DORA: PRONTI? VIA!

Romano STASI

*Segretario Generale Consorzio **ABI Lab** Direttore Operativo **CERTFin***

Osservatorio DORA C&R

ABI Lab

2020 - 2024

Evoluzione dalla Business Continuity alla Resilienza Operativa, poi integrata con le direttive del DORA per gli ambiti digitali.

Partecipano 22 Entità Finanziarie (banche, assicurazioni, ..)

L'Osservatorio ha condotto **Ricerche, Studi, Survey e approfondimenti metodologici a supporto dell'adozione della resilienza in banca,** conformemente al regolamento DORA

- Monitoraggio degli **sviluppi normativi** (DORA, RTS, EBA GL…)
- **Confronto differenziale del DORA** rispetto alla normativa preesistente (inclusa l'implementazione nazionale delle EBA GL)
- Censimento dei **deliverable richiesti da DORA** (Politiche, Piani, Processi, Framework, Strategie, Analisi, Registri, ...)
- **Indagine annuale** sull'evoluzione verso la Resilienza
- How To e Supporto all'implementazione di DORA: Il **B**usiness **R**esilience **F**ramework
- Approfondimenti su **temi di interesse** (terze parti, mappatura e analisi dei rischi, ...)
- Punti di attenzione nella **interpretazione e implementazione dei requisiti normativi**

Con il supporto di 8 partner tecnologici

Risultati del confronto DORA – 285/EBA GL

In totale sono stati analizzati 236 requisiti del DORA

	59 punti di confronto	96 punti di confronto	81 punti di confronto	TOTALE: 236 punti di confronto
Capo II – Gestione dei rischi informatici	43	39	27	**109**
Capo III – Gestione, degli incidenti informatici	11	5	12	28
Capo VI – Test di resilienza operativa digitale	0	5	26	31
Capo V – Gestione dei rischi informatici derivanti da terzi	5	47	10	**62**
Capo VI – Meccanismi di condivisione delle informazioni	0	0	6	6

Risultati del confronto DORA – 285/EBA GL

Capo VI – Meccanismi di condivisione delle informazioni

I temi presenti all'interno del Capo VI, applicabili su base volontaria, sono un **nuovo elemento** introdotto dal DORA.

Tuttavia, in Italia, i meccanismi di condivisione delle informazioni e delle analisi delle minacce informatiche sono regolati dal **CERTFin**.

Le entità finanziarie, quindi, non devono implementare nessuna azione per adeguarsi agli obblighi introdotti.

CERTFin

Tra gli obiettivi del CERTFin:

- Costituire un Single Point of Contact (PoC) per il settore finanziario
- Promuovere la cooperazione pubblico-privato e intersettoriale
- Favorire lo scambio di informazioni su incidenti, minacce informatiche, vulnerabilità e lezioni apprese

