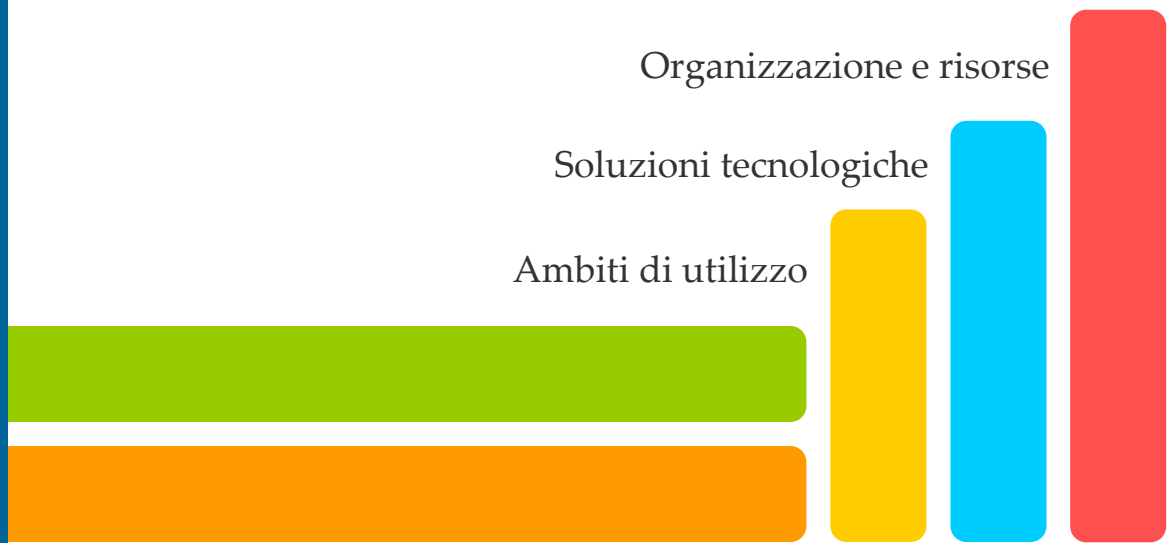
CIPA | Convenzione Interbancaria per l'Automazione

ABI Associazione Bancaria Italiana

Rilevazione sull'IT nel settore bancario italiano

Profili tecnologici e di sicurezza

Il cloud computing e le banche



Anno 2022

CIPA | Convenzione Interbancaria per l'Automazione

ABI Associazione Bancaria Italiana

Rilevazione sull'IT nel settore bancario italiano

Profili tecnologici e di sicurezza
Anno 2022

Il cloud computing e le banche

Maggio 2023

Rif. RILTEC-2023 – 7

CIPA, 2023

Indirizzo
Banca d'Italia
Dipartimento Informatica
Servizio Sviluppo Informatico
Divisione Tecnologie Interbancarie
Centro Donato Menichella
Largo Guido Carli, 1 – 00044 – Frascati (RM)

Telefono
+39 06 4792 6803

Email
segcipa@cipa.it

Sito Internet
www.cipa.it

Questo documento è disponibile nei siti Internet della CIPA e dell'ABI.

Coordinamento del gruppo interbancario	**Banca d'Italia – CIPA**	Paola Paparo
	ABI Lab	Romano Stasi

Membri del gruppo interbancario	**Banca d'Italia – CIPA**	Claudia Piscitelli
		Fabrizio Crocetti
		Domenico Petrucciani
		Katia Boria
		Daniela D'Amicis
		Matteo Elia
	ABI Lab	Marco Rotoloni
	BNL	Carlo Cotroneo
		Francesco Ziaco
		Fulvio Lazzari
		Alessandro De Bartolomeo
	Monte dei Paschi di Siena	Anna Osello
		Andrea Pagni
		Sabrina Ghilardi
	UniCredit	Santo Leonardo
		Sabrina Scanu
	Credito Emiliano – CREDEM	Paolo Torelli
		Sara Giroldi
	Mediolanum	Luca Concetti
		Michele Valente
		Milena Gobbi
	Intesa Sanpaolo	Claudio Paglia
		Antonio Melina
		Rosario Ilardo
		Michela Bulla
	Deutsche Bank	Daniele Colombo
		Tullio Giussani
	Banca Sella	Roberto Mosca Balma
	Banco di Desio e della Brianza	Luca Dettori
	Cassa Centrale Banca	Federico Andreatta
		Maria De Gennaro
	Banco BPM	Giuseppe Grieco
		Elena Rivolta
	Banca Agricola Popolare di Ragusa	Serena Vaturi
		Sergio Digrandi
	BPER Banca	Michele Vetturi
		Massimiliano Baga
		Alessandra Ravera
		Benedetta Govi
		Adelaide Aurora Tomasi
	Banca Popolare di Sondrio	Marco Tempra
		Stefano Garancini
		Luca Martinucci
	Banca Popolare dell'Alto Adige	Philip Weissensteiner

Banca C.R. Asti	Paolo Cerrato
	Marco Stroppiana
Crédit Agricole Italia	Daniele Andrisani
	Maria Libera Granatiero
	Carmine De Bellis
La Cassa di Ravenna	Alessandro Cela
Iccrea Banca	Marco Esposito
	Marco Giulianis
Mediobanca	Alessandro Campanini
	Gaetano Di Luca
Banca Passadore	Maurizio Ceragno
	Enrico Gelli
Dexia Crediop	Pasquale Tedesco
	Antonella Perretta
	Alessandro De Luca

Hanno inoltre collaborato

BNL	Diego Guerriero
Cassa Centrale Raiffeisen dell'Alto Adige	Ivo Martinolli
Allianz Bank	Gianluca Giroli
Cassa Centrale Banca	Alessandro Scipioni
Banco BPM	Claudio Elio Mariani
Banca Agricola Popolare di Ragusa	Andrea Sala
Banca Popolare Pugliese	Domenico Delle Side
Banca Popolare dell'Alto Adige	Thomas Forer
Banca C.R. Asti	Stefano Vaccaneo
Crédit Agricole Italia	Cesare Zuppa

Presentazione

La “Rilevazione sull’IT nel settore bancario italiano”, curata da CIPA (Convenzione Interbancaria per l’Automazione) e ABI (Associazione Bancaria Italiana), offre ogni anno un contributo di riflessione sugli aspetti economici, organizzativi e tecnologici connessi con l’utilizzo dell’Information and Communication Technology nel settore bancario. Oltre che agli operatori bancari – ai quali vuole fornire elementi di confronto e di riferimento utili per valutazioni funzionali alle scelte in ambito informatico – l’indagine si rivolge a tutti coloro che, a vario titolo, sono interessati a conoscere l’evoluzione dell’IT nel settore creditizio.

La Rilevazione si articola in due distinte indagini pubblicate separatamente.

La prima, dedicata all’esame dei profili economici e organizzativi dell’IT, analizza l’andamento e la ripartizione dei costi IT, le principali finalità della spesa informatica, l’assetto organizzativo e le modalità di sourcing, le iniziative di innovazione tecnologica, la composizione e la formazione del personale IT.

La seconda, focalizzata ogni anno su una specifica tematica, è riservata ai profili tecnologici e di sicurezza ed è rivolta all’analisi delle scelte IT in materia di metodologie, strumenti e tecnologie innovative, utilizzati nel contatto con la clientela, a supporto dei processi interni e all’esame dei connessi aspetti di sicurezza informatica.

Questa edizione della Rilevazione tecnologica affronta il tema del cloud computing, analizzandone la maturità e lo stato dell’arte nel settore bancario.

La trasformazione dei sistemi informatici delle aziende bancarie verso questo paradigma è in costante aumento: il cloud favorisce scalabilità e flessibilità, supporta l’innovazione tecnologica, rende più rapido lo sviluppo applicativo, consente un miglioramento complessivo del time to market.

Con l’adozione del cloud le banche sono chiamate ad affrontare nuove sfide che le conducono a rivedere i processi interni, le infrastrutture, le applicazioni, la sicurezza e lo sviluppo di competenze.

I rapporti delle indagini sono disponibili sui siti Internet della CIPA (www.cipa.it) e dell’ABI (www.abi.it).

La Presidenza della CIPA e la Direzione Generale dell’ABI esprimono apprezzamento per il contributo fornito dai gruppi bancari e dalle banche partecipanti alla Rilevazione e ringraziano i componenti del gruppo di lavoro, che ha condotto l’indagine e redatto il presente rapporto.

IL PRESIDENTE DELLA CIPA

Giuseppe ZINGRILLO

IL DIRETTORE GENERALE DELL’ABI

Giovanni SABATINI

Sommario

ANNO 2022

IL CLOUD COMPUTING E LE BANCHE

RILEVAZIONE TECNOLOGICA CIPA

IL QUESTIONARIO

- Strategia
- Percorso di adozione
- Budget
- Skill
- Polo di competenza
- Sicurezza
- CSP
- Contratti e clausole

30 domande

I RISPONDENTI

20 Gruppi bancari

5 Banche

TRA I RISPONDENTI

52% pone il cloud tra le prime 10 priorità di investimento

60% evolve il core banking in ottica cloud

64% lo usa nei processi di Operations

80% lo usa in ambiti innovativi (AI, Data science, DLT, IoT)

92% investe nel cloud

PUBLIC CLOUD

IaaS/PaaS
1,7%

SaaS
5,8%

7,5%
del BUDGET IT 2023

BENEFICI & CRITICITÀ
(TOP 3)

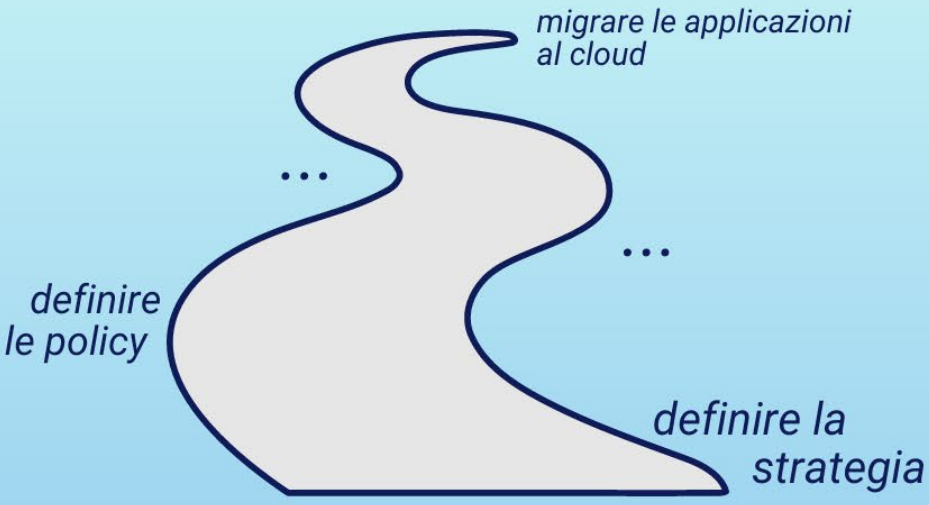
Scalabilità	Negoziazione col provider
Flessibilità d'uso	Limitate competenze interne
Supporto all'innovazione	Definizione contratti e SLA

ANNO 2022

RILEVAZIONE TECNOLOGICA CIPA

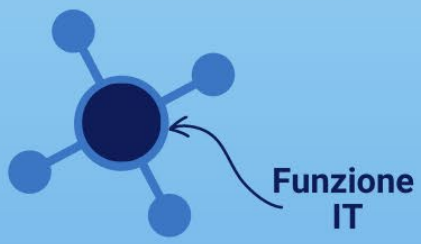
IL CLOUD COMPUTING E LE BANCHE

PERCORSO TIPICO VERSO IL CLOUD



POLO DI COMPETENZA

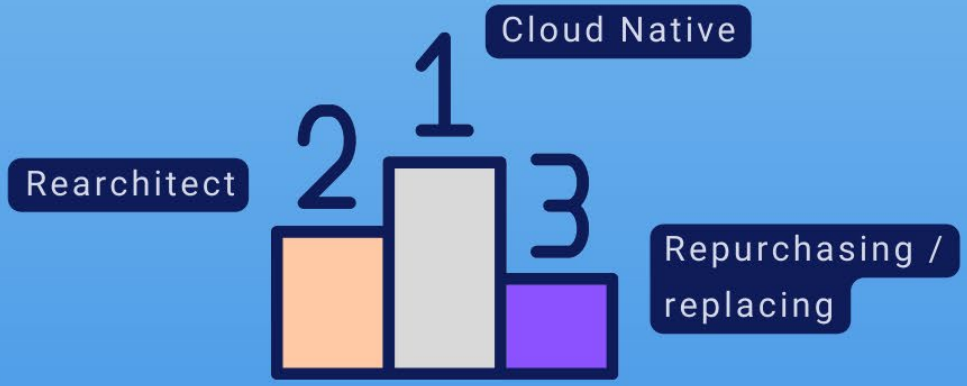
Hub & Spoke
(modello prevalente)



Skill del polo

- Architetture IT
- Gestione IT
- Sicurezza IT
- Dati
- Procurement
- Legale
- ESG

MIGRARE LE APPLICAZIONI AL CLOUD
(METODOLOGIE)



Sintesi dei risultati dell'indagine

La “Rilevazione sull’IT nel settore bancario italiano – Profili tecnologici e di sicurezza” affronta, in questa edizione, il tema del cloud computing nelle banche.

Il campione della Rilevazione è costituito da 20 gruppi bancari, che rappresentano il 93% del totale attivo del settore bancario italiano, e da cinque banche singole.

Il primo capitolo esamina gli aspetti di tipo strategico per l’adozione/evoluzione del cloud da parte delle aziende bancarie; l’adozione del cloud risulta tra le prime dieci priorità di investimento per oltre la metà del campione e per i tre quarti dei rispondenti l’approccio strategico prevalentemente adottato è di tipo tattico su ambiti selezionati[1]. In prospettiva, al 2025 si prevede il ricorso alla strategia Cloud First, che coinvolgerà il 44% dei rispondenti.

Al 2022 il cloud pubblico domina negli ambiti non critici e risulta utilizzato in maniera più contenuta per le infrastrutture critiche e i servizi di core banking, per i quali quasi raddoppierà nel triennio 2023-2025.

Tra i principali benefici riscontrati nell’adozione del cloud figurano la scalabilità e la flessibilità di utilizzo. Tra le principali criticità emergono il limitato potere negoziale nei confronti del fornitore, la scarsa disponibilità di competenze interne, la definizione dei contratti e relativi SLA, il rischio di vendor lock-in, il controllo della spesa.

Nel percorso di adozione oltre la metà del campione ha scelto di iniziare con la fase di definizione di una strategia per il cloud. In generale il percorso ‘tipo’ risulta costituito dalle seguenti fasi: a) definizione della strategia; b) definizione di policy; c) creazione di poli di competenza; d) sperimentazione di un cloud privato; e) adozione di cloud privato; f) porting di servizi su cloud privato; g) adozione del cloud pubblico; h) migrazione di servizi interni in cloud pubblico; i) acquisizione di servizi in cloud pubblico.

Riguardo le relazioni tra banche e fornitori, la metà dei rispondenti ricorre in prevalenza a un unico Cloud Service Provider (CSP); tra i requisiti principali considerati nella scelta del provider rilevano la solidità dell’azienda, le garanzie aggiuntive offerte per la tutela della privacy e della sicurezza dei dati e la trasparenza delle policy e dei contratti.

Sono limitati i casi di banche e gruppi bancari che offrono a loro volta servizi in cloud a terzi.

In media il 7,4% del budget IT 2023 è destinato al cloud pubblico. La quota per il SaaS è decisamente più elevata rispetto a IaaS/PaaS. Il budget IT impiegato per la modernizzazione/evoluzione delle applicazioni in ottica cloud si attesta mediamente al 3,9% e quello per la migrazione al cloud al 3,1%.

Il secondo capitolo è dedicato agli aspetti organizzativi aziendali connessi con l’adozione ed evoluzione al cloud. Al 2022 tra gli interventi per la governance del cloud figurano, per oltre la metà del campione, la revisione del security framework e la definizione delle policy per la cloud governance che, in previsione, sono segnalati per il 2025 da quasi tutti i rispondenti.

[1] Cfr. par. 1.1.

Riguardo il governo dei costi, circa un terzo del campione segnala interventi per l'adeguamento del consuntivo della spesa, dei modelli di budgeting e forecasting e del processo di procurement. In previsione, al 2025 gli interventi sul governo dei costi coinvolgeranno oltre il 60% del campione.

Per il rafforzamento delle competenze emergono le iniziative di promozione di 'laboratori' di supporto per il cloud, l'adozione di un piano di formazione e lo sviluppo interno della conoscenza, che hanno coinvolto circa la metà delle banche. Al 2025 tali iniziative saranno più diffuse, insieme all'assunzione di personale con specifiche competenze e alla creazione di una knowledge base per il cloud. Inoltre, per sfruttare le sinergie e agevolare lo sfruttamento della conoscenza, la metà delle banche ha costituito un polo di competenza per il cloud e, nel triennio 2023-2025, la quota aumenterà fino al 75%. I modelli adottati per il polo sono soprattutto di tipo 'accentrato' e 'hub&spoke' e, in prospettiva, quest'ultimo assetto sarà prevalente. Nella 'cabina di regia' del polo di competenza sono presenti, per oltre l'80% del campione, le conoscenze del comparto IT, riguardanti soprattutto le architetture, la gestione e la sicurezza informatica.

Le funzioni di business non sono autonome per l'adozione di soluzioni cloud ma devono interessare altre funzioni aziendali, in particolare l'IT per oltre l'80% del campione.

I processi di comunicazione interna, risorse umane, gestione sicurezza, gestione dei canali di contatto con la clientela[2] sono quelli che beneficiano più diffusamente del paradigma cloud e in quasi tutti è presente il cloud pubblico di tipo SaaS. Nelle aree dei processi di governo, di supporto e di marketing commerciali e customer service, il cloud pubblico appare più utilizzato del cloud privato, mentre nei processi di Operations prevale il cloud privato, che offre un'infrastruttura dedicata alla singola organizzazione. Con riferimento al ricorso al cloud negli ambiti e nei servizi IT, il cloud pubblico, in particolare di tipo SaaS, risulta più diffuso rispetto al cloud privato. In particolare spiccano la posta elettronica e i servizi di collaboration, seguiti dai servizi in area aziendale e quelli per l'analisi dei dati. In generale, per le nuove tecnologie (AI e ML, Data Science, Blockchain e DLT, IoT) sono utilizzati diffusamente tutti i modelli di cloud.

Il terzo capitolo riguarda gli aspetti di natura tecnologica e contrattuale. Tra gli interventi tecnologici, per l'86% delle aziende bancarie, rileva l'adeguamento dell'architettura IT per il cloud, che tutti prevedono di realizzare entro il 2025. A seguire figurano l'adeguamento dei presidi di Cyber Security, l'utilizzo di una Infrastructure as Code e l'automatizzazione del rilascio delle applicazioni, tutti segnalati da oltre la metà del campione e che al 2025 coinvolgeranno oltre l'80% delle realtà bancarie.

Con riferimento alla migrazione delle applicazioni al cloud, le metodologie più utilizzate, sia per il core banking che per gli altri servizi, sono la costruzione di nuove applicazioni secondo paradigmi di tipo cloud-native, seguita dall'approccio 'rearchitect'[3].

Le banche mostrano un grado di soddisfazione medio-alto per i principali processi di sicurezza attuati in collaborazione con il CSP, a esclusione dei processi di auditing IT e digital forensics, che sono riportati con un livello di soddisfazione medio. Quasi tutte le banche segnalano la presenza di presidi di sicurezza interni a complemento delle misure adottate dal fornitore; in particolare, per oltre la metà del campione si tratta dell'integrazione del monitoraggio interno con quello del CSP, delle policy e regole di rete e dei presidi di sicurezza nella migrazione dei servizi in cloud.

Riguardo le clausole contrattuali per il cloud, emerge una forte esigenza di ottenere garanzie contrattuali da parte del fornitore; negli accordi stipulati con i CSP, le clausole più rilevanti, segnalate a livello alto per il 95% dei rispondenti, sono quelle in tema di sicurezza dei servizi e dei dati, di logistica e geolocalizzazione, di segnalazione degli incidenti e di conformità agli standard di

[2] I processi fanno riferimento alla mappa applicativa ABILab.

[3] Cfr. par. 3.1.

sicurezza. Oltre la metà dei rispondenti segnala che le clausole contrattuali indicate sono diffuse nell'offerta dei CSP a livello alto o medio.

Circa i due terzi del campione ha definito policy ad hoc per i contratti: la metà con tutti i CSP, il 14% con la maggior parte e il 5% limitatamente ad alcuni provider.

Riguardo il monitoraggio dei livelli di servizio, circa il 90% dei rispondenti si avvale, a vario titolo, del fornitore: il 45% indica che il CSP collabora nel monitoraggio, il 32% che questo è attuato dal CSP salvo verifica a posteriori da parte della banca, il 14% esegue in autonomia il monitoraggio mediante tool messi a disposizione dal CSP.

