilità e visibilità dei dati	☐
Integrabilità delle soluzioni offerte con l'architettura IT aziendale anche in termini di monitoraggio	☐
Integrabilità delle soluzioni offerte con quelle di altri cloud provider anche in termini di monitoraggio	☐
Offerta di strumenti per la migrazione dei dati	☐
Attenzione a exit strategy	☐
Convenienza economica rispetto a soluzioni "tradizionali"	☐
Trasparenza nella determinazione dei costi	☐
Scalabilità (rispetto a volumi, servizi, etc.)	☐
Rapidità di deployment dei servizi	☐
Possibilità di effettuare audit da parte della banca/gruppo	☐
Altro, specificare:	☐

1.7 **Indicare il percorso di cloud transformation intrapreso dalla banca/gruppo ordinando temporalmente, tutte o solamente alcune, le seguenti fasi in elenco.**

1=prima, …, n=ultima/fase corrente

Fasi	Ordinamento
Definizione di una strategia per il cloud pubblico/privato	☐
Definizione di policy per il cloud pubblico/privato	☐
Creazione di centro/i di competenza per il cloud	☐
Sperimentazione di un cloud privato Iaas/PaaS	☐
Adozione di cloud privato Iaas/PaaS	☐
Porting di servizi su cloud privato (SaaS)	☐
Adozione di IaaS/PaaS in cloud pubblico	☐
Migrazione di servizi interni in cloud pubblico (SaaS)	☐
Acquisizione di servizi in cloud pubblico (SaaS)	☐
Altro, specificare:	☐

1.8 **Indicare se una componente della banca/gruppo si pone come fornitore di servizi cloud e, in caso affermativo, specificare la tipologia di enti a cui si rivolge l'offerta.**

1. Sì, solo ad altre banche o altri gruppi bancari[9]
2. Sì, solo ad aziende non bancarie
3. Sì, a entrambe le tipologie di enti
4. No

Ambito IT	Italia	Estero
IaaS/PaaS	☐	☐
Servizi di pagamento (SaaS)	☐	☐
Credito (SaaS)	☐	☐
Servizi finanziari e di investimento (SaaS)	☐	☐
Servizi in ambito Cyber Security (SaaS)	☐	☐
Servizi SaaS in ambito innovativo (AI&ML, blockchain, IoT, analytics, quantum computing, etc.)	☐	☐
Servizi di Continuous Development/Integration	☐	☐
Altro, specificare:	☐	☐

[9] In tale fattispecie rientra anche il caso di fornitura di servizi IT a componenti del gruppo estere.

1.9 **Se la strategia della banca/gruppo prevede partnership con CSP per fornire servizi cloud, indicarne la tipologia.**

1. Hyperscaler (Amazon, Google, etc.)
2. Altri CSP europei/internazionali
3. Altri CSP nazionali

	Risposta
Partnership già attiva per "core banking" (SaaS)	☐
Partnership già attiva per altri servizi (SaaS)	☐
Partnership già attiva IaaS/PaaS	☐
Partnership prevista entro il 2025	☐
Altro specificare:	☐

1.10 **Con riferimento all'adozione/evoluzione del cloud computing, indicare i benefici <u>attesi</u> e, nel caso di iniziative in corso o completate, quelli <u>riscontrati</u>, specificandone il livello di rilevanza.**

Livello: da 0 (min) a 5 (max)