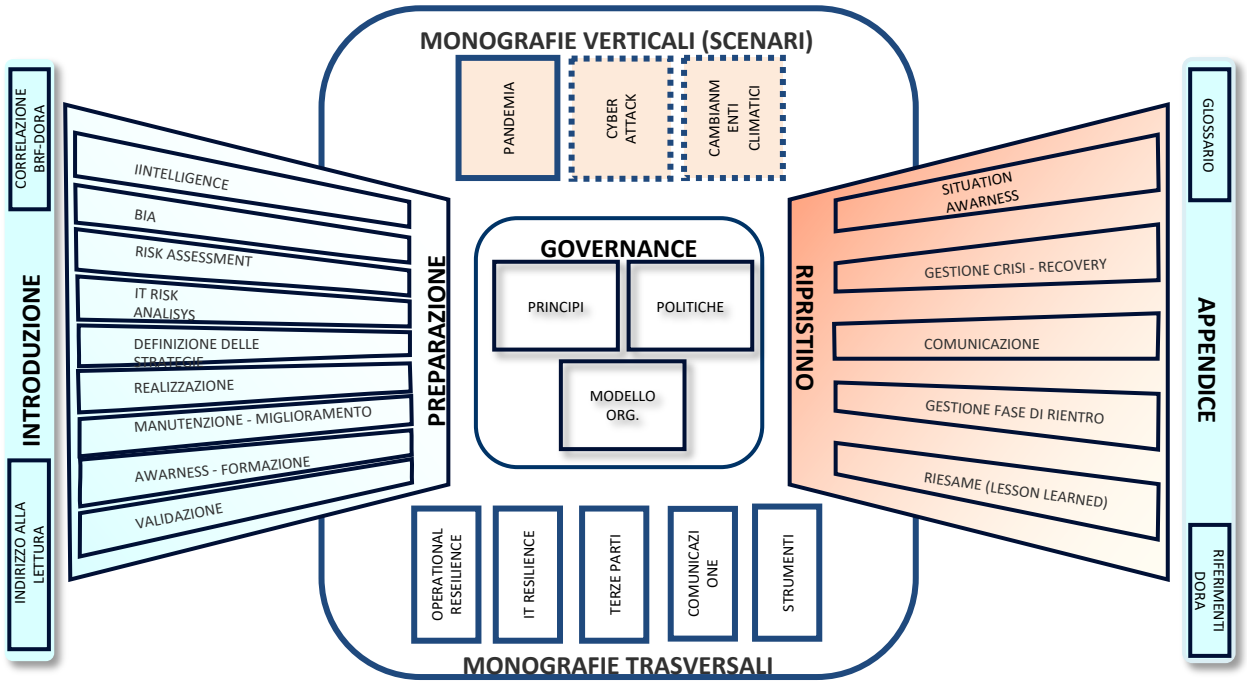
Business Resilience Framework

OBIETTIVI:

- Approccio pragmatico e flessibile alla Resilienza Operativa
- Evoluzione della Business Continuity integrando principi di **Resilience**
- Attenzione alla gestione di tutte le funzioni aziendali e di **ogni incidente**
- Integrazione dei principi del **DORA** ampliandone il campo d'azione verso la **resilienza complessiva** (non solo digitale)

COME :

- Collezione di autonomi **Playbook** operativi**, ciascuno con la medesima struttura,** navigabile in orizzontale per fase e in verticale (per tema di interesse)
- **Modello di resilienza** efficiente nella sua gestione ed efficace nella sua **applicazione in caso eventi (avversi)**
- **Riferimenti puntuali** ai requisiti **DORA** (articolo e paragrafo) e **Tabelle di correlazione** DORA/RTS con i singoli PlayBook
- Completato da **monografie** tematiche e trasversali



ESITI:

MAGGIORI INTEGRAZIONI IN:

- 2: Governance
- 3.4: IT Risk Analisys
- 3.3: Risk Assessment
- 3.8: Validazione
- 3.6: Realizzazione
- 4.4: Comunicazione

Integrate le sezioni dedicate alle **Terze Parti** in tutti i Playbook

ELEMENTI INNOVATIVI:

- **Intelligence** a supporto delle analisi del **rischio** e alla Due Diligence nella **selezione dei fornitori**
- Attenzione **all'IT risk analisys**
- **Situational awareness** per una risposta su misura dell'incidente

DORA ed il BRF

DORA		Capitoli BRF														
		GOV	PREPARAZIONE									RISPOSTA E RIPRISTINO				
CAPO		2	3.1	3.2	3.3	3.4	3.5	3.6	3.7	3.8	3.9	4.1	4.2	4.3	4.4	4.5	4.6
		Governance	Intelligence	BIA	Risk Assessement	ICT Risk Analysis	Strategie	Realizzazione	Awareness e Formazione alla resilienza	Test e Validazione	Manutenzione e miglioramento continuo	Risposta e ripristino	Situational Awareness	Escalation, gestione e recovery	Gestione della comunicazione	Gestione fase di rientro	Riesame
2	ICT RISK MANAGEMENT	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
3	ICT MAJOR INCIDENT REPORTING	X		X	X			X		X			X	X	X	X	X
4	TESTING									X							
5	THIRD-PARTY RISK	X	X	X	X	X	X	X		X					X		

Le Monografie del BRF

- Resilienza e Comunicazione
- Resilienza IT
- Resilienza Operativa
- Resilienza Terze parti
- Scenario Pandemico

Le trovate qui

https://www.abilab.it/web/guest/brf-monografie

Prossimamente: Altri scenari

(Cambiamenti climatici, Cyber attack, …)