Campione e note metodologiche

La “Rilevazione sull’IT nel settore bancario italiano – Profili tecnologici e di sicurezza” affronta, in questa edizione, il tema del cloud computing nelle banche.

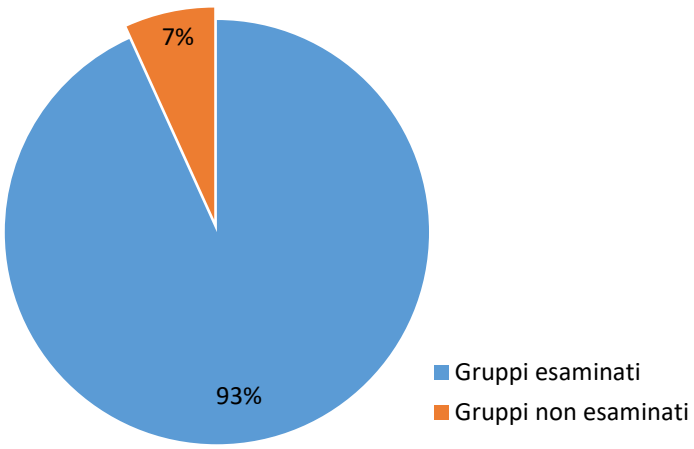
In particolare l’analisi si focalizza sulla strategia per l’adozione del cloud, i benefici e le criticità, il percorso di adozione del cloud, il rapporto con i Cloud Service Provider (CSP), la spesa per il cloud, gli ambiti di utilizzo, gli interventi organizzativi e tecnologici effettuati.

Campione dei partecipanti all'indagine

Ha aderito all’indagine un campione di 25 rispondenti composto da 20 gruppi - selezionati fra i primi gruppi bancari per totale attivo - e cinque banche singole, denominati nel seguito rispondenti o banche.

I gruppi partecipanti alla Rilevazione rappresentano il 93% dell’insieme dei gruppi bancari in termini di totale attivo[4] (Figura 1).

Figura 1 – Rappresentatività del campione dei gruppi per totale attivo



[4] Il totale attivo considerato al 31.12.2022 fa riferimento al gruppo bancario, comprensivo di tutte le sue componenti (bancarie e non bancarie) soggette a normativa prudenziale (es. banche, società strumentali, società finanziarie, SIM, filiali estere).

Dal punto di vista dell'operatività bancaria, calcolata sulla base del margine di intermediazione[5], la maggior parte dei gruppi rispondenti svolge prevalentemente attività di retail banking, seguita da corporate and investment banking, private banking e altre forme di operatività residuali.

Il campione dei gruppi, in base alla classificazione per dimensione operativa[6], risulta composto da: 6 gruppi Principali, 9 gruppi Medi e 5 gruppi Piccoli. L'elenco dei gruppi e delle banche partecipanti è riportato in Tabella 1.

Tabella 1 – Gruppi bancari e banche partecipanti alla Rilevazione

	6 gruppi Principali
1030	Gruppo Monte dei Paschi di Siena
2008	Gruppo UniCredit
3069	Gruppo bancario Intesa Sanpaolo
5034	Gruppo Banco BPM
5387	Gruppo BPER Banca
8000	ICCREA Banca
	9 gruppi Medi
1005	Gruppo bancario Banca Nazionale del Lavoro
3032	Gruppo Credito Emiliano – CREDEM
3062	Gruppo bancario Mediolanum
3104	Gruppo Deutsche Bank
3311	Gruppo Sella
3599	Cassa Centrale Banca
5696	Gruppo Banca Popolare di Sondrio
6230	Gruppo bancario Crédit Agricole Italia
10631	Gruppo bancario Mediobanca
	5 gruppi Piccoli
3440	Gruppo Banco di Desio e della Brianza
5036	Gruppo bancario Banca Agricola Popolare di Ragusa
5856	Gruppo Banca Popolare dell'Alto Adige

[5] Riferito al perimetro CIPA (cfr. Note metodologiche).

[6] La classificazione prevede l'utilizzo, come parametro dimensionale, del Totale attivo (aggregato della Matrice di Vigilanza Consolidata). Il Totale attivo considerato (al 31.12.2022) si riferisce al gruppo bancario comprensivo di tutte le sue componenti, bancarie e non bancarie, soggette a normativa prudenziale. Pertanto le classi dimensionali dei gruppi sono definite come segue:

- **Principali** per totale attivo > 120 miliardi di euro;
- **Medi** per totale attivo ≤ 120 miliardi e > 20 miliardi;
- **Piccoli** per totale attivo ≤ 20 miliardi.

6085	Gruppo Cassa di Risparmio di Asti
6270	Gruppo La Cassa di Ravenna
	5 Banche singole
3030	Dexia Crediop
3332	Banca Passadore & C.
3493	Cassa Centrale Raiffeisen dell'Alto Adige
3589	Allianz Bank
5262	Banca Popolare Pugliese

Note metodologiche

L'indagine è basata su un questionario, predisposto dalla Segreteria Tecnica della CIPA con la collaborazione del gruppo di lavoro interbancario e pubblicato sul sito Internet della CIPA (www.cipa.it); i dati sono stati acquisiti tramite la piattaforma Sondaggi della Banca d'Italia.

Nella Rilevazione si fa riferimento alla realtà bancaria all'interno del perimetro nazionale. Per i gruppi si considerano le componenti bancarie e le società strumentali, IT e non IT, che operano a supporto dell'attività bancaria (c.d. perimetro CIPA).

Le percentuali di partecipanti all'indagine indicate nelle rappresentazioni grafiche ("% di rispondenti") sono calcolate rapportando il numero di soggetti che forniscono una specifica risposta rispetto al totale dei partecipanti. In alcune analisi, un singolo soggetto può fornire più risposte e quindi comparire più volte nei risultati forniti; in tal caso viene riportata l'indicazione "risposte multiple".

Per molte analisi presenti in questa Rilevazione è stato richiesto di assegnare un punteggio crescente da 0 a 5 per esprimere un livello di rilevanza, sulla base del quale si calcola un valore medio. Una mancata risposta a un singolo item è, di norma, equiparata a una risposta con punteggio zero qualora il rispondente abbia risposto ad almeno un altro item della domanda. I punteggi medi vengono associati alle seguenti fasce di rilevanza: bassa tra 0 e 1, medio-bassa tra 1 e 2, media tra 2 e 3, medio-alta tra 3 e 4, alta tra 4 e 5.

Nel calcolo delle percentuali, i valori numerici riportati su alcuni grafici possono risentire dell'arrotondamento. Pertanto, la somma dei valori rappresentati può non risultare pari al 100%.

Capitolo 1. Aspetti strategici

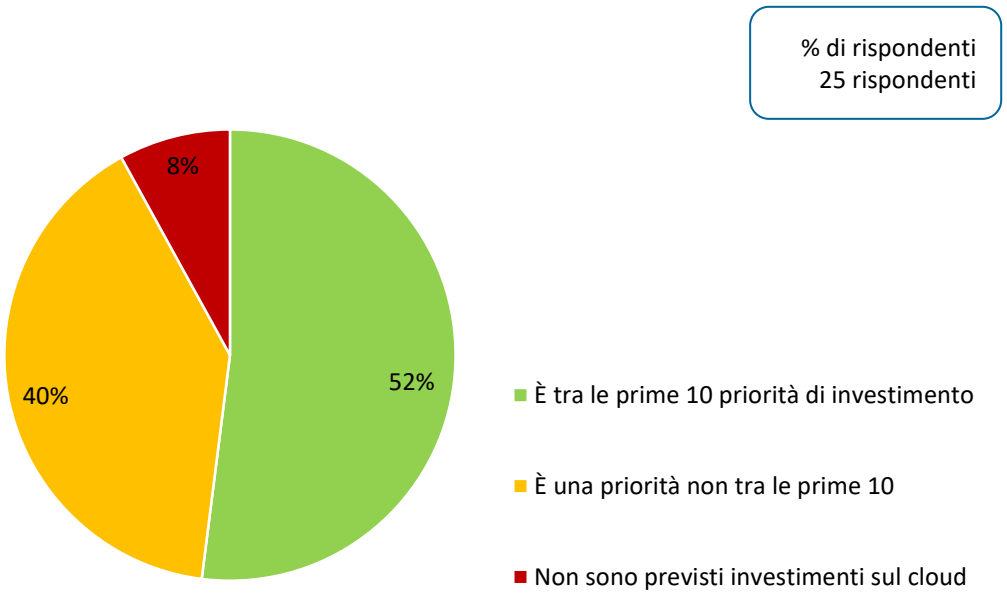
Il primo capitolo esamina gli aspetti strategici relativi al percorso intrapreso dalle banche per l'adozione del cloud, attraverso l'analisi delle priorità di investimento, lo specifico approccio strategico seguito, l'utilizzo dei service model e deployment model, la valutazione dei benefici e delle criticità, il rapporto con i Cloud Service Provider (CSP), la spesa per il cloud.

1.1 Strategia di investimento e utilizzo dei modelli cloud

In questo paragrafo vengono esaminate le priorità di investimento delle banche, l'approccio strategico e i modelli di cloud prevalentemente adottati.

Emerge che l'adozione del cloud risulta tra le prime dieci priorità di investimento per oltre la metà del campione (52%) (Figura 2).

Figura 2 – Strategia di investimento



APPROCCI STRATEGICI DI ADOZIONE DEL CLOUD

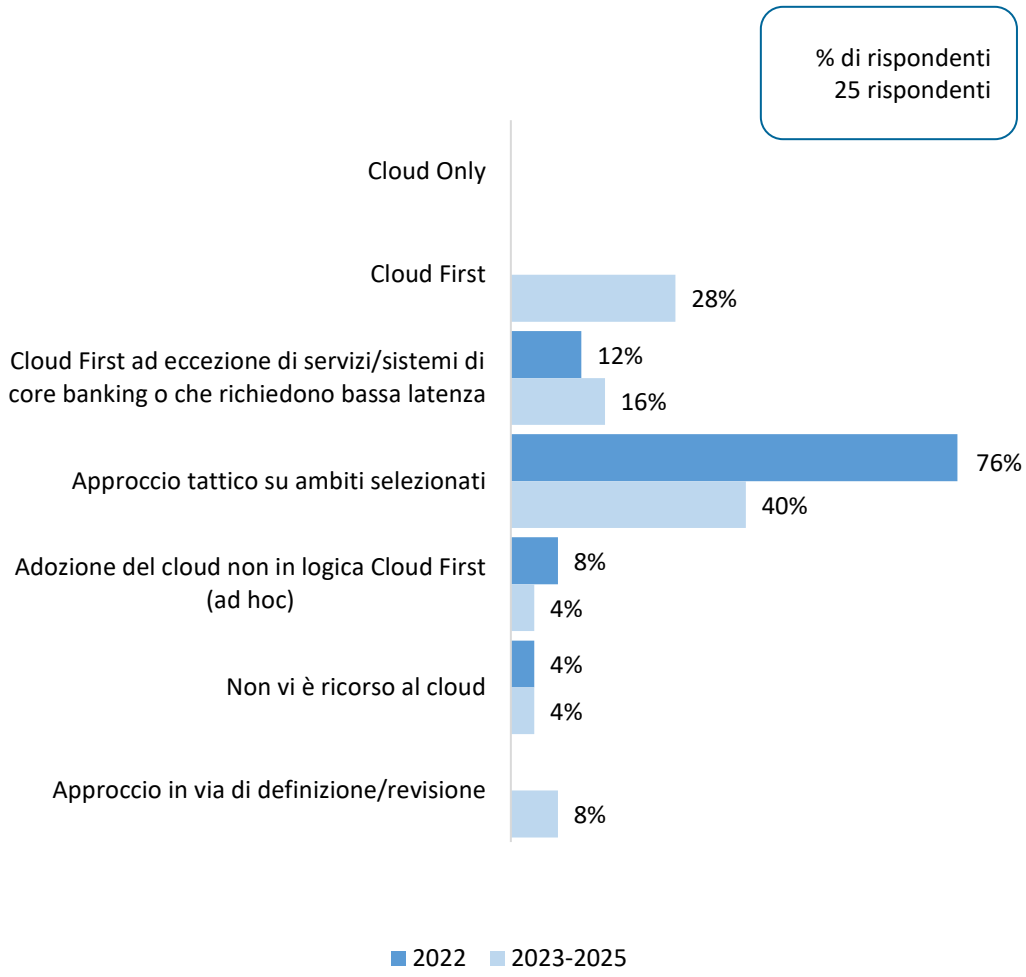
Approccio Cloud Only: *prevede l'utilizzo del cloud per tutti i sistemi e servizi aziendali.*

Approccio Cloud First: *privilegia l'adozione del cloud nella predisposizione o modifica di un servizio applicativo o di un'infrastruttura.*

Approccio tattico su ambiti selezionati*: prevede l'adozione del cloud su specifici ambiti anche senza una strategia ben definita.*

Nella situazione al 2022, l'approccio strategico di adozione del cloud, per il 76% dei rispondenti, è tattico su ambiti selezionati. L'approccio Cloud First (due voci del grafico), sebbene al 2022 sia poco diffuso, in previsione coinvolgerà il 44% dei rispondenti, superando l'approccio tattico su ambiti selezionati. Quest'ultimo permarrà comunque per il 40% dei rispondenti. Nessun rispondente indica l'approccio Cloud Only, né nella situazione attuale, né in previsione (Figura 3).

Figura 3 – Approccio strategico di adozione del cloud (attuale e in prospettiva)



DEPLOYMENT MODEL E SERVICE MODEL

Definizioni tratte da Orientamenti in materia di esternalizzazione dell'EBA:

***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.*

I servizi di cloud computing si distinguono in tre modelli, a seconda di quanta parte dello stack tecnologico è offerta e controllata dal fornitore:

***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.*

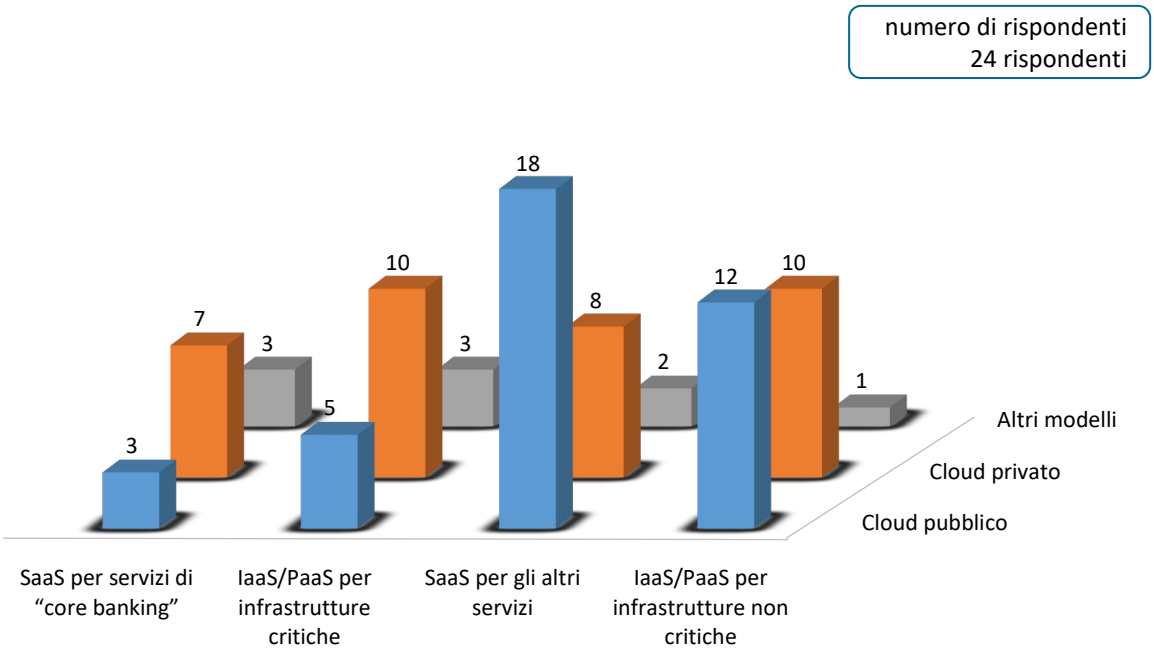
***Platform as a Service (PaaS):** il provider offre l'ambiente necessario (piattaforme elaborative, linguaggi di programmazione - API, ambienti di sviluppo e testing, tools e librerie) per lo sviluppo e il deploy di applicazioni del cliente o di una terza parte.*

***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.*

Alle banche è stato chiesto di indicare quali modelli IaaS, PaaS o SaaS, suddivisi per ambiti critici (core banking e infrastrutture critiche) e ambiti non critici (altri servizi e infrastrutture non critiche), sono utilizzati al 2022 e con quale deployment model prevalente, tra pubblico, privato e altri modelli. Quest'ultima classificazione include situazioni di cloud ibrido per le quali i gruppi non hanno identificato la prevalenza tra pubblico e privato. Il cloud privato ricomprende eventuali cloud di community della propria realtà bancaria.

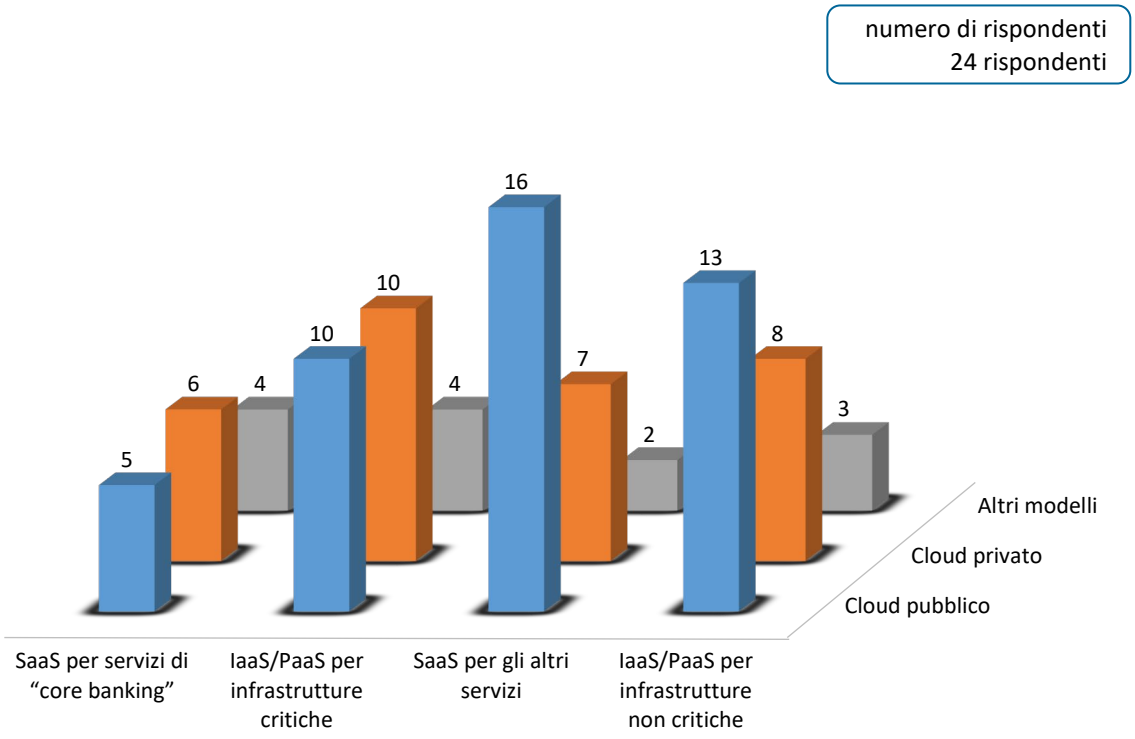
Emerge che, al 2022, il cloud pubblico prevale negli ambiti non critici, mentre per i servizi di core banking e le infrastrutture critiche il ricorso al cloud pubblico è più contenuto. Il cloud privato è invece utilizzato in maniera più uniforme per tutti i modelli (Figura 4).

Figura 4 – Uso del cloud: Service e Deployment model (al 2022)



In previsione, nel triennio 2023-2025 cresce l'utilizzo del cloud pubblico per i servizi di core banking e per le infrastrutture critiche, pur rimanendo prevalente per altri servizi e le infrastrutture non critiche. Aumenta, anche se in maniera non significativa, l'utilizzo di altri modelli (Figura 5).

Figura 5 – Uso del cloud: Service e Deployment model (triennio 2023-2025)



1.2 Benefici e criticità nell'adozione/evoluzione del cloud

L'indagine prosegue con una valutazione dei benefici e delle criticità attesi e riscontrati dalle banche nel percorso di adozione/evoluzione del cloud.