Benefici	Attesi	Riscontrati
– Flessibilità di utilizzo (capacità elaborativa on-demand, modalità pay per use, possibilità di adozione graduale)	☐	☐
– Riduzione dei costi	☐	☐
– Scalabilità	☐	☐
– Rapidità di implementazione di soluzioni innovative	☐	☐
– Rapidità di allestimento di ambienti di test/sperimentazione	☐	☐
– Facilità di adeguamento al contesto tecnologico e/o standard	☐	☐
– Facilità di adeguamento al contesto normativo	☐	☐
– Maggiore integrazione dei servizi informatici	☐	☐
– Maggior controllo della spesa (da CAPEX a OPEX)	☐	☐
– Indipendenza dall'obsolescenza tecnologica	☐	☐
– Riduzione del time-to-market	☐	☐
– Opportunità di focalizzare gli investimenti e le risorse nel core business	☐	☐
– Miglioramento della Sicurezza IT	☐	☐
– Accesso a servizi "best of breed"	☐	☐
– Supporto alla Digital Transformation	☐	☐
– Riduzione della complessità dell'architettura IT	☐	☐
– Migliore governance nei servizi IT	☐	☐
– Gestione tempestiva delle emergenze	☐	☐
– Sostenibilità ambientale	☐	☐
– Altro, specificare:	☐	☐

1.11 **Con riferimento all'adozione/evoluzione del cloud computing, indicare le criticità attese e, nel caso di iniziative in corso o completate, quelle riscontrate, specificandone il livello di rilevanza.**

Livello: da 0 (min) a 5 (max)

Criticità	Attese	Riscontrate
– Controllo sui dati (es. collocazione geografica o utilizzo dei dati per altri fini)	☐	☐
– Controllo sull'architettura IT aziendale e/o sui processi di gestione (es. change management)	☐	☐
– Controllo della spesa e dei costi	☐	☐
– Controllo e gestione dei servizi	☐	☐
– Previsione della spesa	☐	☐
– Salvaguardia degli investimenti	☐	☐
– Integrazione con i servizi informatici aziendali	☐	☐
– Personalizzazione dei servizi informatici	☐	☐
– Garanzia di sicurezza IT	☐	☐
– Incertezza del quadro normativo	☐	☐
– Aderenza ai requisiti di compliance	☐	☐
– Aderenza alla normativa sulla privacy	☐	☐
– Scelta di fornitori affidabili	☐	☐
– Definizione di contratti e relativi SLA	☐	☐
– Limitato potere negoziale nei confronti del fornitore	☐	☐
– Rischio di vendor lock-in	☐	☐
– Elevati oneri di gestione dei servizi in cloud (monitoraggio SLA e auditing sulle procedure)	☐	☐
– Scarsa disponibilità di competenze interne	☐	☐
– Altro, specificare:	☐	☐

2 Organizzazione, competenze, ambiti di utilizzo

2.1 **Con riferimento al budget IT previsto per il 2023, indicare la quota percentuale totale per il cloud pubblico e le quote SaaS e IaaS/PaaS.**

Totale cloud pubblico SaaS/IaaS/PaaS (% del budget IT)	☐☐,☐%
SaaS in cloud pubblico (% del budget IT)	☐☐,☐%
IaaS/PaaS in cloud pubblico (% del budget IT)	☐☐,☐%

2.2 **Indicare la quota percentuale del budget IT prevista per il 2023 dedicata alla modernizzazione/evoluzione delle applicazioni in ottica cloud e alla migrazione al cloud.**

Modernizzazione/evoluzione applicazioni per il cloud (refactoring, container, microservizi, etc.)	☐☐,☐ %
Migrazione al cloud (spostamento workload, lift&shift, integrazione, attivazione SaaS, etc.)	☐☐,☐ %

2.3 **Con riferimento alla strategia e alla governance per il cloud, indicare quali interventi di tipo organizzativo sono stati effettuati al 2022 e quali, in prospettiva, lo saranno nel 2023-2025.**

	Al 2022	**2023-2025**
Definizione policy per la Cloud Governance	☐	☐
Formalizzazione di una Cloud Strategy (obiettivi, etc.)	☐	☐
Revisione del Security framework (aggiornamento mappa dei rischi e dei controlli, shared responsability, etc.)	☐	☐
Definizione di un modello organizzativo e operativo per il cloud (definizione di interazioni tra stakeholder e IT, unità costi, etc.)	☐	☐
Definizione di una exit strategy complessiva per il cloud	☐	☐
Altro, specificare:	☐	☐

2.4 Con riferimento al governo dei costi per il cloud, indicare quali interventi sono stati attuati al 2022 e quali, in prospettiva, lo saranno nel 2023-2025.