DORA si appoggia su RTS/ITS/Guidelines alcune in corso di approvazione

Entrata in vigore del Regolamento DORA: **Gennaio 2023**

	AVVIO CONSULTAZIONE	DRAFT FINALE	APPROVAZIONE
• RTS on classification of major incidents and significant cyber threats • RTS to specify the policy on ICT services supporting critical or important functions • *ITS on Register of Information* • RTS on ICT Risk Management Framework	GIUGNO 2023	GENNAIO 2024	MARZO 2024 tranne l'ITS
• RTS and ITS on the content, format, templates and timelines for reporting major ICT-related incidents and significant cyber threats; • Guidelines on the estimation of aggregated costs/losses caused by major ICT-related incidents • RTS to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions • RTS on threat-led penetration testing (TLPT)	DICEMBRE 2023	LUGLIO 2024	?????
• DRY RUN sul registro di tutti gli accordi contrattuali sull'utilizzo dei servizi ICT da fornitori di servizi ICT di terze parti	MARZO 2024	DICEMBRE 2024	
• Valutazione della fattibilità per HUB unico dell'UE per la segnalazione di incidenti ICT (DORA Art.21.1). (ESAa in consultazione con BCE e ENISA)	LUGLIO 2024	GENNAIO 2025	?????

Due anni per adeguarsi ma diversi requisiti sono definiti nei **R**egulatory **T**echnical **S**tandard, alcuni dei quali non ancora approvati e disponibili in draft finali solo dallo scorso luglio

Avvio della applicazione di DORA: **Gennaio 2025**

Adeguamento al DORA (rilevazione 2024 su dati 2023)