Per valutare il livello di rilevanza, è stato chiesto ai rispondenti di assegnare un punteggio crescente da 0 a 5, in modo da collocarlo in una delle seguenti fasce: bassa tra 0 e 1, medio-bassa tra 1 e 2, media tra 2 e 3, medio-alta tra 3 e 4, alta tra 4 e 5 (cfr. note metodologiche).

Esaminando la Figura 6, risulta che molti benefici attesi si collocano in fascia medio-alta o alta. I benefici riscontrati si collocano invece a livelli inferiori. Questo fenomeno potrebbe dipendere da iniziative non ancora concluse e per le quali bisognerà attendere la conclusione dei progetti per rilevarne i benefici. I valori maggiori emergono per scalabilità e flessibilità di utilizzo, sia come livello atteso (4,3 e 4,5) che riscontrato (3,2 e 3).

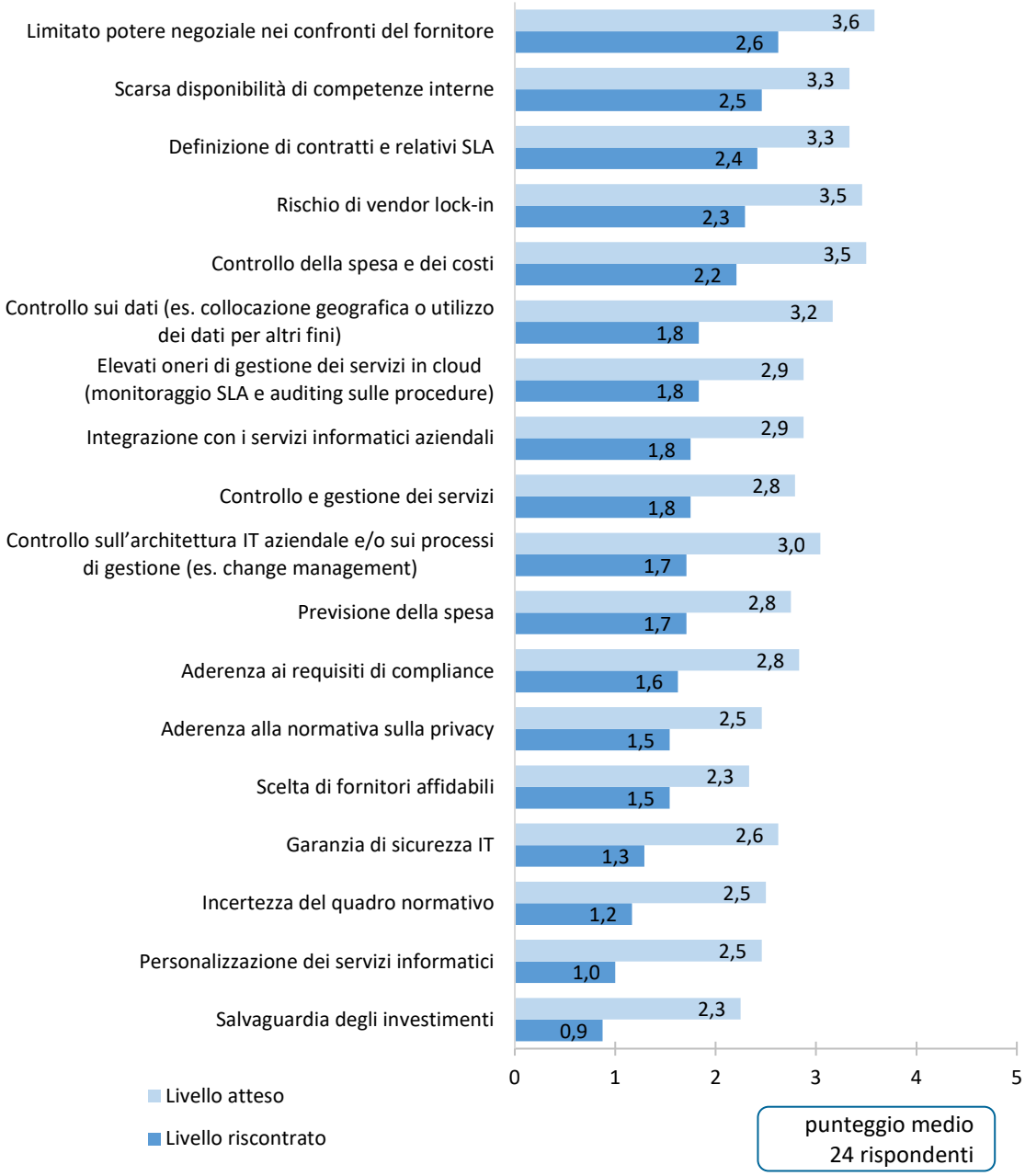
Tra i benefici riscontrati la riduzione dei costi si colloca agli ultimi posti (1,3), nonostante fosse considerato un beneficio atteso di livello medio-alto.

Figura 6 – Rilevanza dei benefici attesi e riscontrati nell'adozione del cloud

Dall'analisi emerge che le criticità complessivamente sono percepite con minore rilevanza rispetto ai benefici.

Le principali criticità riscontrate sono: limitato potere negoziale nei confronti del fornitore, scarsa disponibilità di competenze interne, definizione di contratti e relativi SLA, rischio di vendor lock-in, controllo della spesa e dei costi, tutte in fascia media (Figura 7).

Figura 7 – Rilevanza delle criticità attese e riscontrate nell'adozione del cloud

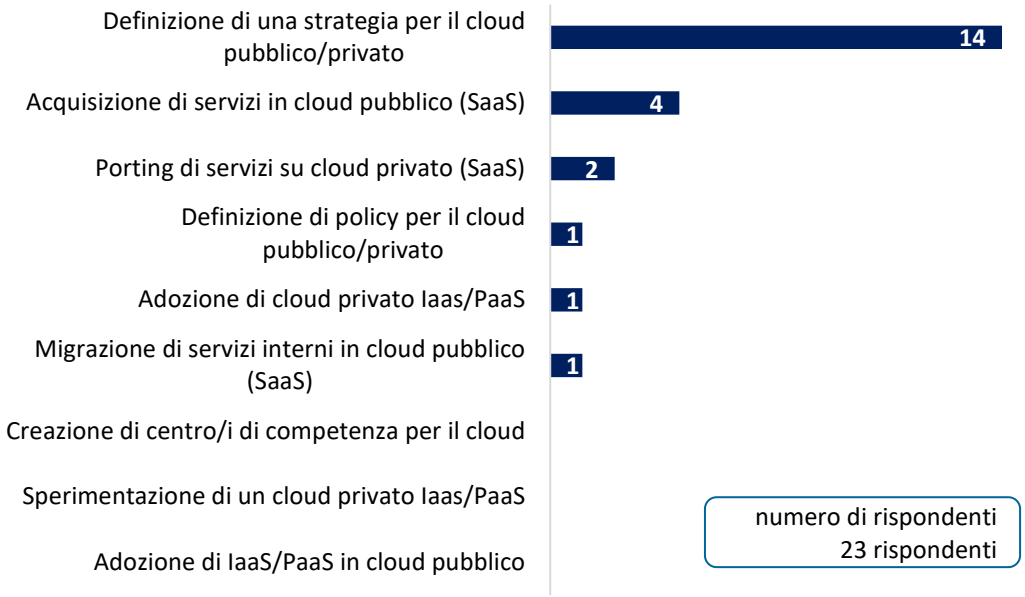


1.3 Percorso di adozione del cloud

Questo paragrafo mostra il percorso compiuto dai rispondenti nell'adozione del cloud. È stato infatti chiesto alle banche di ordinare temporalmente ciascuna fase di un ipotetico cammino di adozione del cloud, in modo da identificare il loro specifico percorso.

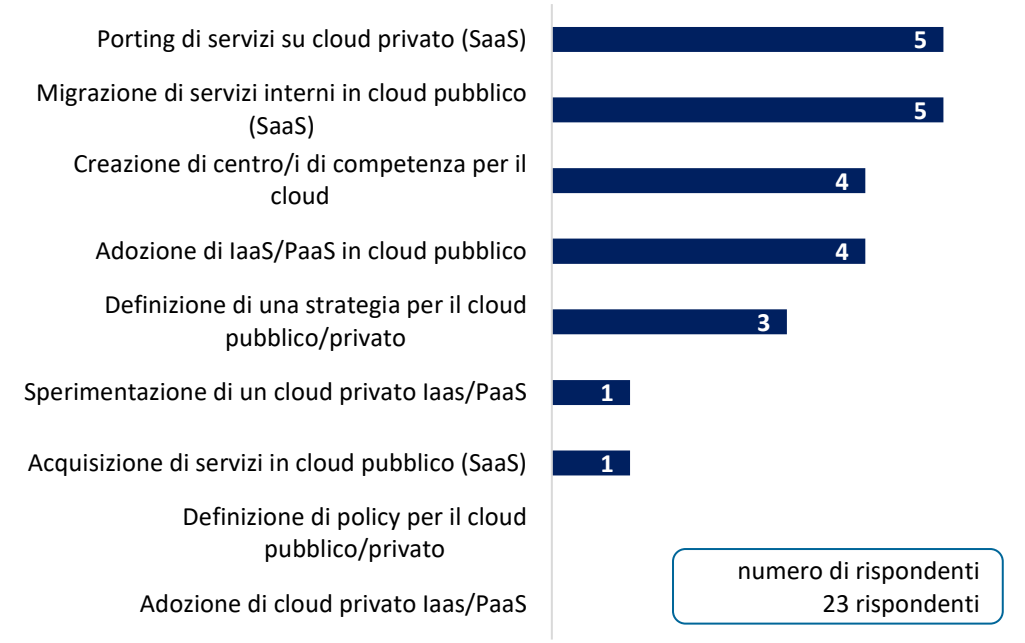
Restringendo l'analisi alla sola prima fase indicata (Figura 8), emerge che oltre la metà del campione (14) ha scelto di iniziare con la definizione di una strategia per il cloud.

Figura 8 – Prima fase del percorso di adozione del cloud



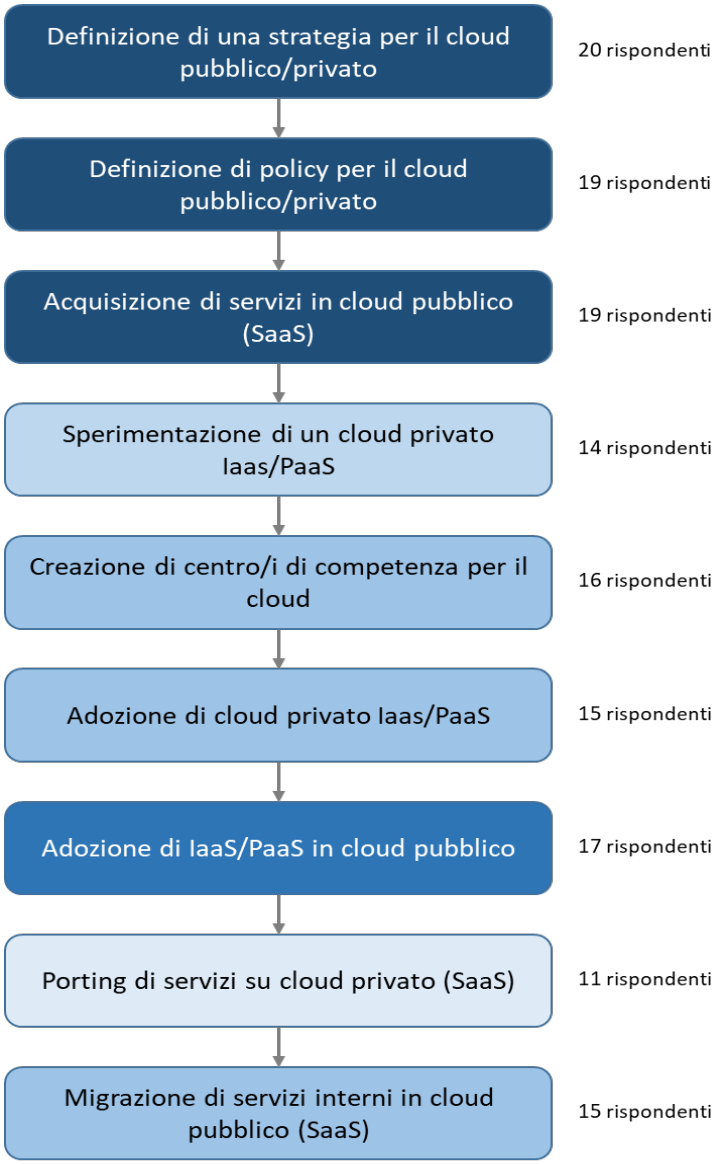
Le fasi che più di frequente sono poste alla fine del percorso di adozione del cloud sono il porting di servizi su SaaS privato e la migrazione di servizi su SaaS pubblico (Figura 9).

Figura 9 – Ultima fase del percorso di adozione del cloud



Il diagramma seguente (Figura 10) colloca le tappe di adozione del cloud all'interno di un 'percorso rappresentativo', ottenuto calcolando la posizione media sulla base di quella indicata all'interno dei singoli percorsi dei 23 rispondenti. L'intensità di colore dei blocchi rispecchia la frequenza con cui ciascuna fase è presente nei vari percorsi dichiarati: a intensità maggiore corrisponde frequenza maggiore (il numero di rispondenti è indicato a destra).

Figura 10 – Percorso 'tipo' di cloud transformation

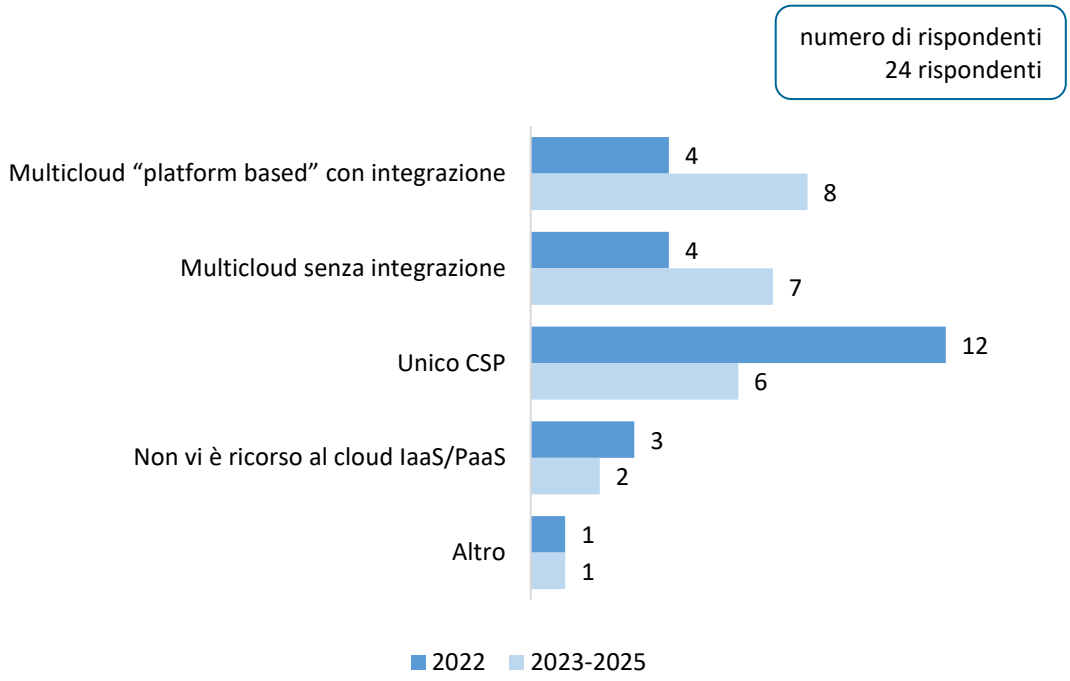


1.4 Rapporto con i Cloud Service Provider (CSP)

Questo paragrafo analizza le relazioni tra le banche e i CSP attraverso i principali requisiti considerati nella scelta del fornitore. Il paragrafo si conclude con l'analisi dei rispondenti che ricoprono a loro volta anche il ruolo di fornitore di servizi cloud.

Al 2022 emerge che la metà dei rispondenti ricorre in prevalenza a un unico CSP. In previsione quasi raddoppia il ricorso al multicloud, con o senza integrazione (Figura 11).

Figura 11 – Strategia di ricorso a CSP per IaaS/PaaS

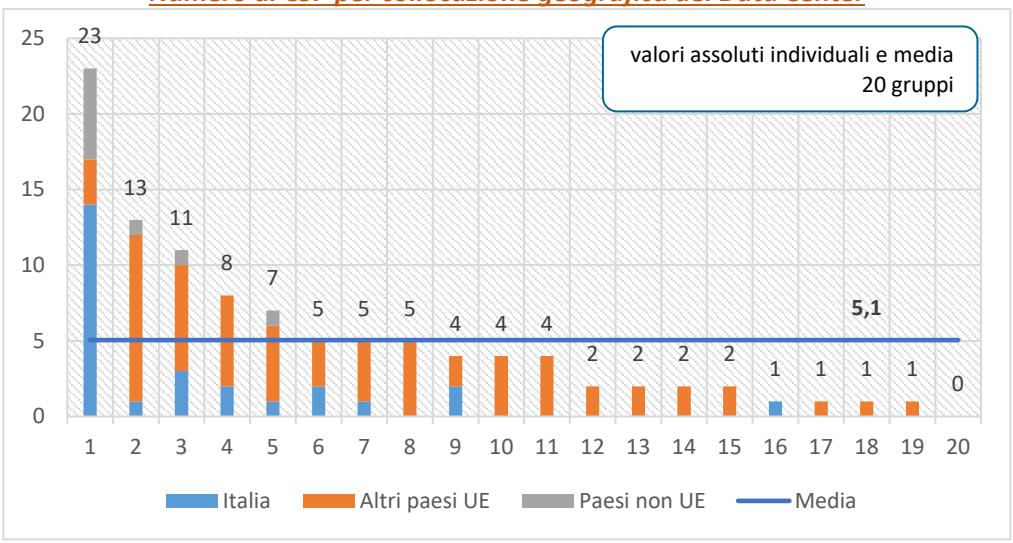


NUMERO DI CSP - RILEVAZIONE ECONOMICA ESERCIZIO 2021

Di seguito è mostrata un'analisi tratta dalla Rilevazione Economica CIPA dell'esercizio 2021, dalla quale emerge che il numero medio dei CSP coinvolti nel percorso di adozione del cloud, su un campione di 20 gruppi bancari, si ***attestava a 5,1****.*

Nel grafico è rappresentata, per ciascun gruppo, una barra con il numero totale di CSP che erogavano servizi in cloud, suddivisa a sua volta in base all'area geografica del Data Center.

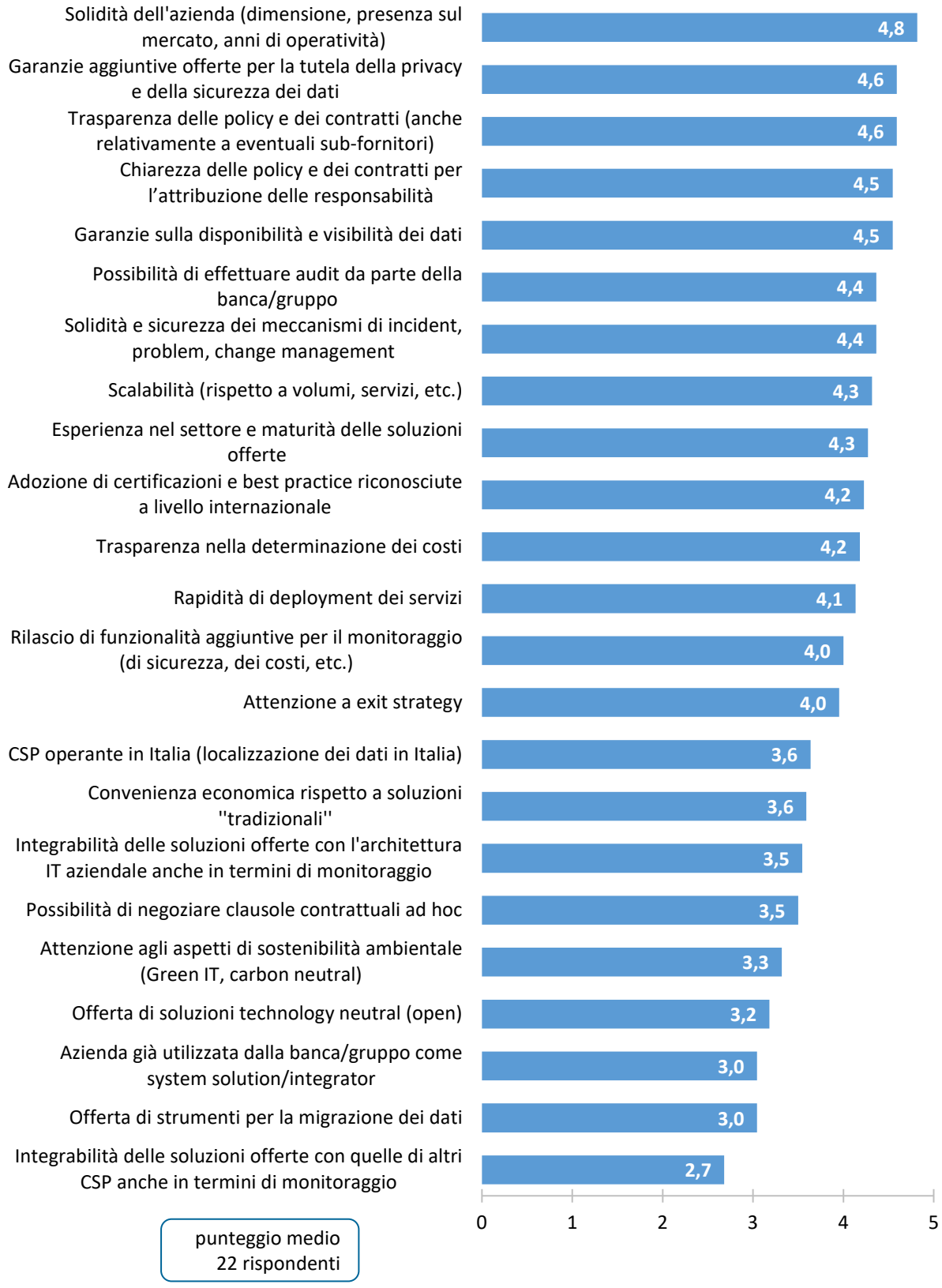
Numero di CSP per collocazione geografica del Data Center



Analizzando il livello di rilevanza attribuito ai requisiti nella scelta di un CSP, dalla Figura 12 risulta che la maggior parte di essi è in fascia alta. Tra i principali emergono la solidità dell'azienda (4,8), le

garanzie aggiuntive offerte per la tutela della privacy e della sicurezza dei dati e la trasparenza delle policy e dei contratti (4,6).