	Al 2022	2023-2025
Adeguamento dei modelli di budgeting e forecasting per il cloud	☐	☐
Adeguamento nel consuntivo della spesa (Opex vs Capex)	☐	☐
Adeguamento del processo di Procurement per il cloud	☐	☐
Definizione di un modello di gestione dei costi per il cloud (es. FINOps)	☐	☐
Adeguamento della metodologia di analisi costi/benefici per il cloud (TCO e ROI)	☐	☐
Nessun intervento sul modello dei costi	☐	☐
Altro, specificare:	☐	☐

2.5 Con riferimento agli skill in ambito cloud, indicare quali interventi sono stati effettuati al 2022 e quali, in prospettiva, lo saranno nel 2023-2025.

	Al 2022	2023-2025
Piano di formazione per il cloud, anche con certificazioni specifiche	☐	☐
Creazione di una knowledge base per il cloud (best practice, etc.)	☐	☐
Promozione di "Laboratori" di supporto alle iniziative cloud	☐	☐
Assunzione di personale con competenze su tematiche cloud	☐	☐
Sviluppo interno di competenze per il cloud (Cloud Architect, Cloud Engineer, etc.)	☐	☐
Altro, specificare:	☐	☐

2.6 Indicare se è stato creato o è previsto nel 2023-2025 uno specifico "polo" di competenza per il cloud.

	Al 2022	2023-2025
1. Sì, con modello "accentrato"[10] 2. Sì, con modello "hub&spoke"[11] 3. Sì, con modello "distribuito"[12] 4. No	☐	☐

[10] Una struttura organizzativa formalizzata e accentrata che agisce come centro di competenza per il cloud.

[11] Esiste una struttura organizzativa formalizzata accentrata che agisce come "cabina di regia" e collabora con team competenti sul cloud, distribuiti in diverse funzioni aziendali.

[12] Le competenze sul cloud sono distribuite all'interno delle diverse funzioni aziendali.

2.7 Nel caso sia stato creato o sia previsto il "polo" di competenza di tipo accentrato o hub&spoke, indicare la funzione organizzativa nel quale è collocato il centro di competenza o la cabina di regia.

	Risposta
1. Funzione Organizzazione	
2. Funzione di Governance Aziendale	
3. Funzione di Governance IT	
4. Funzione IT – Sviluppo applicativo	☐
5. Funzione IT – Gestione operativa	
6. Funzione IT – Altro	
7. Altro, specificare:	

2.8 Indicare gli skill presenti nel "polo" di competenze per il cloud.

Sviluppo IT	☐
Architetture IT	☐
Gestione IT	☐
Sicurezza IT	☐
Dati	☐
Gestione contratti/procurement	☐
Legale	☐
Business	☐
Competenze ESG (Environmental, Social, Governance)	☐
Altro, specificare:	☐

2.9 Con riferimento al modello SaaS, indicare il grado di autonomia delle unità di business nell'adozione di soluzioni cloud.

	Risposta
1. Completa autonomia, nell'ambito di linee guida aziendali organizzative/architetturali (anche per la redazione dei contratti, etc.)	
2. Devono essere coinvolte le funzioni aziendali non IT (organizzazione, funzione legale, etc.)	
3. Devono essere coinvolte le funzioni IT (architetture IT, sicurezza IT, etc.)	☐
4. Devono essere coinvolte sia le funzioni IT che le altre funzioni aziendali (organizzazione, funzione legale, architetture IT, sicurezza, etc.)	
5. Nessuna autonomia	

2.10 Con riferimeno ai processi della tassonomia ABI Lab, indicare quali si avvalgono del cloud specificandone il livello di adozione e, con un criterio di prevalenza, il modello.