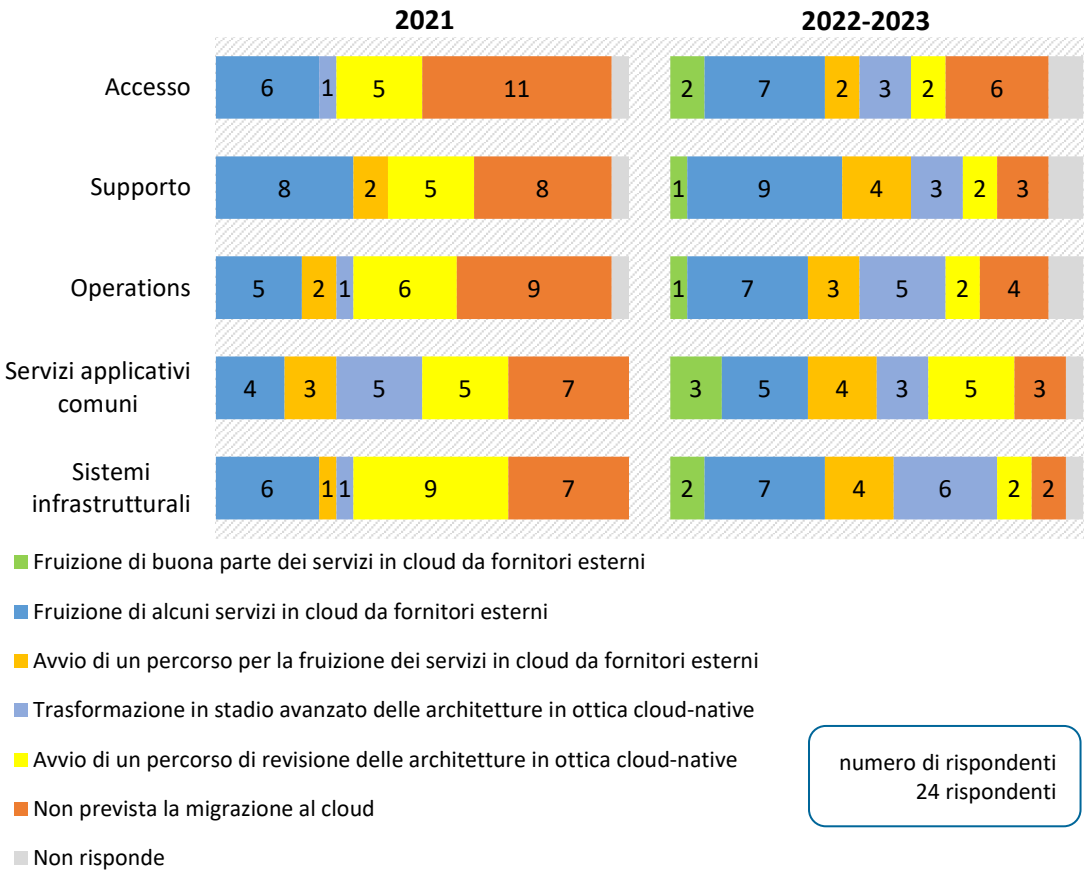
Figura 12 – Importanza dei requisiti nella selezione di un nuovo CSP



MIGRAZIONE AL CLOUD - RILEVAZIONE TECNOLOGICA CIPA 2021

Di seguito si ripropone l'analisi del livello di migrazione a tecnologie cloud rilevato nel 2021 (Rilevazione Tecnologica CIPA 2021 sulla trasformazione digitale in banca), per 24 rispondenti (banche e gruppi bancari).

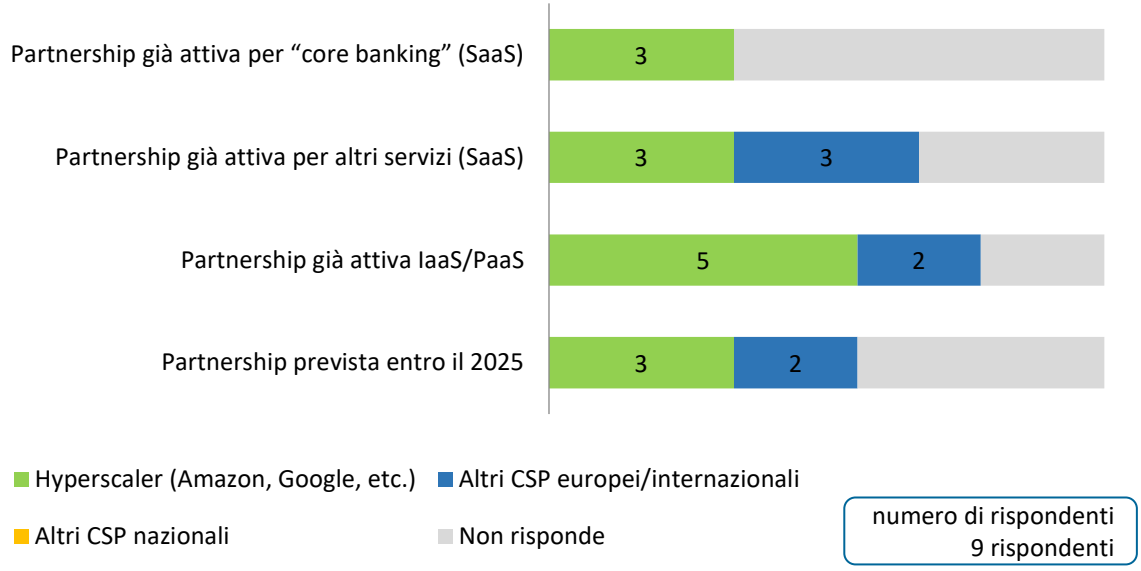
Il grafico mostra la situazione al 2021 e previsionale 2022-2023 con riferimento alle aree della mappa applicativa ABI Lab. Vengono presi in esame sei livelli di migrazione (cfr. legenda del grafico), partendo dal livello in cui buona parte dei servizi sono fruiti in cloud da fornitori esterni per arrivare, con tappe intermedie, a quello in cui la migrazione al cloud non è prevista.



Sono limitati i casi di banche che offrono a loro volta servizi in cloud. Gli ambiti principali in cui ciò accade sono elencati nella Figura 13. L'analisi di un campione di 22 rispondenti mostra che l'offerta è variegata sia verso soggetti in Italia che all'estero. L'offerta dei servizi può avvenire in partnership con hyperscaler o CSP europei/internazionali (Figura 14).

Figura 13 – Fornitura di servizi cloud in Italia e all'estero

Figura 14 – Partnership per la fornitura di servizi in cloud



1.5 La spesa per il cloud

L'esame delle strategie di adozione del cloud si conclude con la valutazione del relativo impegno economico: budget IT 2023 per il cloud pubblico SaaS e IaaS/PaaS, per la modernizzazione ed evoluzione delle applicazioni e per la migrazione al cloud propriamente detta.

Riguardo il budget IT 2023 per il cloud pubblico (per tutti i modelli), vi è una grande variabilità tra i 16 gruppi che hanno fornito una risposta, che stanziano da meno dell'1% fino al 15%, con una media del 7,4%. La quota per il SaaS è decisamente più elevata rispetto a IaaS/PaaS pubblico (Figura 15 e Figura 16).

Figura 15 – Budget IT 2023 per il cloud pubblico

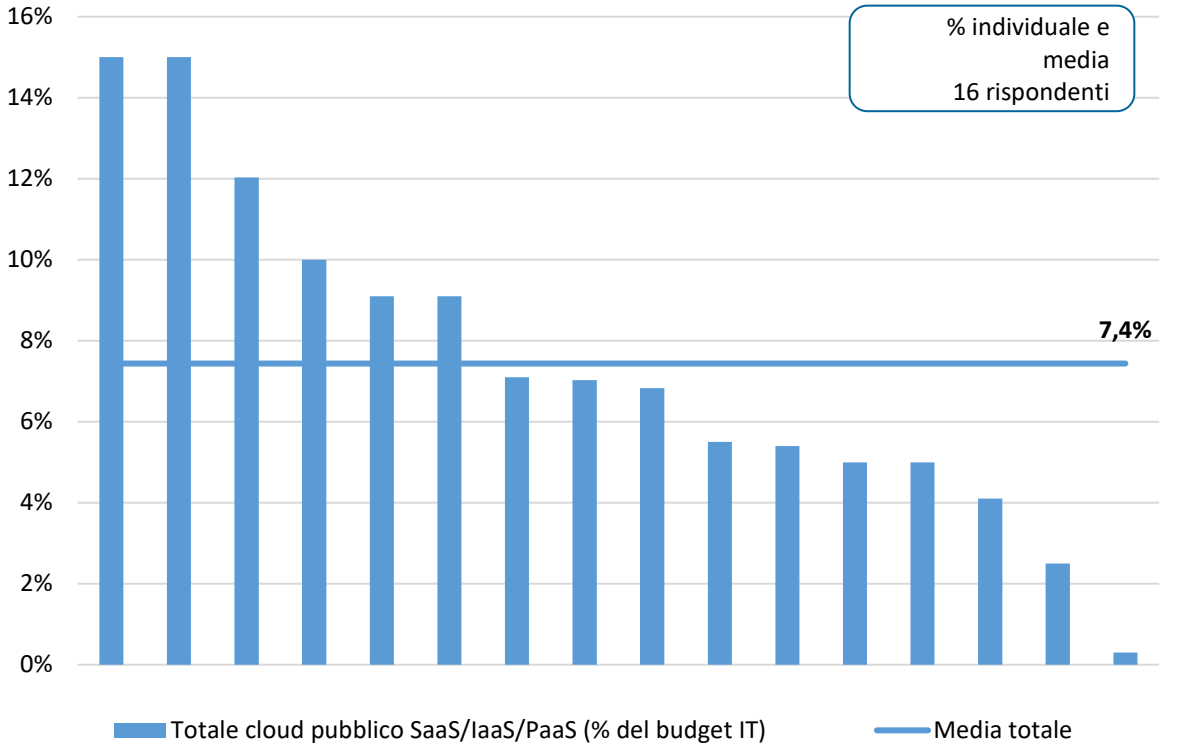
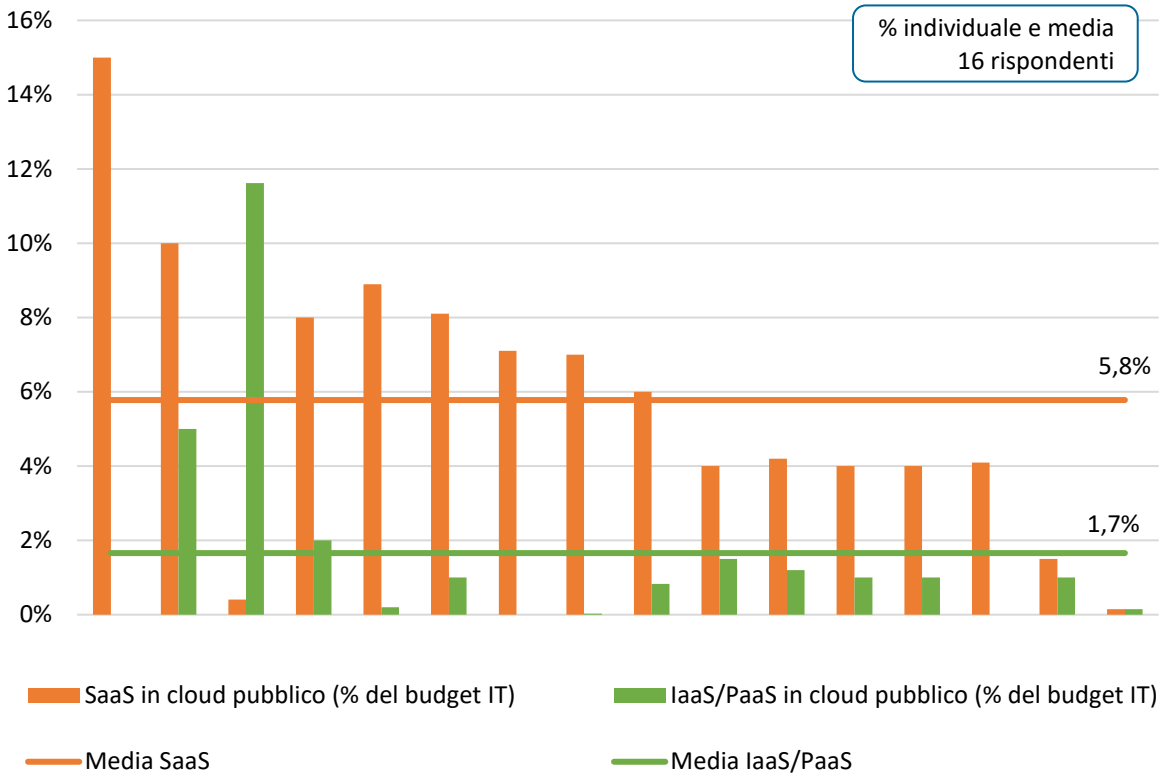
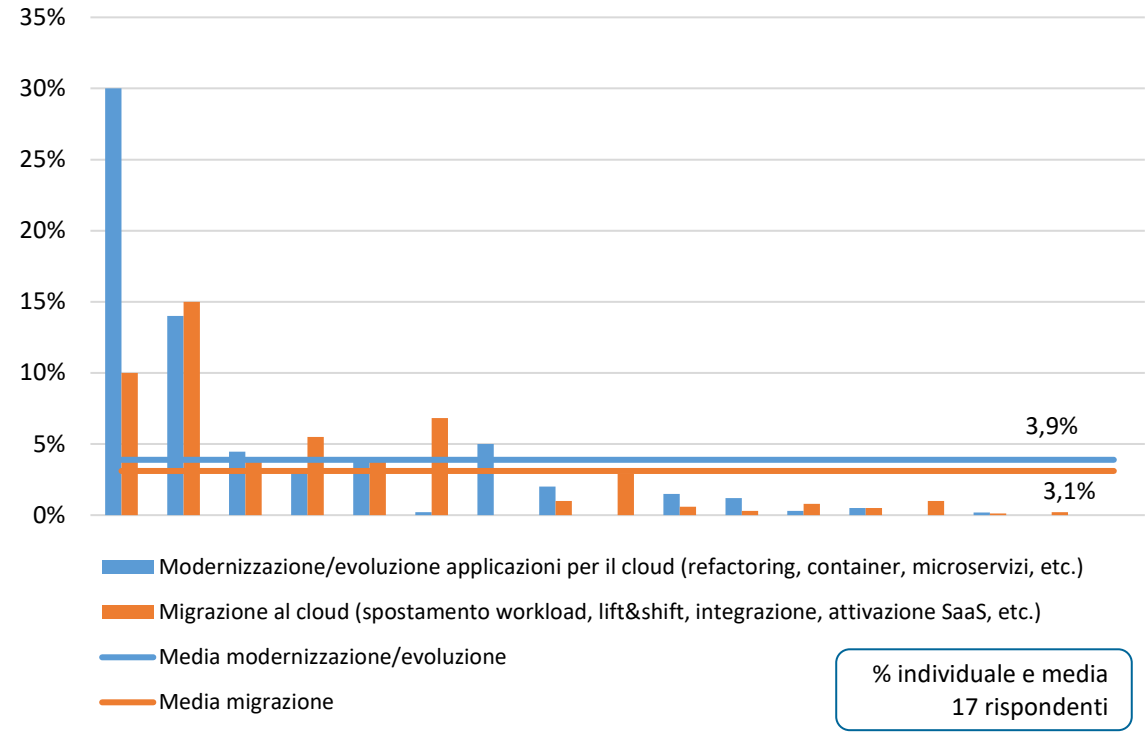


Figura 16 – Budget IT 2023 per il cloud pubblico ripartito per SaaS e IaaS/PaaS



In media il budget IT per la modernizzazione ed evoluzione delle applicazioni si attesta al 3,9% e quella per la migrazione al cloud propriamente detta al 3,1% (Figura 17). Anche in questo caso si registra ampia variabilità dei valori individuali.

Figura 17 – Budget IT 2023 per evoluzione delle applicazioni e migrazione al cloud



Capitolo 2. Aspetti organizzativi

Un proficuo percorso di adozione del cloud richiede una serie di interventi, sia di natura organizzativa sia di tipo tecnologico. Come già visto nel capitolo 1, tra le principali criticità riscontrate nell'adozione del cloud da parte delle realtà bancarie rientrano aspetti di governance, la scarsa disponibilità di competenze interne, il controllo e la gestione dei costi. Si tratta di priorità che il settore bancario deve affrontare per sfruttare appieno il potenziale sotteso all'adozione del cloud computing.

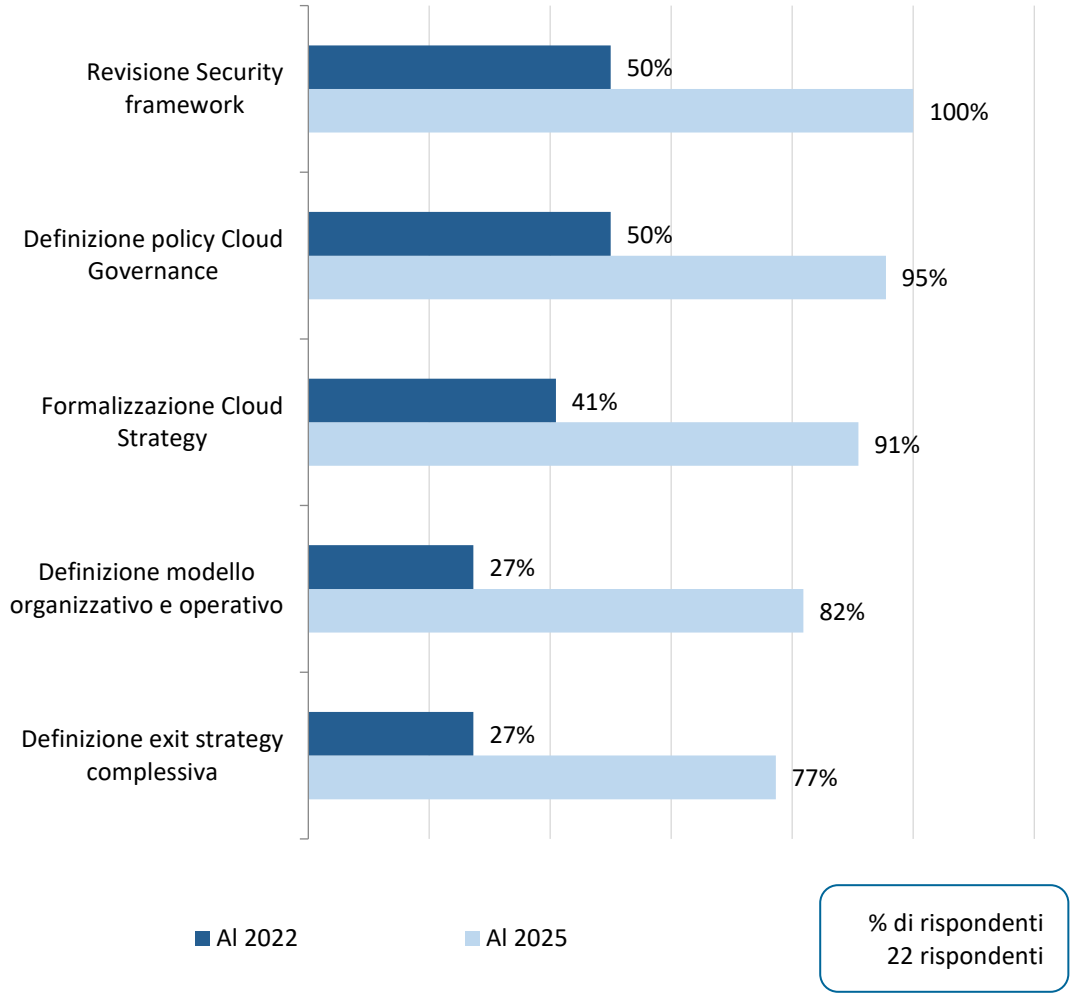
In questo capitolo la Rilevazione affronta tali priorità e, in particolare, individua gli interventi attuati e previsti per la governance del cloud, la gestione dei costi, i modelli organizzativi, anche a supporto del rafforzamento delle competenze. D'altra parte individua quali sono i modelli di cloud (SaaS, IaaS o PaaS, pubblico o privato) utilizzati più diffusamente nei processi bancari e nei diversi ambiti e servizi dell'Information Technology, anche in prospettiva, per il conseguimento dei principali benefici di flessibilità, innovazione, riduzione del time to market.

2.1 Interventi organizzativi per la gestione del cloud

Al 2022, tra gli interventi già attuati dai rispondenti per la governance del cloud, spiccano quelli relativi alla revisione del security framework, la definizione delle policy per la cloud governance (50%) e la formalizzazione della cloud strategy (41%).

In previsione, al 2025, tutti i rispondenti avranno rivisto il security framework e la quasi totalità avrà definito le policy per la cloud governance; oltre i tre quarti degli intervistati avrà attuato tutti gli interventi evidenziati in Figura 18. Tra gli interventi organizzativi in crescita al 2025 vi è anche la definizione di una "exit strategy". La strategia di uscita dal cloud consente una mitigazione del rischio in caso di cessazione dell'accordo di outsourcing con il Cloud Service Provider. Attraverso la definizione di uno specifico piano di uscita viene assicurata la continuità e la qualità dei servizi informatici aziendali.

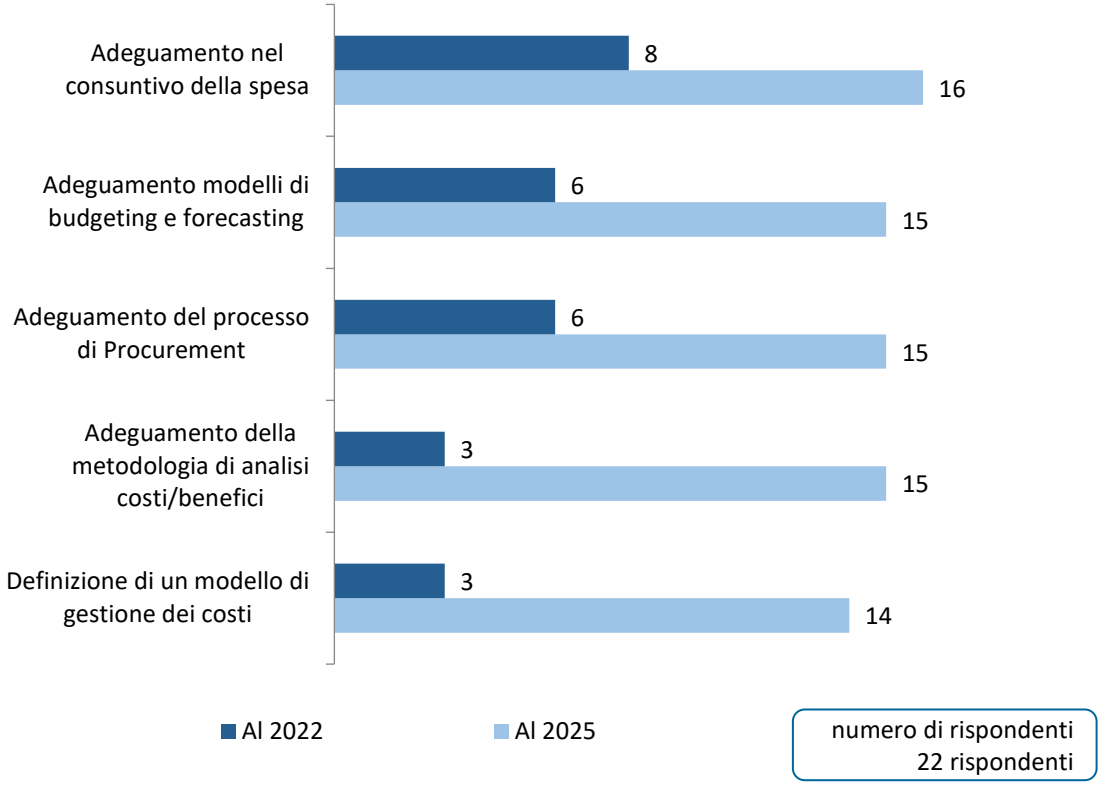
Figura 18 – Interventi organizzativi per la governance del cloud



Nell'ambito del governo dei costi, al 2022 gli interventi attuati da circa un terzo del campione sono i seguenti: adeguamento nel consuntivo della spesa, dei modelli di budgeting e forecasting, del processo di procurement (Figura 19).

In previsione, al 2025, il coinvolgimento delle banche per tutti gli interventi elencati sarà più ampio, superando il 60% del campione.

Figura 19 – Interventi organizzativi per il governo dei costi



2.2 Le competenze per il cloud

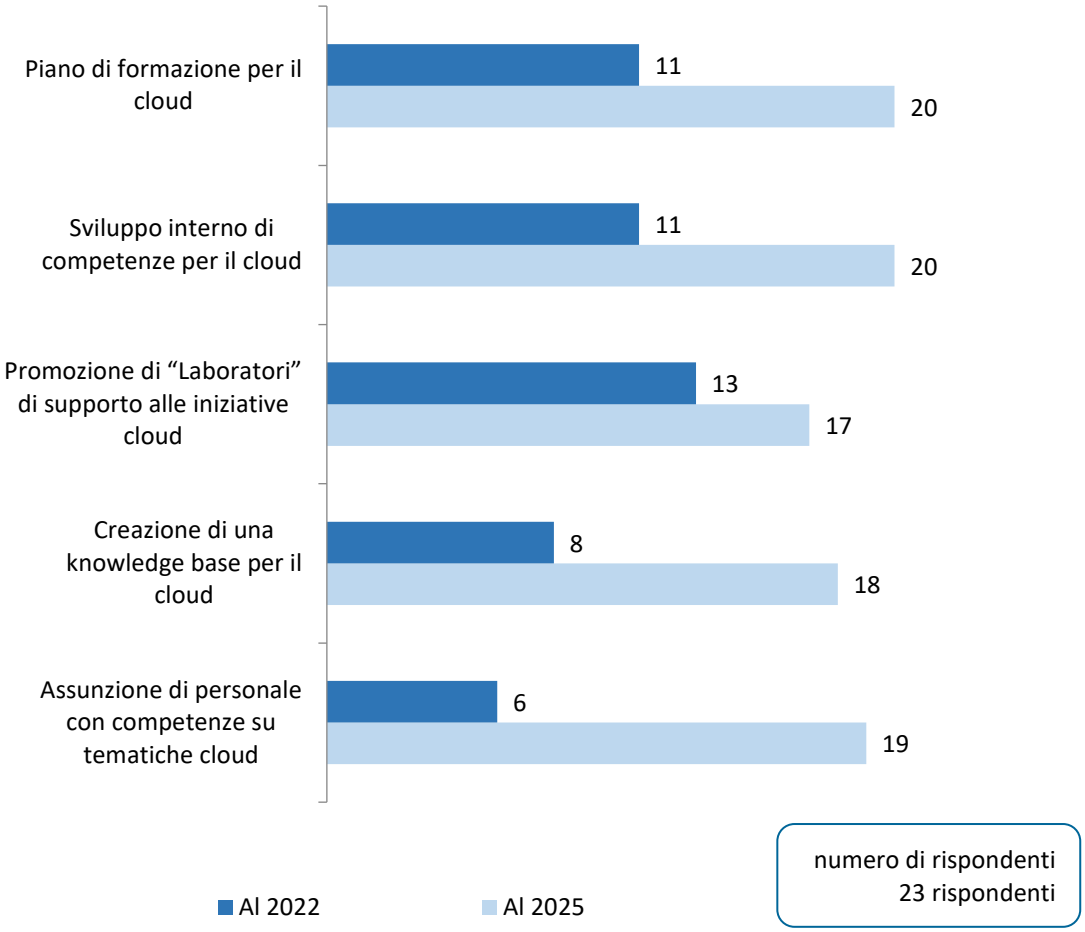
Una delle criticità emersa nelle analisi del capitolo 1 riguarda il tema delle competenze. Acquisire le conoscenze è una delle leve da considerare per sfruttare le opportunità offerte dal cloud computing.

In questo paragrafo l'analisi si focalizza sugli interventi già attuati per il rafforzamento delle competenze, facendo emergere d'altra parte quelli che risultano necessari in prospettiva.

La creazione di 'poli' di competenza per il cloud computing, con l'implementazione di specifici modelli organizzativi, evidenziati nel seguito, può certamente creare sinergie e agevolare lo sfruttamento della conoscenza aziendale sul tema.

Al 2022, in merito al rafforzamento delle competenze l'analisi della Figura 20 evidenzia che le iniziative di promozione di 'laboratori' di supporto per il cloud, l'adozione di un piano di formazione e lo sviluppo interno della conoscenza hanno coinvolto circa la metà del campione. In prospettiva al 2025, queste iniziative saranno sempre più diffuse, insieme all'assunzione di personale con competenze specifiche e alla creazione di una knowledge base.

Figura 20 – Interventi organizzativi per il rafforzamento delle competenze



Nella metà delle realtà bancarie si registra la presenza di un 'polo' di competenza per il cloud al 2022 e, in prospettiva nel triennio 2023-2025, la quota aumenterà fino al 75% (Figura 21). Come mostrato nel seguito, il 'polo' di competenza può aggregare conoscenze di diversa natura (tecnico-architetturali, gestionali, di governance, legali, etc.), con diversi modelli organizzativi (accentrato, distribuito e di tipo 'hub&spoke').

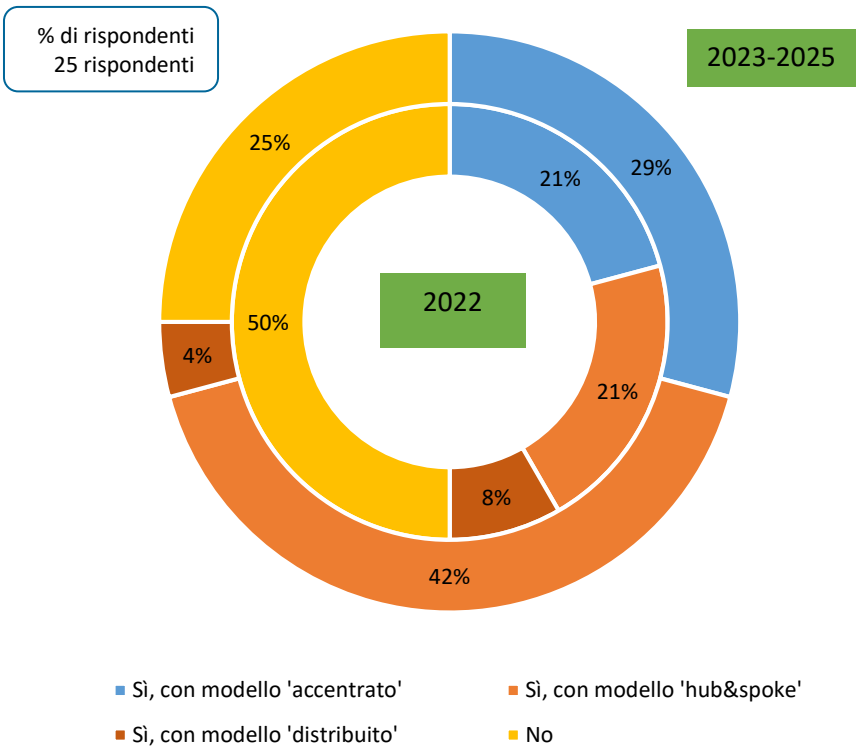
MODELLI DI RIFERIMENTO PER L'ORGANIZZAZIONE DEL "POLO" DI COMPETENZA

***Accentrato**: una struttura organizzativa accentrata agisce come centro di competenza per il cloud.*

***Hub&spoke**: esiste una struttura organizzativa formalizzata accentrata che agisce come "cabina di regia" e collabora con team competenti sul cloud, distribuiti in diverse funzioni aziendali.*

***Distribuito**: non è formalizzata una struttura organizzativa che agisce da cabina di regia ma le competenze sul cloud sono distribuite all'interno delle diverse funzioni aziendali.*

Figura 21 – 'Polo' di competenza per il cloud



Al 2022, come già evidenziato, la metà dei rispondenti ha formalizzato la creazione del 'polo' di competenza, in prevalenza con modello accentrato e modello hub&spoke (entrambi al 21%).

In previsione, nel triennio 2023-2025, le banche e i gruppi bancari ricorreranno perlopiù al modello hub&spoke, con una percentuale doppia rispetto al 2022 (42%). Il modello distribuito, senza cabina di regia, segnalato solo dall'8% del campione al 2022, scenderà nel triennio 2023-2025 al 4%.

Come riportato in Figura 22, la conformazione organizzativa del 'polo' di competenza può aggregare funzioni e conoscenze di diversa natura e dall'analisi emerge che sono presenti maggiormente le funzioni del comparto IT (tecnico-architetturale, gestione operativa, etc.).

Nella Figura 23 è possibile infatti osservare che le competenze presenti, per oltre l'80% del campione, riguardano soprattutto le architetture IT, la gestione dell'IT, la sicurezza IT. Non sono rappresentate le funzioni di business, coinvolte di volta in volta su specifica esigenza.

Figura 22 – Caratterizzazione 'polo' di competenza – funzioni rappresentate

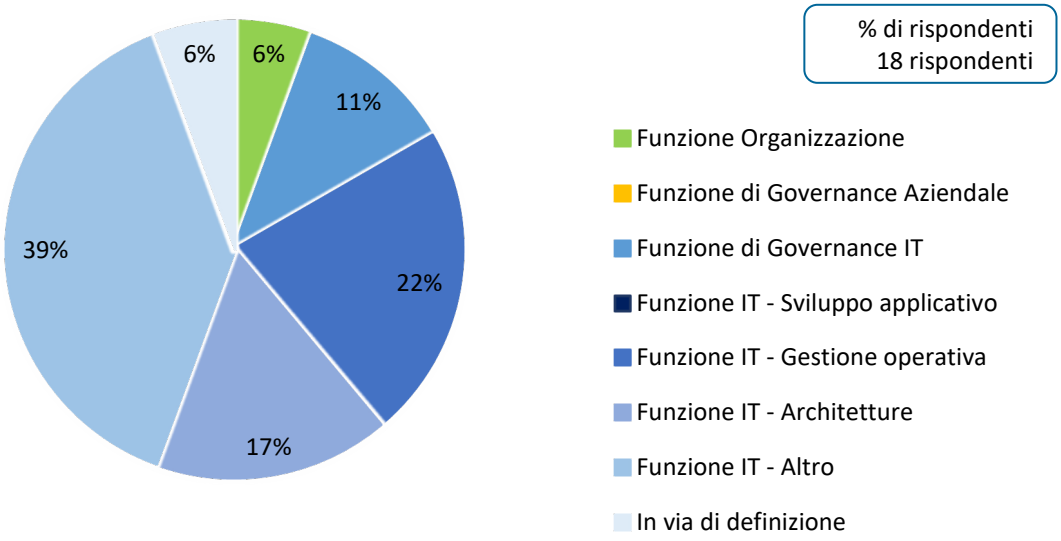
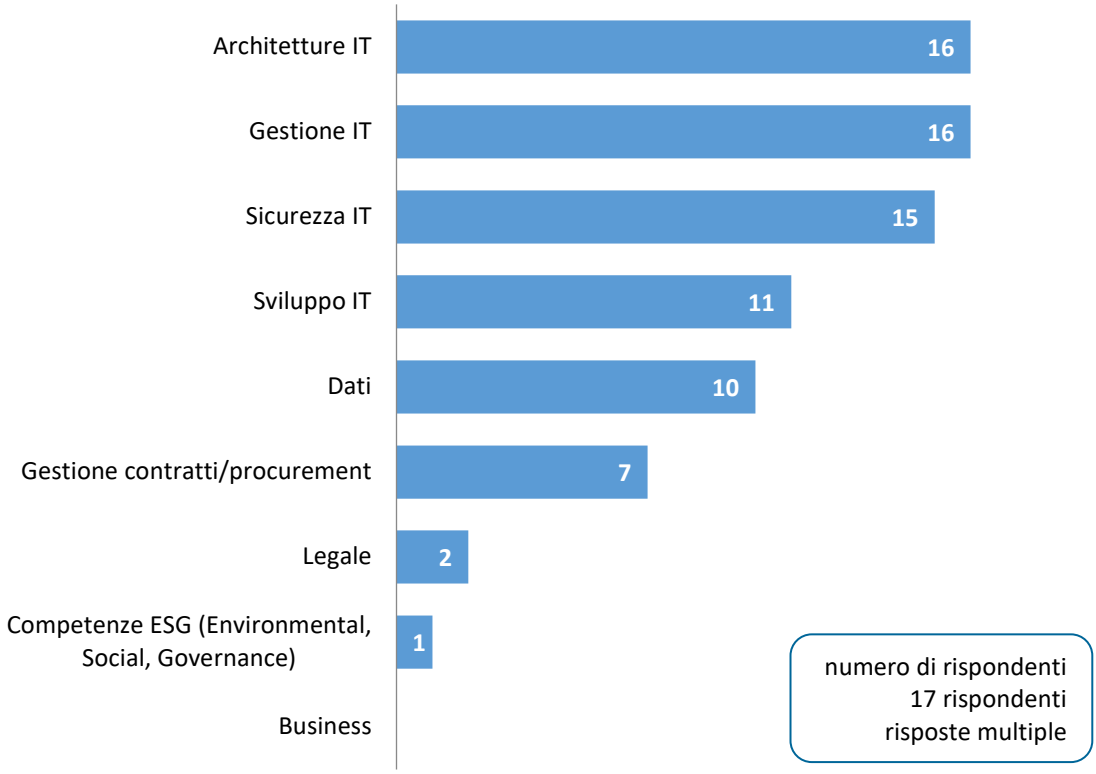
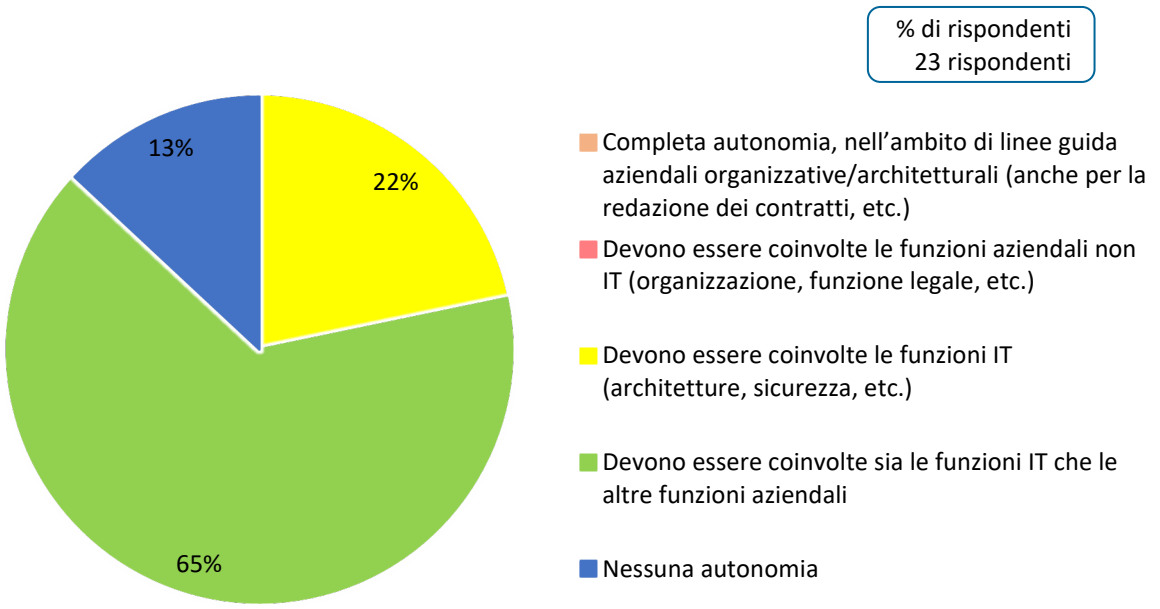


Figura 23 – Caratterizzazione del 'polo' – competenze presenti



Come emerge dal grafico della Figura 24, per l'adozione di soluzioni cloud, le funzioni di business non sono autonome ma devono coinvolgere altre funzioni aziendali, in particolare l'IT.