Livello: da 0 (no cloud) a 5 (max)

Modello prevalente
1=SaaS pubblico
2=IaaS/PaaS pubblico
3=SaaS/IaaS/PaaS privato
4=Altri modelli

Area funzionale	Processo	Livello	Modello
A Processi di governo	Pianificazione strategica	☐	☐
	Allocazione risorse e definizione del budget	☐	☐
	Controllo di gestione	☐	☐
	Gestione rischio e determinazione patrimonio vigilanza	☐	☐
	Processo di audit	☐	☐
	Gestione della compliance	☐	☐
	Relazioni esterne	☐	☐
	Comunicazione interna	☐	☐
B Processi di supporto	Organizzazione	☐	☐
	Gestione sicurezza	☐	☐
	Risorse umane	☐	☐
	Amministrazione	☐	☐
	Gestione tesoreria aziendale	☐	☐
	Supporto e consulenza legale e tributaria	☐	☐
	Gestione organi sociali e partecipazioni	☐	☐
	Supporto logistico e tecnico	☐	☐
	Gestione contante e valori	☐	☐
C Processi di Operations	Servizi bancari tipici	☐	☐
	Servizi accessori	☐	☐
	Credito	☐	☐
	Finanza	☐	☐
	Incassi e pagamenti	☐	☐
D Processi di marketing, commerciali e customer service	Sviluppo e gestione piano di marketing	☐	☐
	Gestione portafoglio prodotti	☐	☐
	Gestione canali di contatto con la clientela	☐	☐
	Pianificazione e sviluppo commerciale	☐	☐
	Customer service	☐	☐

2.11 Con riferimento agli ambiti/servizi IT elencati, indicare quali si avvalgono del cloud specificandone il livello di adozione e, con un criterio di prevalenza, il modello.

Livello: da 0 (no cloud) a 5 (max)

Modello prevalente
1=SaaS pubblico
2=IaaS/PaaS pubblico
3=SaaS/IaaS/PaaS privato
4=Altri modelli

Ambito/servizio	Livello	Modello
IT Governance	☐	☐
Progettazione, sviluppo e test IT (piattaforme di sviluppo, etc.)	☐	☐
Database	☐	☐
Sistemi operativi e middleware	☐	☐
Servizi di monitoraggio	☐	☐
Help desk IT	☐	☐
Sicurezza IT (identity, difese perimetrali, escluso penetration test)	☐	☐
Penetration test	☐	☐
Servizi di continuità (backup, DR, etc.)	☐	☐
AI e Machine Learning	☐	☐
Data Science, Data Analytics, Business Intelligence	☐	☐
Blockchain e DLT	☐	☐
IoT	☐	☐
Posta elettronica, UC & Collaboration	☐	☐
Portali Web	☐	☐
Social aziendale	☐	☐
Servizi di mobile banking e internet banking	☐	☐
Servizi in area aziendale (ERP, HR, CRM, etc.)	☐	☐
Altro, specificare:	☐	☐

3 Assetti tecnologici, sicurezza e contratti

3.1 Con riferimento agli assetti tecnologici, indicare se sono stati effettuati alcuni degli interventi di seguito elencati al 2022 e in prospettiva nel 2023-2025.

Interventi	Al 2022	2023-2025
Adeguamento dell'architettura IT per supporto/integrazione con il cloud	☐	☐
Adeguamento dell'architettura dati per il cloud	☐	☐
Automatizzazione del rilascio delle applicazioni (Continuous Delivery)	☐	☐
Utilizzo di una Infrastructure as a Code[13]	☐	☐
Adeguamento dei presidi di Cyber Security per il cloud	☐	☐
Definizione di un'architettura di Landing zone[14] per IaaS/PaaS	☐	☐
SASE architecure[15]	☐	☐
Adozione di un CASB (Cloud Access Security Broker)[16]	☐	☐
Uso di ZTNA (Zero Trust Network Access)	☐	☐
Uso di IGA[17] (Identity Governance Administration)	☐	☐
Definizione di metriche e tecniche per il monitoraggio dei carichi operativi	☐	☐
Integrazione nel monitoraggio IT aziendale del monitoraggio offerto dai CSP	☐	☐