Figura 24 – Grado di autonomia del business per l'adozione di soluzioni cloud



2.3 Modelli cloud, ambiti IT e processi bancari coinvolti

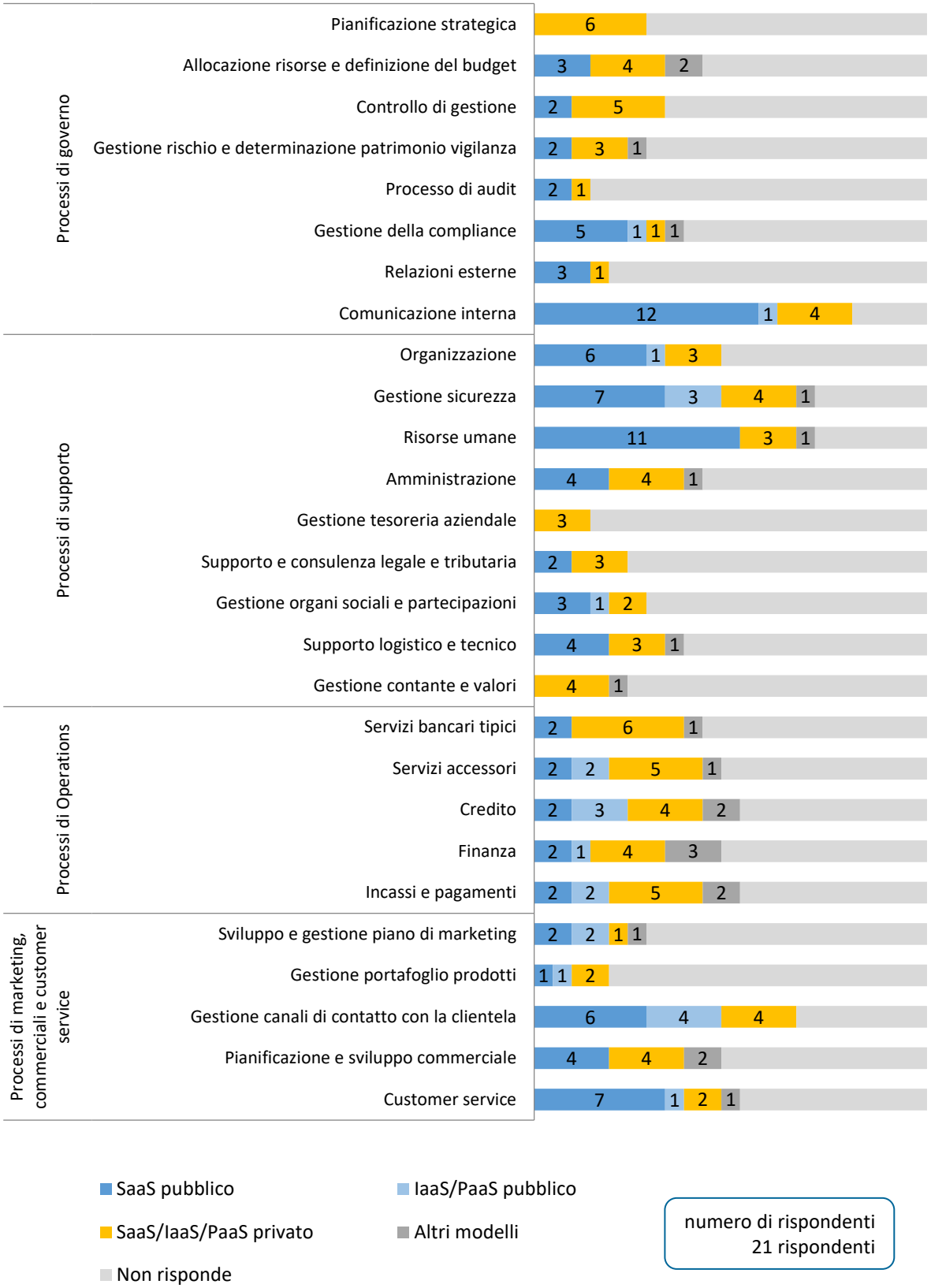
La scelta del service e del deployment model che meglio risponde alle esigenze del business è importante per garantire il successo e sfruttare pienamente i benefici di un servizio in cloud.

I grafici che seguono mostrano lo stato dell'arte nelle banche, sia per processi bancari che per ambiti e servizi IT, così da identificare quali di essi fruiscono del cloud e con quale modello (pubblico o privato, IaaS/PaaS o SaaS).

Nella Figura 25, con riferimento ai processi della mappa applicativa ABILab[7], è possibile osservare il posizionamento dei servizi e infrastrutture in cloud, pubblico o privato.

[7] Nei processi di supporto non è considerato 'Gestione sistemi informativi e telecomunicazioni' in quanto l'ambito IT (processi, servizi, etc.) viene poi approfondito nella Figura 27.

Figura 25 – Modelli cloud prevalenti per processi



In generale Comunicazione interna, Risorse umane, Gestione sicurezza, Gestione dei canali di contatto con la clientela sono i processi che beneficiano più diffusamente del ricorso al paradigma cloud; per quasi tutti è presente il cloud pubblico di tipo SaaS.

Nei processi di governo, il cloud pubblico appare più utilizzato del cloud privato in particolare per il processo di Comunicazione interna già citato (13 rispondenti) e nella Gestione della compliance (6); d'altra parte, il cloud privato risulta più diffuso rispetto al cloud pubblico, per circa il 30% del campione, in Pianificazione strategica. Anche per i processi di supporto si conferma la prevalenza del cloud pubblico, in particolare di tipo SaaS, che è maggiormente in uso per Risorse umane (11) già citato, Gestione sicurezza (10) e Organizzazione (7).

Nei processi di Operations invece il cloud privato, offrendo un'infrastruttura dedicata alla singola organizzazione e percepito quindi come più sicuro, è maggiormente diffuso rispetto al cloud pubblico, in particolare nei Servizi bancari tipici (6), Servizi accessori (5) e Incassi e pagamenti (5). Il cloud pubblico è comunque utilizzato in tutti i processi delle Operations.

Infine, per i processi di Marketing, commerciali e customer service, il cloud pubblico appare complessivamente più utilizzato del cloud privato e, in particolare, nella Gestione dei canali di contatto con la clientela (10) già citato e nel Customer service (8).

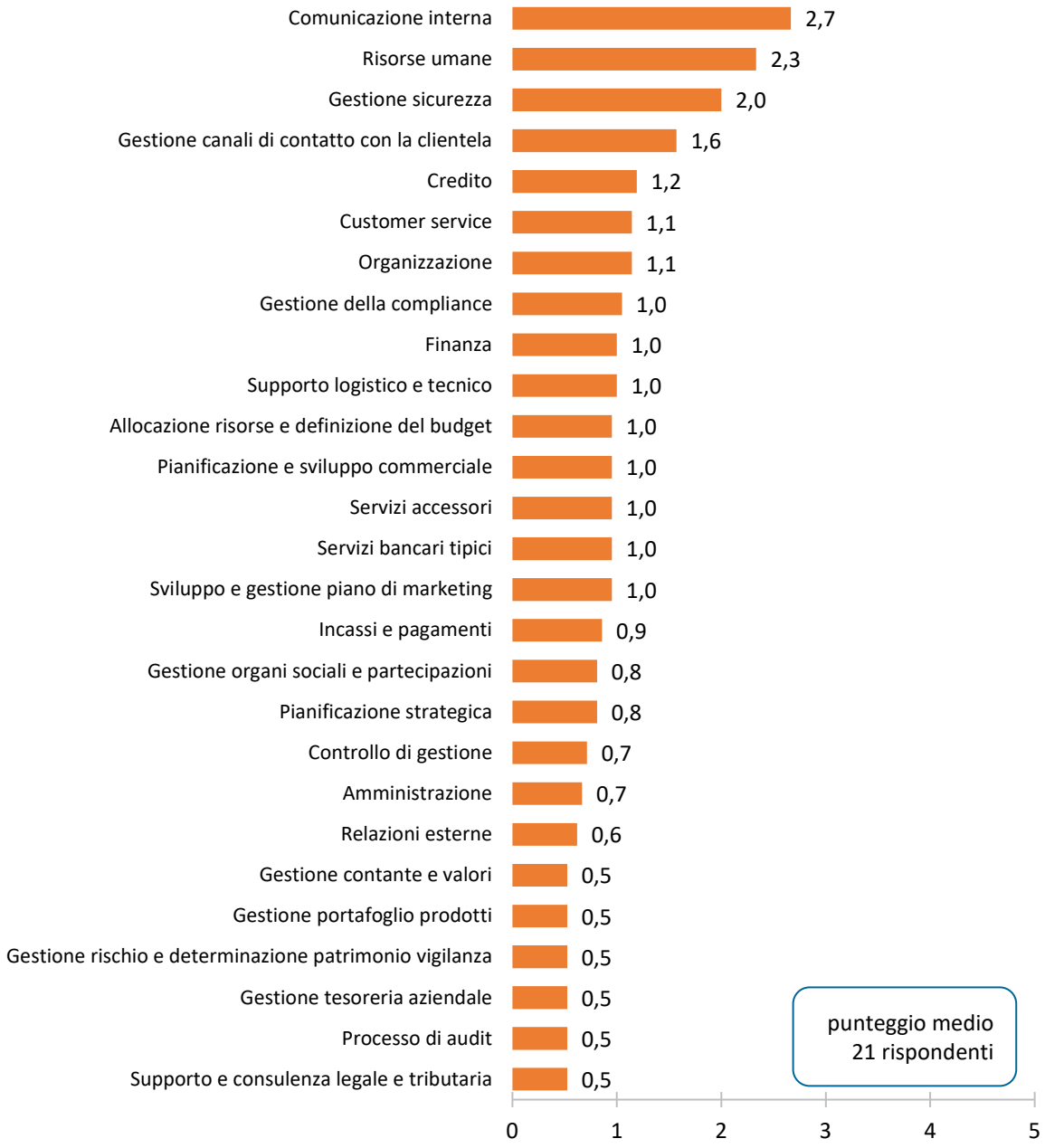
IL RICORSO AL CLOUD NELL'AREA OPERATIONS

Analizzando in dettaglio l'utilizzo del cloud nell'area funzionale che più da vicino riguarda il ***core business*** *della banca (Operations),* ***il 65% degli intervistati dichiara di far uso del cloud in almeno uno dei processi di quest'area****.*

Restringendo l'analisi ai soli rispondenti che ne fanno uso, anche se il ricorso al cloud pubblico risulta più frequente rispetto al modello privato, quest'ultimo è utilizzato mediamente a livelli maggiori (su una scala da 0 a 5, il livello medio di utilizzo è pari a 2,6 per il privato e a 1,7 per il pubblico).

Sulla base del calcolo del livello di adozione del cloud per tutti i processi bancari, in una scala crescente da 0 a 5 (cfr. note metodologiche) risulta il seguente ordinamento, che rafforza le precedenti considerazioni (Figura 26).

Figura 26 – Livello di adozione del cloud per processi bancari



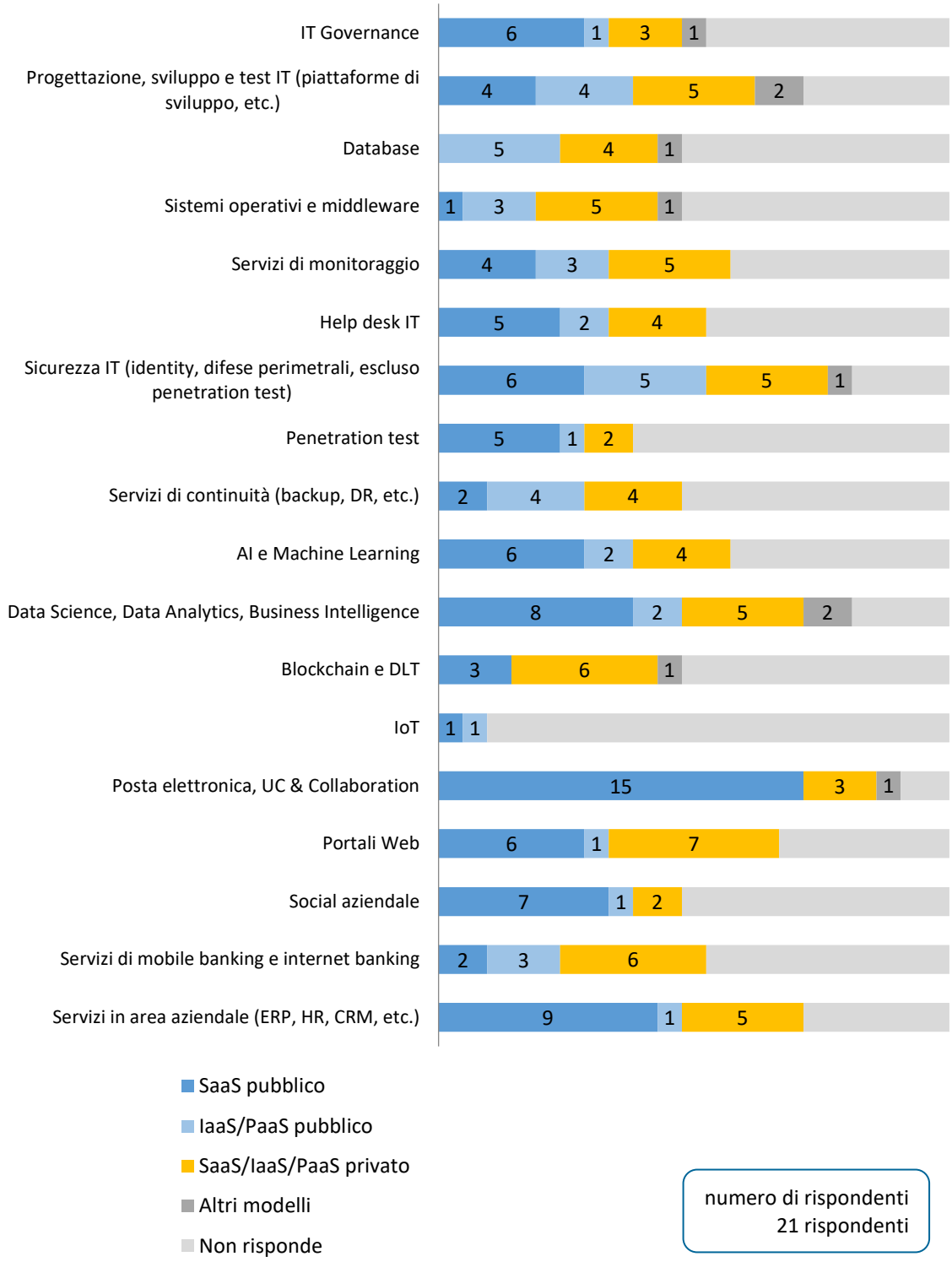
La Figura 27 indaga l'utilizzo del cloud negli ambiti e nei servizi IT. In generale il cloud pubblico, in particolare di tipo Saas, risulta più diffuso del cloud privato, ma si osserva comunque un utilizzo di quest'ultimo per taluni ambiti/servizi IT.

Considerando il solo ricorso a servizi SaaS su cloud pubblico, spiccano la posta elettronica e i servizi di collaboration (15 rispondenti), seguiti dai servizi in area aziendale (9) e quelli per l'analisi dei dati (8).

Se invece si osserva il solo ricorso al cloud privato, emerge che i portali Web (7), i servizi di mobile e Internet banking e blockchain/DLT vi ricorrono più di frequente (6).

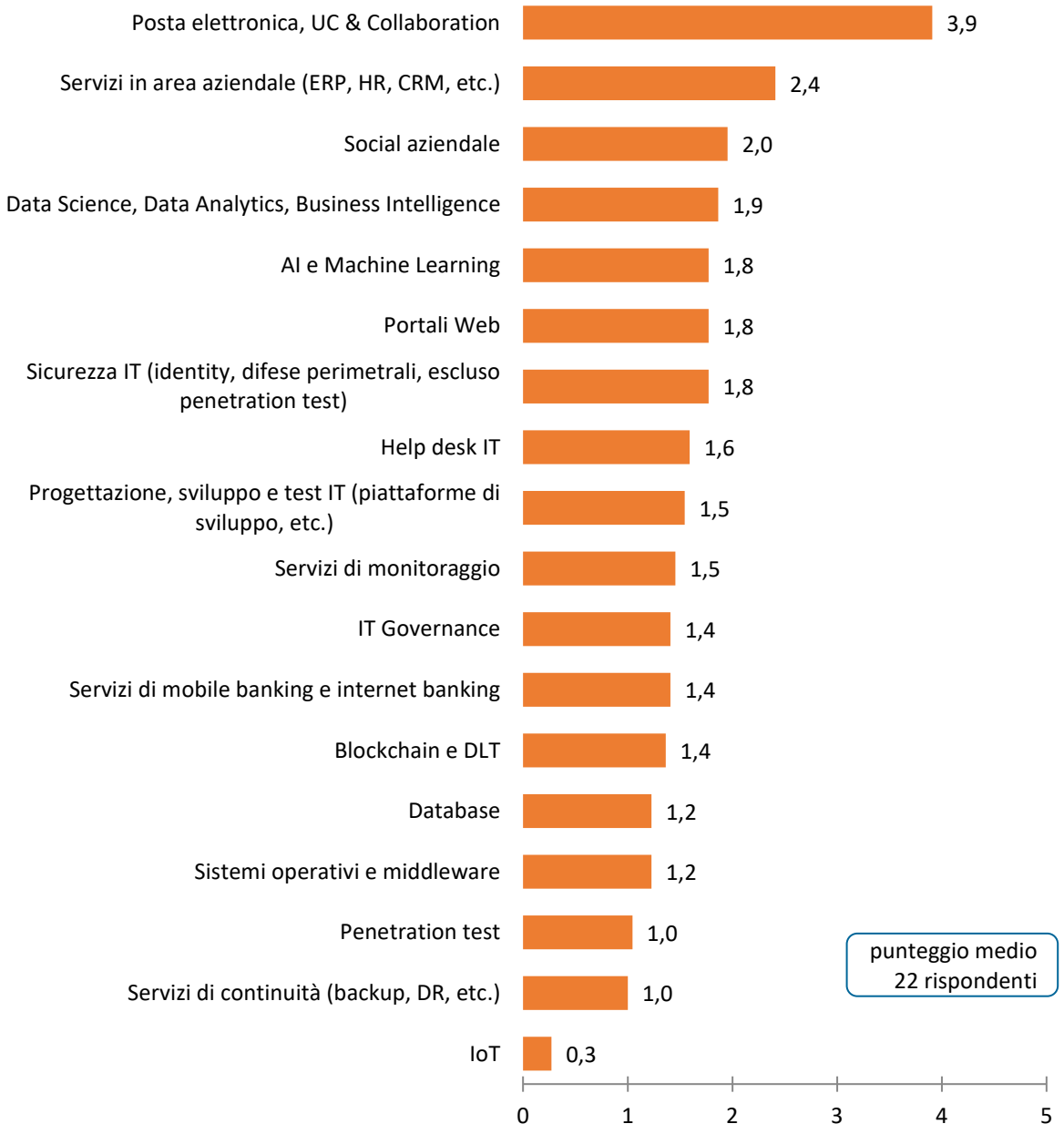
In generale, nel contesto delle nuove tecnologie (AI e ML, Data Science, Blockchain e DLT, IoT) sono utilizzati tutti i modelli di cloud ma è nell'ambito dell'analisi dei dati che ne emerge un uso più diffuso.

Figura 27 – Modello prevalente per ambiti/servizi IT



Sulla base del calcolo del livello di adozione del cloud, in una scala crescente da 0 a 5 risulta il seguente ordinamento degli ambiti/servizi IT (Figura 28).

Figura 28 – Livello di adozione del cloud per ambiti/servizi IT



Capitolo 3. Aspetti tecnologici e contrattuali

L'introduzione e l'evoluzione del cloud nelle banche comporta adeguamenti di natura organizzativa e tecnologica. Con riferimento ai 24 rispondenti che utilizzano il cloud, questo capitolo esamina gli interventi tecnologici attuati e necessari, gli approcci metodologici utilizzati nella migrazione delle applicazioni e taluni aspetti di sicurezza e di monitoraggio dei servizi.

A garanzia dell'affidabilità, sicurezza ed efficienza, all'interno degli accordi stipulati con i Cloud Service Provider (CSP) sono state esaminate le clausole contrattuali più rilevanti per le banche e il loro grado di diffusione all'interno dell'offerta di mercato dei CSP.

3.1 Interventi tecnologici per il cloud

In questo paragrafo viene fornita l'analisi degli interventi tecnologici attuati e previsti dalle banche e gli approcci metodologici utilizzati nella migrazione delle applicazioni al cloud.

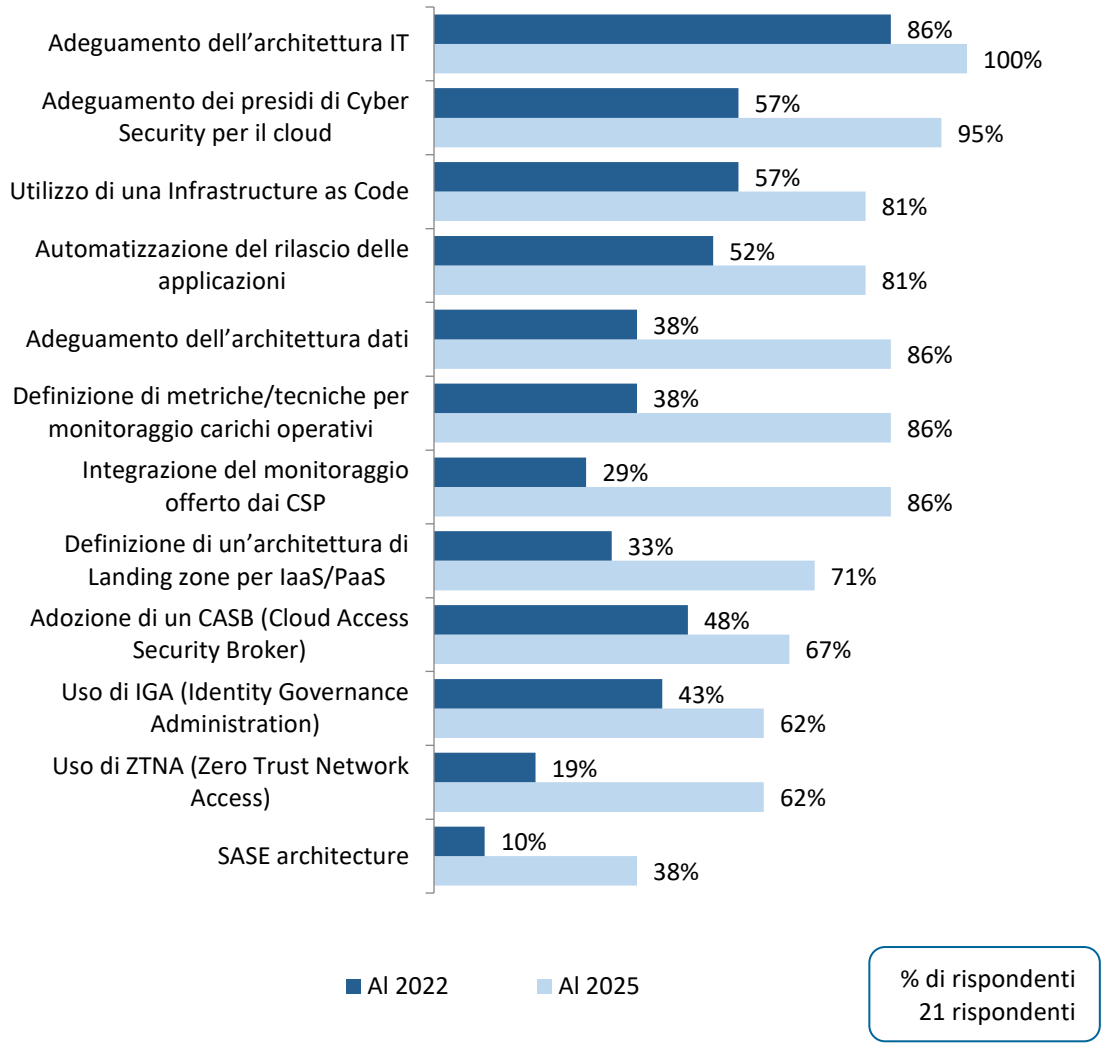
Dall'elenco degli interventi proposti nella Figura 29, i rispondenti hanno indicato quelli effettuati al 2022 e quelli previsti al 2025. Per l'86% del campione l'adeguamento dell'architettura IT per il cloud è l'intervento più di rilievo al 2022 e, in previsione, al 2025 tutti gli intervistati l'avranno realizzato. A seguire, l'adeguamento dei presidi di Cyber Security, l'utilizzo di una Infrastructure as Code[8] e l'automatizzazione del rilascio delle applicazioni, interventi già attuati al 2022 per oltre la metà dei rispondenti, e che al 2025 coinvolgeranno più dell'80% delle realtà bancarie.

Tra i principali interventi pianificati, per oltre l'80% del campione figurano anche l'adeguamento dell'architettura dei dati, la definizione di metriche/tecniche per il monitoraggio dei carichi operativi, l'integrazione del monitoraggio con quello offerto dai CSP, l'automatizzazione del rilascio delle applicazioni.

[8] Infrastructure as Code (IaC): approccio alla gestione e al provisioning dell'infrastruttura tramite codice anziché con processi manuali.

Interventi di tipo più strettamente tecnologico, quali la definizione di una Landing Zone per IaaS/PaaS[9], l'adozione di un CASB[10], l'uso di IGA[11], l'utilizzo di ZTNA[12], che non sono tra i più rilevanti al 2022, sono previsti al 2025 per oltre il 60% dei rispondenti.

Figura 29 – Interventi tecnologici per il cloud



Tra i più importanti temi affrontati dalle realtà bancarie vi è quello della migrazione delle applicazioni e dei dati verso il cloud. Non si tratta solo di spostare, ma soprattutto di modernizzare ed evolvere, rendendo più flessibili, integrati e agili i servizi offerti alla clientela. Per una vera

[9] 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).

[10] CASB (Cloud Access Security Broker) 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.

[11] IGA (Identity Governance and Administration) 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.

[12] ZTNA (Zero Trust Network Access) fornisce accesso remoto sicuro alle applicazioni, ai dati e ai servizi di un'organizzazione in base a criteri di controllo degli accessi chiaramente definiti.

trasformazione digitale, oltre che cogliere le opportunità offerte dalle nuove tecnologie è necessario ricercare la migliore efficienza operativa, flessibilità e agilità delle architetture applicative, così da essere pronti e tempestivi anche nel caso in cui i servizi debbano essere riportati all'interno della banca.

Tuttavia, la migrazione delle applicazioni al cloud deve tener conto della gestione della sicurezza dei dati e della scelta strategica della metodologia da utilizzare.

METODOLOGIE DI MIGRAZIONE DELLE APPLICAZIONI VERSO IL CLOUD

***Repurchasing**: le applicazioni aziendali sono sostituite da nuovi servizi SaaS in public cloud che hanno analoghe funzionalità.*

***Rearchitect**: prevede la riprogettazione dell'architettura applicativa e dei dati. Il codice viene riscritto mantenendo alcuni aspetti dell'architettura originale. Le applicazioni sono così pronte per essere spostate sul cloud e sfruttare appieno le funzionalità da esso offerte.*

***Cloud-native**: prevede la scrittura da zero dell'applicazione per adattarla alle architetture e ai servizi offerti dall'ambiente cloud. Il codice viene scritto in modo da sfruttare appieno le funzionalità cloud-native (es. funzioni serverless, container, architetture a microservizi).*

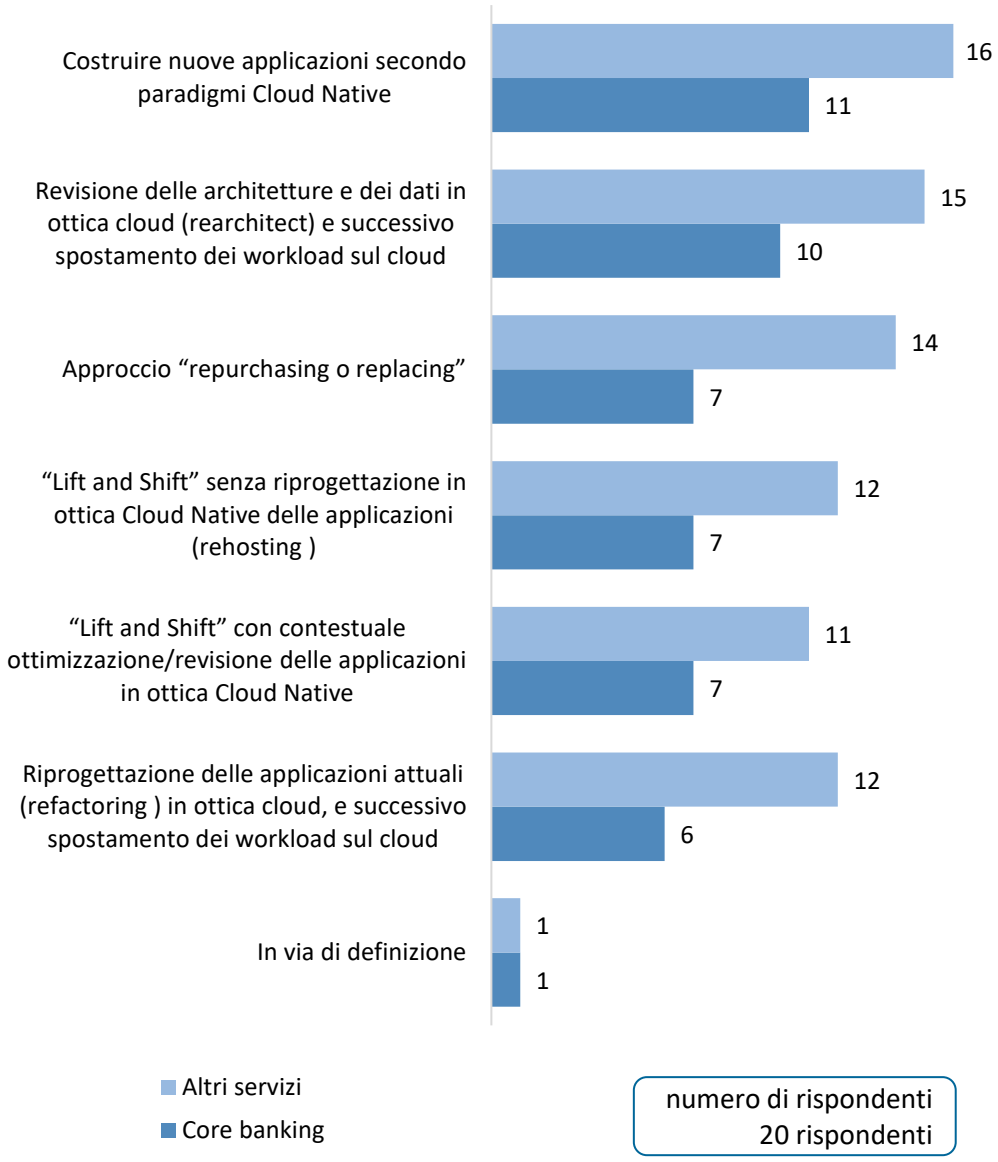
***Refactoring**: prevede che il codice sorgente venga ristrutturato e ottimizzato per migliorarne la qualità (modularità del codice, eliminazione di codice duplicato e ottimizzazione di query per migliorare le prestazioni). Il refactoring del codice è un'operazione meno invasiva del rearchitect ma può agire sulla scalabilità e semplificare la gestione in un ambiente cloud.*

***Lift and shift**: prevede il trasferimento dell'intero sistema esistente, senza apportare alcuna modifica al codice o all'architettura. Si 'alza' (lift) l'infrastruttura esistente e si 'sposta' (shift) nel cloud. Questo tipo di migrazione non sfrutta appieno i benefici del cloud ma può prevedere un successivo miglioramento delle applicazioni.*

Ai rispondenti è stato chiesto di indicare quali metodologie della Figura 30 sono impiegate per la migrazione delle applicazioni. Tra quelle in elenco, che risultano tutte utilizzate, la costruzione di nuove applicazioni secondo paradigmi di tipo cloud-native è la metodologia più diffusa, sia per il core banking che per gli altri servizi, seguita dall'approccio 'rearchitect'.

Approfondendo ulteriormente l'analisi, risulta che il 75% dei 20 rispondenti utilizza almeno una metodologia in elenco per il core banking.

Figura 30 – Metodologie migrazione delle applicazioni al cloud



3.2 Aspetti di sicurezza nell’adozione del cloud

Come noto, la sicurezza nel cloud pubblico è un tema di estrema importanza, considerato che i presidi adottati non sono completamente sotto il dominio dell’organizzazione ma dipendono dagli assetti impiegati dal fornitore.

L'accesso non autorizzato ai dati, l’intercettazione di dati sensibili durante la trasmissione o l’utilizzo improprio di dati e altre minacce richiedono misure robuste quali l’uso della crittografia, la protezione delle applicazioni e dei sistemi, la sicurezza fisica dei data center.

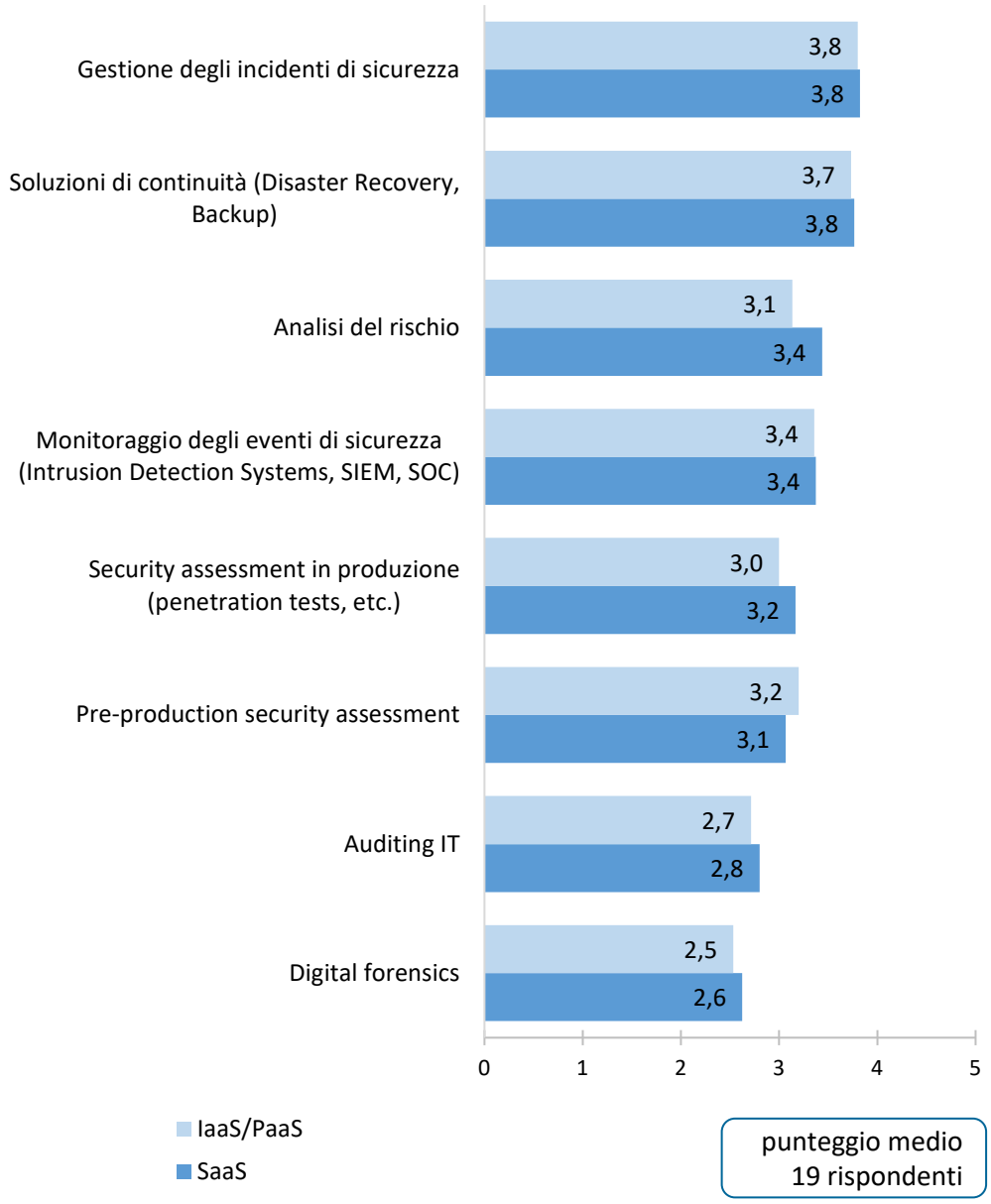
Questa Rilevazione non approfondisce gli specifici assetti di sicurezza menzionati, dipendenti dalla tipologia del servizio esternalizzato, ma tratta il tema della sicurezza in generale. Alcuni interventi infrastrutturali sono già stati evidenziati nella Figura 29 del precedente paragrafo; nel successivo

verrà proposto l'esame delle specifiche clausole contrattuali con i CSP anche per l'area della sicurezza.

Dall'analisi condotta, emerge la percezione e soddisfazione delle banche per i principali processi di sicurezza attuati in collaborazione con il fornitore.

La Figura 31 mostra il grado di soddisfazione degli intervistati, per tutti i service model, in una scala crescente da 0 a 5. Il livello di soddisfazione risulta medio-alto per tutti i processi di sicurezza elencati, a esclusione di auditing IT e digital forensics, a livello medio.

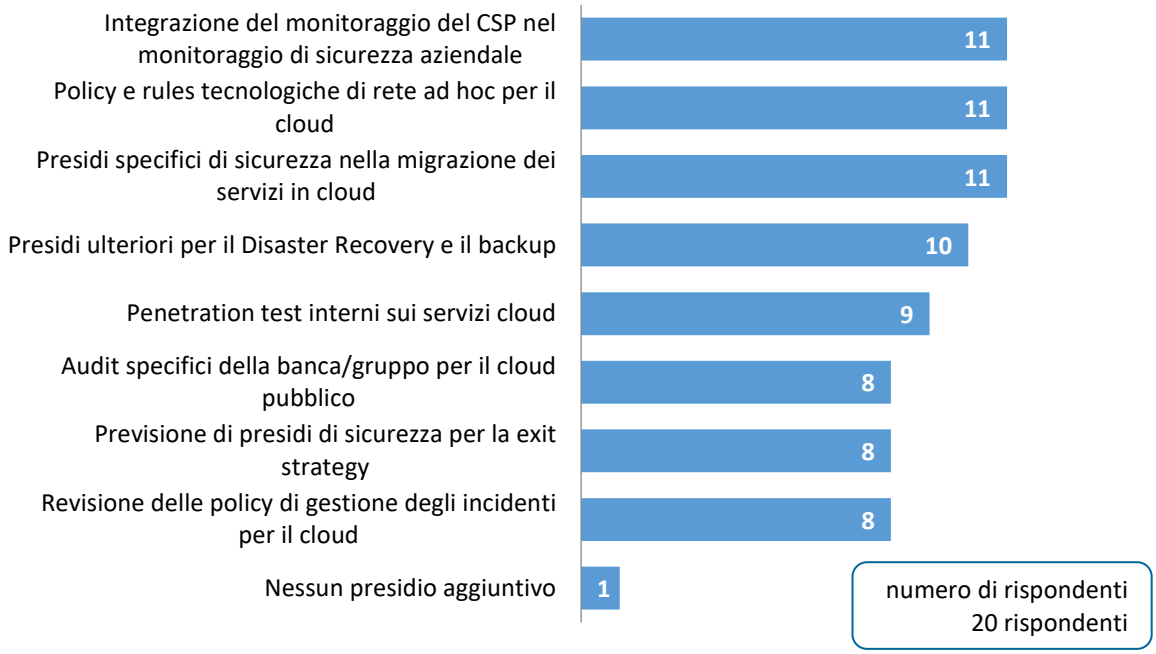
Figura 31 – Livello di soddisfazione dell'offerta dei CSP per i processi di sicurezza



Alle banche è stato chiesto di indicare quali presidi di sicurezza aggiuntivi sono presi in considerazione al proprio interno, a complemento di quelli presenti nell'offerta dei CSP. Emerge che l'integrazione del monitoraggio interno con quello del CSP, le policy e regole di rete e i presidi di sicurezza nella migrazione dei servizi in cloud sono tenuti in maggior conto da oltre la metà dei

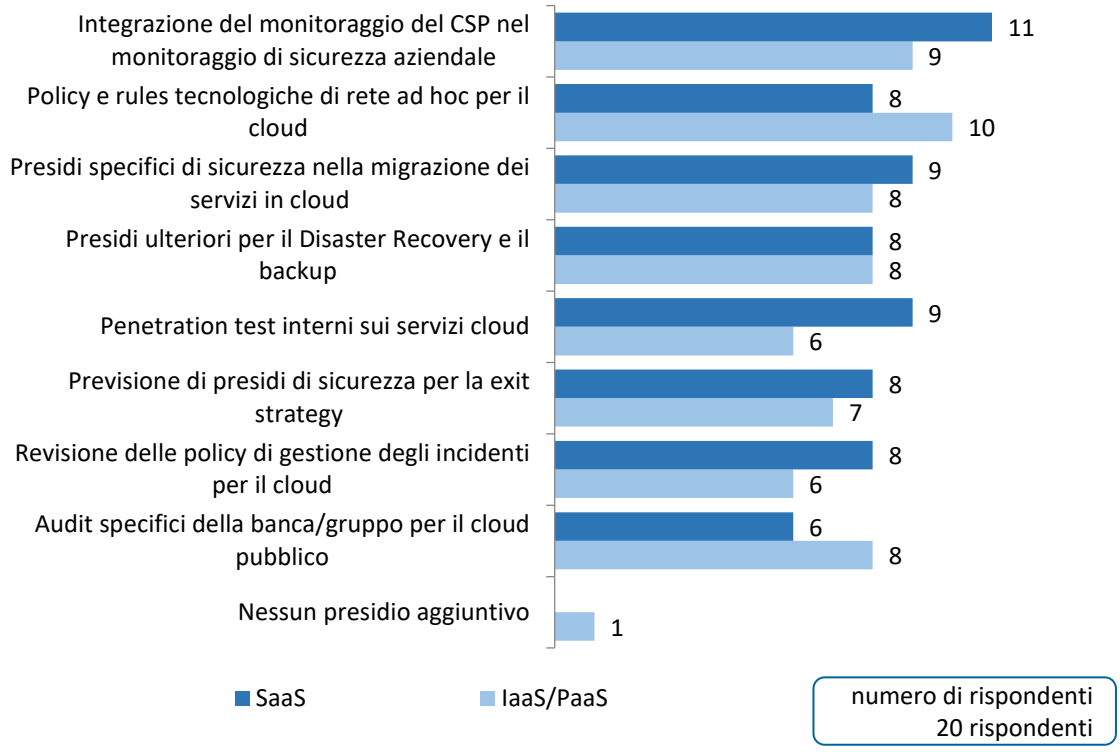
rispondenti. Solo un rispondente dichiara di non considerare presidi di sicurezza aggiuntivi (Figura 32).