[13] "Infrastructure as Code" (IaC): approccio alla gestione e al provisioning dell'infrastruttura tramite codice anziché con processi manuali.
[14] Landing Zone: insieme di configurazioni, template, automatismi e appliance per gestire in modo centralizzato la governance dei servizi in cloud (creazione, configurazione di ambienti multi-account, monitoring, logging, auditing e gestione delle policy di sicurezza).
[15] Secure Access Service Edge - nell'architettura SASE la gestione delle reti e sicurezza convergono in un unico servizio cloud globale.
[16] CASB definisce punti di controllo della sicurezza che si collocano tra gli utenti dei servizi e i CSP per verificare che i servizi siano utilizzati in conformità alle policy di sicurezza aziendali.
[17] IGA permette di gestire in maniera centralizzata le identità e i relativi accessi alle applicazioni, controllandone la profilatura e l'applicazione del principio del minimo privilegio tramite report e revisioni periodiche.

3.2 **Con riferimento alla migrazione delle applicazioni al cloud, assegnare un livello di ricorso a ciascuno dei seguenti approcci, distinguendo tra core banking e altri servizi.**

Livello: da 0 (min) a 5 (max)

Approccio metodologico	Core banking	Altri servizi
Approccio "repurchasing o replacing"[18]	☐	☐
Riprogettazione delle applicazioni attuali (refactoring[19]) in ottica cloud e successivo spostamento dei workload sul cloud	☐	☐
Revisione delle architetture e dei dati in ottica cloud (rearchitect) e successivo spostamento dei workload sul cloud	☐	☐
Costruire nuove applicazioni secondo paradigmi Cloud Native	☐	☐
"Lift and Shift" senza riprogettazione in ottica Cloud Native delle applicazioni (rehosting[20])	☐	☐
"Lift and Shift" con contestuale ottimizzazione/revisione delle applicazioni in ottica Cloud Native	☐	☐
Altro, specificare:	☐	☐

3.3 **Con riferimento al SaaS, IaaS/PaaS, indicare il livello di soddisfazione della banca/gruppo in relazione all'offerta complessiva dei CSP riguardo ai processi di sicurezza elencati.**

Livello: da 0 (min) a 5 (max)

	SaaS	IaaS/PaaS
Analisi del rischio	☐	☐
Pre-production security assessment	☐	☐
Security assessment in produzione (penetration tests, etc.)	☐	☐
Gestione degli incidenti di sicurezza	☐	☐
Monitoraggio degli eventi di sicurezza (Intrusion Detection Systems, SIEM, SOC)	☐	☐
Digital forensics	☐	☐
Auditing IT	☐	☐
Soluzioni di continuità (Disaster Recovery, Backup)	☐	☐
Altro, specificare:	☐	☐

[18] Le applicazioni aziendali sono sostituite da nuovi servizi SaaS in public cloud che hanno analoghe funzionalità.
[19] Attività in cui il codice sorgente viene ristrutturato e riprogettato per migliorarne la qualità.
[20] Porting delle applicazioni nel nuovo ambiente senza modifiche/ammodernamenti.

3.4 Indicare quali presidi di sicurezza aggiuntivi sono considerati dalla banca/gruppo per i service model specificati.

	SaaS	IaaS/PaaS
Policy e rules tecnologiche di rete ad hoc per il cloud	☐	☐
Audit specifici della banca/gruppo per il cloud pubblico	☐	☐
Penetration test interni sui servizi cloud	☐	☐
Integrazione del monitoraggio del CSP nel monitoraggio di sicurezza aziendale (es. SIEM)	☐	☐
Revisione delle policy di gestione degli incidenti per il cloud	☐	☐
Presidi specifici di sicurezza nella migrazione dei servizi in cloud	☐	☐
Previsione di presidi di sicurezza per la exit strategy	☐	☐
Presidi ulteriori per il Disaster Recovery e il backup	☐	☐
Altro, specificare:	☐	☐

3.5 Ai fini della stipula dei contratti per l'acquisizione di servizi in cloud, indicare i requisiti e/o le clausole considerati, specificandone il livello di importanza e il livello di diffusione nell'offerta dei CSP.

Livello: da 0 (min) a 5 (max)

Requisiti contrattuali/Clausole	Importanza	Diffusione
– Indicazioni sulle finalità, sulle limitazioni e sull'orizzonte temporale del trattamento dei dati personali	☐	☐
– Indicazione dettagliata delle misure tecniche e organizzative adottate per la protezione dei dati	☐	☐
– Logistica e geolocalizzazione dei dati	☐	☐
– Obbligo di certificare la cancellazione dei dati personali su richiesta del cliente	☐	☐
– Obbligo di comunicare la lista di eventuali subfornitori	☐	☐
– Consenso sulle modifiche alla lista dei subfornitori	☐	☐
– Estensione delle clausole contrattuali ai subfornitori	☐	☐
– Disposizioni riguardanti l'accessibilità, la disponibilità, l'integrità, la riservatezza e la sicurezza dei dati	☐	☐
– Conformità a standard di sicurezza informatica	☐	☐
– Possibilità di ispezionare e sottoporre a verifiche di audit il CSP, incluso l'accesso ai locali, da parte della banca/gruppo	☐	☐
– Processo di analisi dei rischi ICT	☐	☐
– Gestione delle crisi e continuità operativa	☐	☐
– Certificazioni conseguite dal CSP sulla Data Protection	☐	☐
– Obbligo di comunicare gli incidenti di sicurezza informatica alla banca/gruppo (es. interruzioni del servizio, data breach)	☐	☐
– Previsione del risarcimento dei danni causati da incidenti di sicurezza fra cui la perdita o l'accesso non consentito ai dati	☐	☐
– Inserimento clausole di salvaguardia per modifiche unilaterali sulle funzionalità dei servizi contrattualizzati	☐	☐
– Monitoraggio delle performance del CSP e indicazioni degli SLA	☐	☐
– Previsione di penali per mancato rispetto del contratto e/o degli SLA	☐	☐
– Obblighi del fornitore in caso di cessazione del contratto	☐	☐
– Diritti di cessazione	☐	☐
– Altro, specificare:	☐	☐

3.6 Indicare chi svolge prevalentemente il monitoraggio dei Service Level Agreement per i servizi in cloud.

1. Il CSP, mediante report periodici, verificati successivamente dalla banca/gruppo
2. La banca/gruppo, mediante tool messi a disposizione dal CSP
3. La banca/gruppo, mediante propri tool ☐
4. Il CSP e la banca/gruppo collaborano nel monitoraggio
5. Altro, specificare:

3.7 E' prevista l'adozione di policy ad hoc per la stesura dei contratti con i CSP?

1. Sì, con tutti i CSP
2. Sì, con la maggior parte di CSP
3. Sì, con alcuni CSP ☐
4. No

3.8 Illustrare un business case rappresentativo di un'iniziativa IT di portata significativa, realizzata o in corso di sviluppo, nel percorso di adozione/migrazione al cloud.

Nome del business case:	
CSP (scrivere "interno" se private cloud):	
Deployment model:	
Service model:	
Descrizione:	
Principali benefici conseguiti/previsti:	**Indicare uno o più (max 3) benefici conseguiti/previsti:**
Principali criticità riscontrate/previste:	**Indicare una o più (max 3) delle criticità riscontrate/previste:**