Figura 32 – Presidi di sicurezza aggiuntivi



Nella Figura 33 la stessa analisi è riproposta distinguendo per modelli SaaS e IaaS/PaaS.

Figura 33 – Presidi di sicurezza aggiuntivi per SaaS, IaaS/PaaS

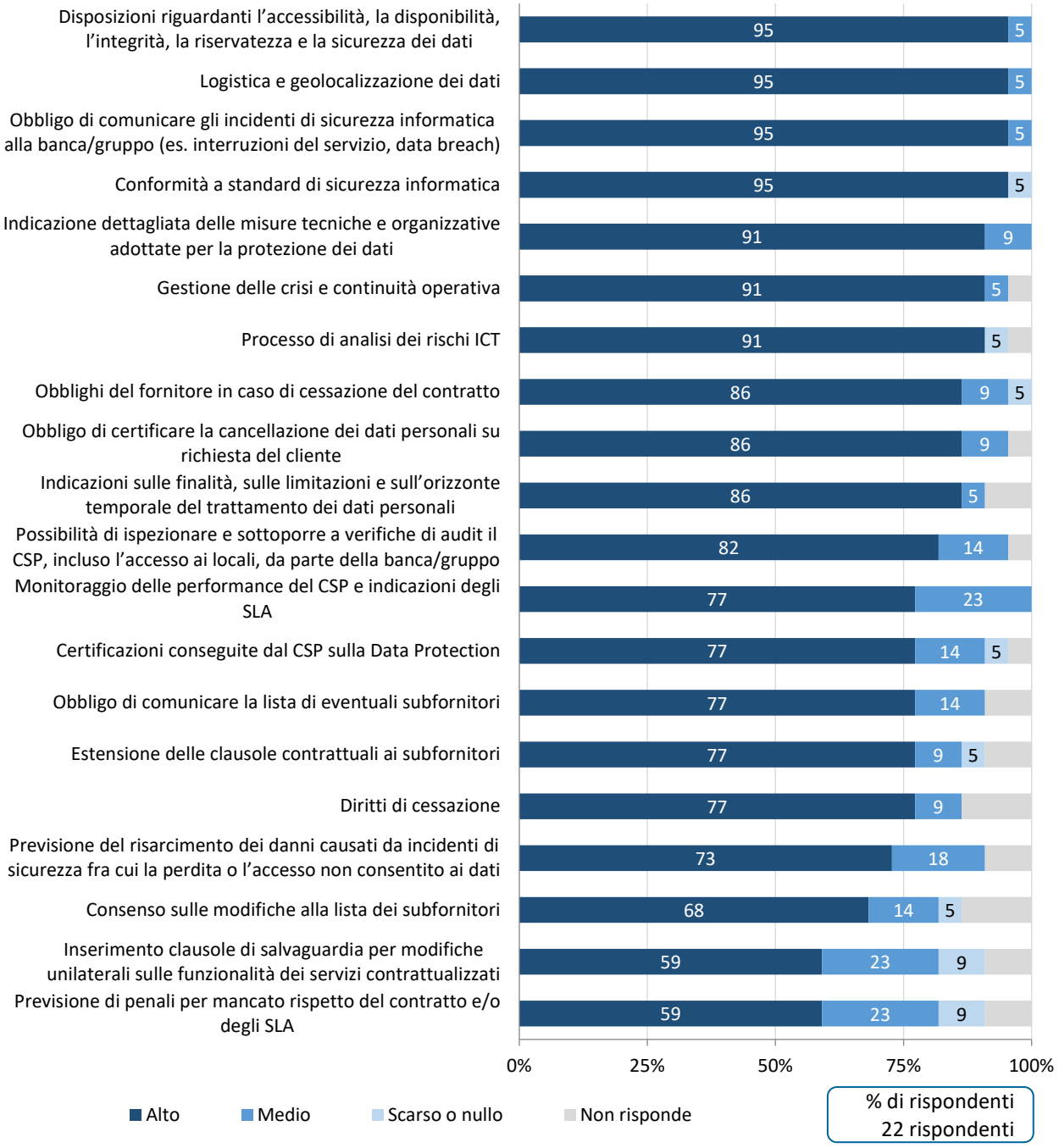


3.3 Clausole contrattuali per il cloud

Il profilo legale rappresenta un tema rilevante per il settore bancario, che può risolvere alcune criticità riguardanti l'acquisizione dei servizi in cloud, quali la sicurezza e i livelli di servizio, anche attraverso la redazione di opportuni contratti con i fornitori.

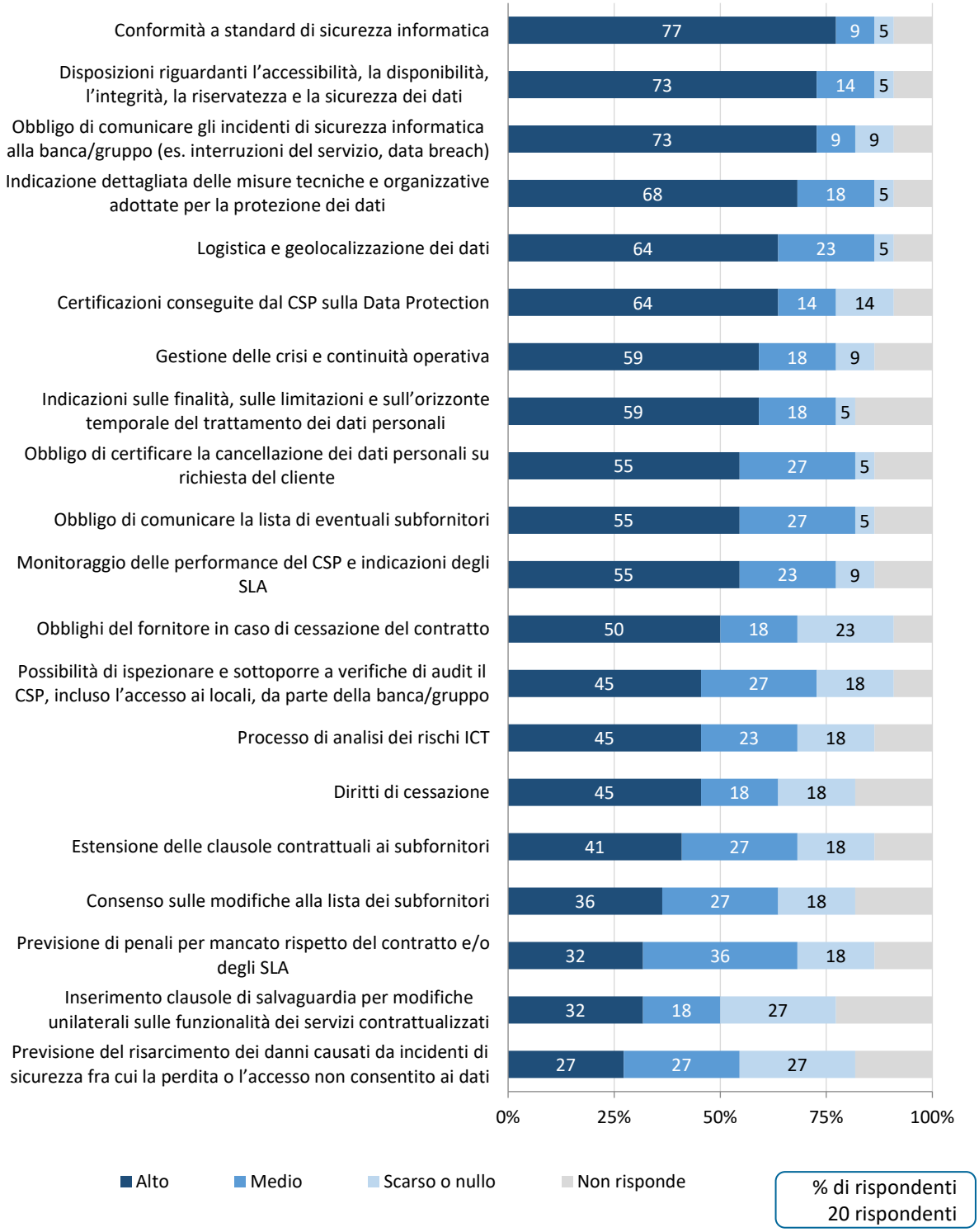
Nella Figura 34 è stata analizzata la rilevanza dei principali requisiti ai fini della stipula dei contratti. In generale, emerge una forte esigenza di ottenere garanzie da parte del fornitore per tutte le clausole contrattuali qui esaminate, indicate con livello di rilevanza medio o alto per oltre il 70% dei rispondenti. In particolare, l'esigenza è avvertita a livello alto dal 95% dei rispondenti in tema di sicurezza dei servizi e dei dati, di logistica e geolocalizzazione, di segnalazione degli incidenti e di conformità agli standard di sicurezza dei servizi.

Figura 34 – Livello di rilevanza clausole/requisiti contrattuali



La Figura 35 mostra la diffusione, nell'offerta dei CSP, dei requisiti contrattuali precedentemente indicati.

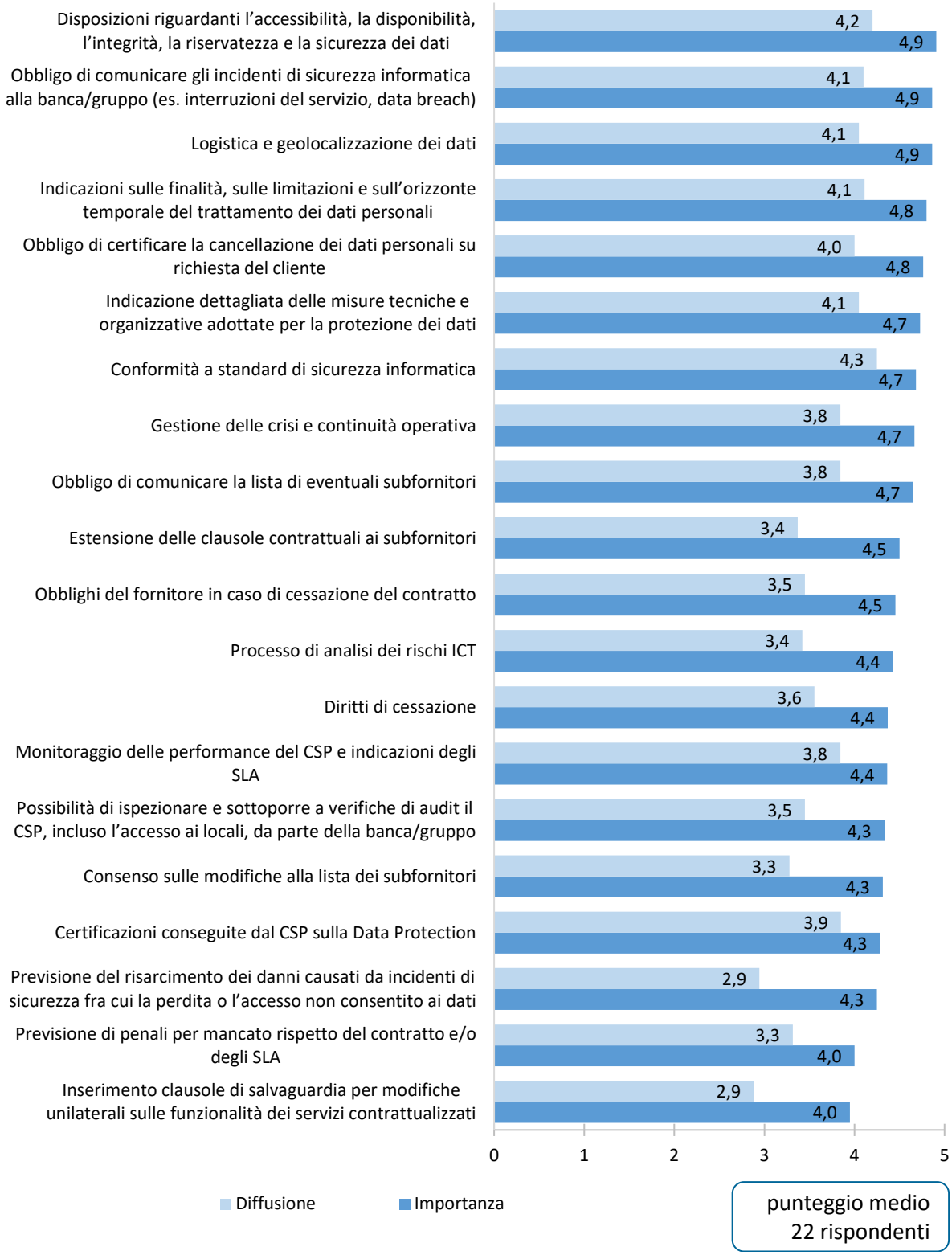
Figura 35 – Livello di diffusione clausole/requisiti contrattuali



Nella Figura 36, dall'analisi dei livelli, in una scala crescente da 0 a 5, emerge l'ordinamento dei requisiti per importanza insieme al corrispondente livello di diffusione. Le clausole di previsione del risarcimento dei danni causati da incidenti di sicurezza e l'inserimento di clausole di salvaguardia

per modifiche unilaterali di contratti mostrano il gap più elevato tra livello di importanza e diffusione.

Figura 36 – Confronto del livello di importanza/diffusione delle clausole contrattuali



CONFRONTO CON RILEVAZIONE TECNOLOGICA CIPA 2015

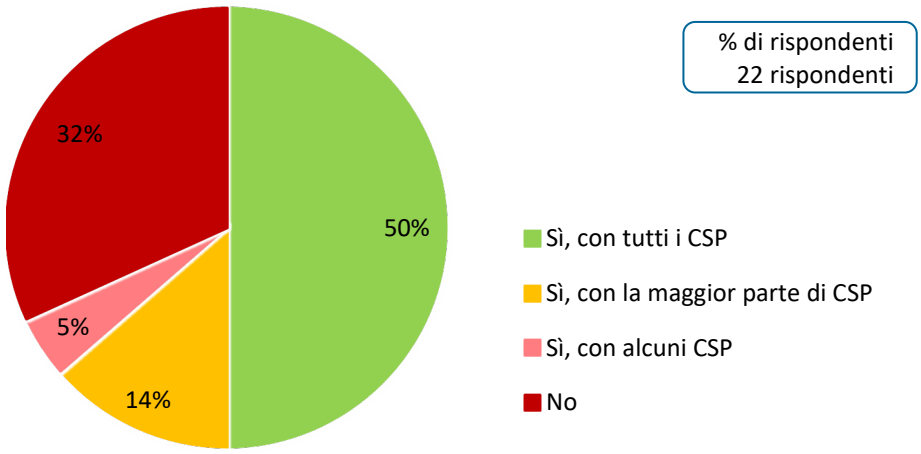
Il confronto dei dati attuali con quelli della Rilevazione Tecnologica CIPA 'Il cloud e le banche' del 2015 fa emergere oggi un quadro decisamente più maturo rispetto all'adozione di servizi in cloud pubblico da parte delle realtà bancarie.

In particolare, circa la percezione del livello di diffusione nell'offerta dei CSP delle clausole contrattuali necessarie si evidenzia un deciso salto in avanti, anche grazie all'impulso dato in tal senso dalla normativa di settore.

Infatti, ad esempio, la clausola di 'Obbligo di certificare la cancellazione dei dati personali su richiesta del cliente', che nel 2015 era valutato irrinunciabile dal 73,3% del campione, e segnalato allora con diffusione alta dal 27,3% dei rispondenti, scarsa o nulla dal 36,4%, al 2022 vede oltre la metà dei rispondenti dichiararla con diffusione alta o media e, solo il 5% dei rispondenti, scarsa o nulla. In generale, nel 2015 solo pochissime clausole esaminate erano percepite come altamente diffuse (e quindi i requisiti ben trattati nei contratti), al 2022 ciò si verifica per la maggior parte delle clausole contrattuali.

Dopo aver analizzato i requisiti più importanti ai fini della stipula dei contratti per l'acquisizione di servizi in cloud e rilevata la forte esigenza di ottenere garanzie contrattuali da parte del fornitore, è possibile comprendere come sia spesso necessario definire delle policy ad hoc per i contratti. Circa i due terzi dei rispondenti hanno adottato tali policy: la metà degli intervistati con tutti i CSP, il 14% con la maggior parte e il 5% con alcuni provider (Figura 38).

Figura 37 – Adozione di policy ad hoc per i contratti



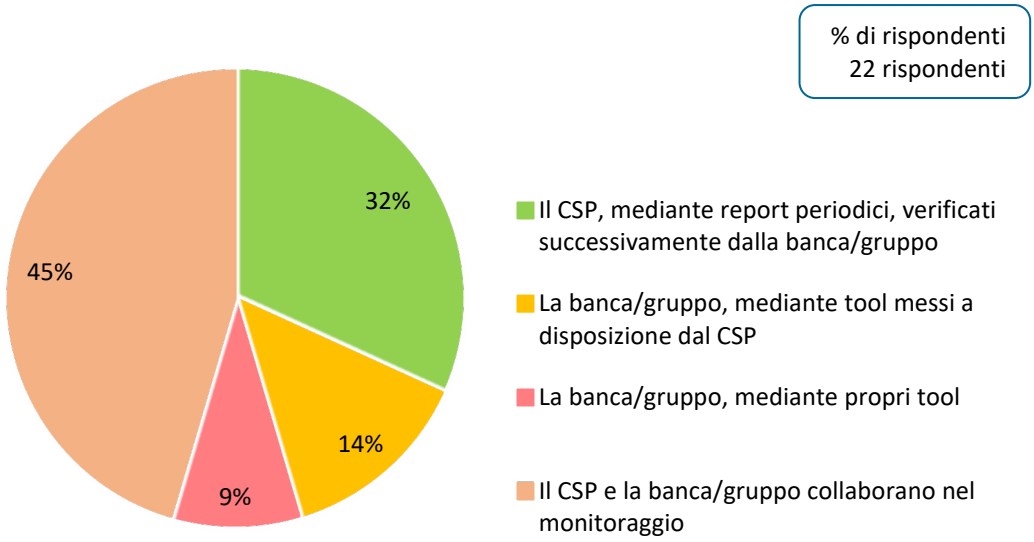
3.4 Livelli di servizio nel cloud

Un altro aspetto importante riguarda i livelli di servizio offerti dal fornitore per i servizi in cloud, che devono essere opportunamente monitorati.

La Figura 38 riporta le modalità con le quali le banche eseguono tale monitoraggio. Circa il 90% dei rispondenti dichiara di avvalersi, a vario titolo, del fornitore: il 45% asserisce che il CSP e la banca/gruppo bancario collaborano, il 32% che il monitoraggio è attuato dal CSP, salvo verifica a

posteriori da parte della banca, il 14% esegue il monitoraggio mediante tool messi a disposizione dal CSP.

Figura 38 – Monitoraggio degli SLA per i servizi cloud



Indice delle figure