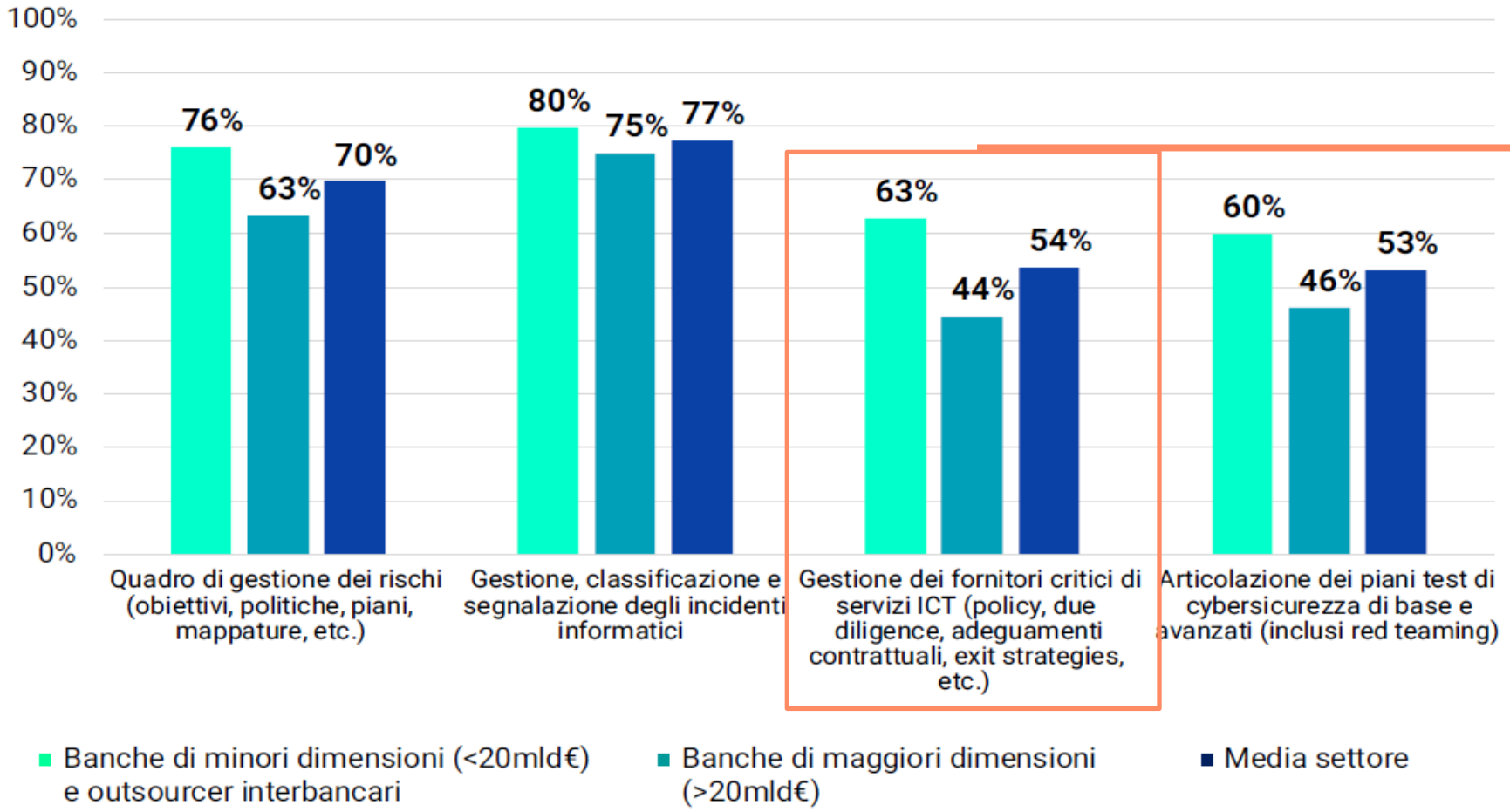


Figura 2.7.2

Grado di copertura dichiarato dalle banche italiane in relazione ad alcuni requisiti previsti dal DORA, a un anno dalla sua piena applicazione

Fonte: ABI Lab, Rilevazione sulle priorità ICT delle banche italiane, marzo 2023, 18 rispondenti

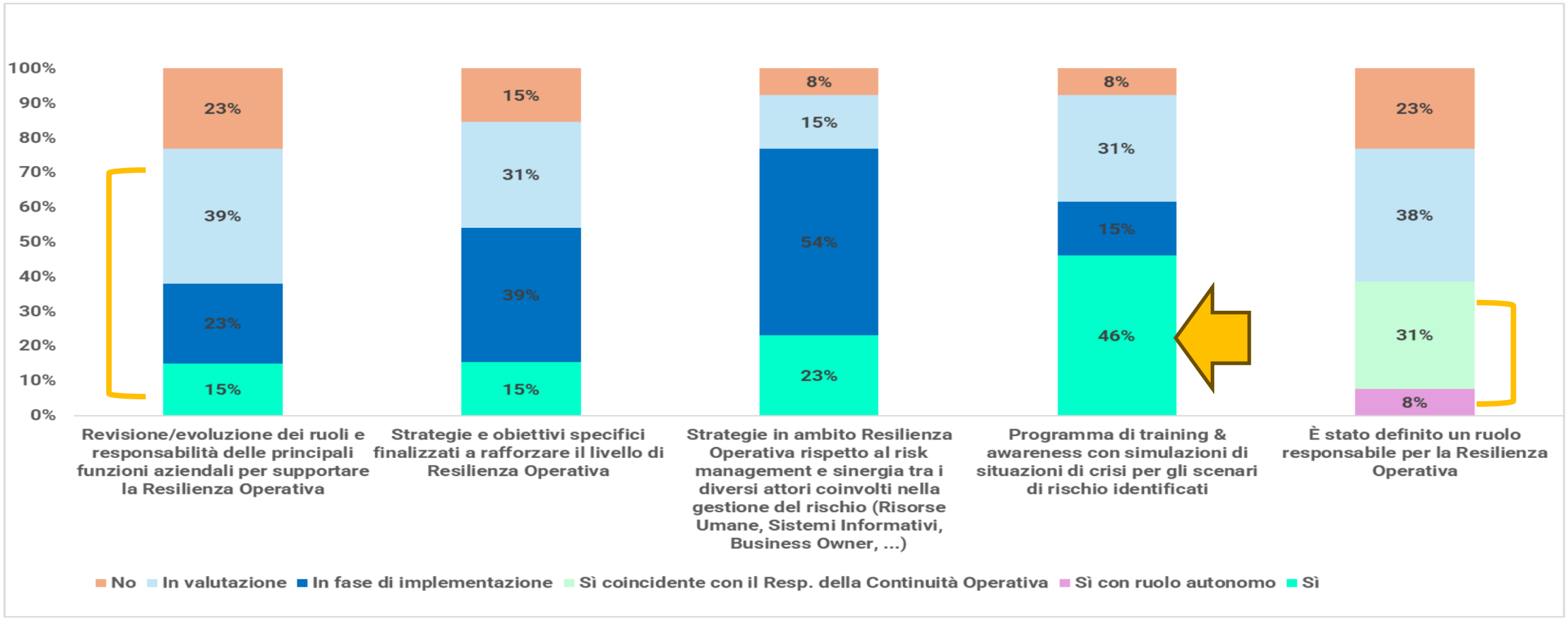
L'implementazione dei requisiti relativi alla gestione dei fornitori è meno avanzata che in altri ambiti.

Sono state segnalate complessità nell'aggiornamento di un numero rilevante di contratti di fornitura

Orientamento organizzativo in tema di Continuità e Resilienza Operativa

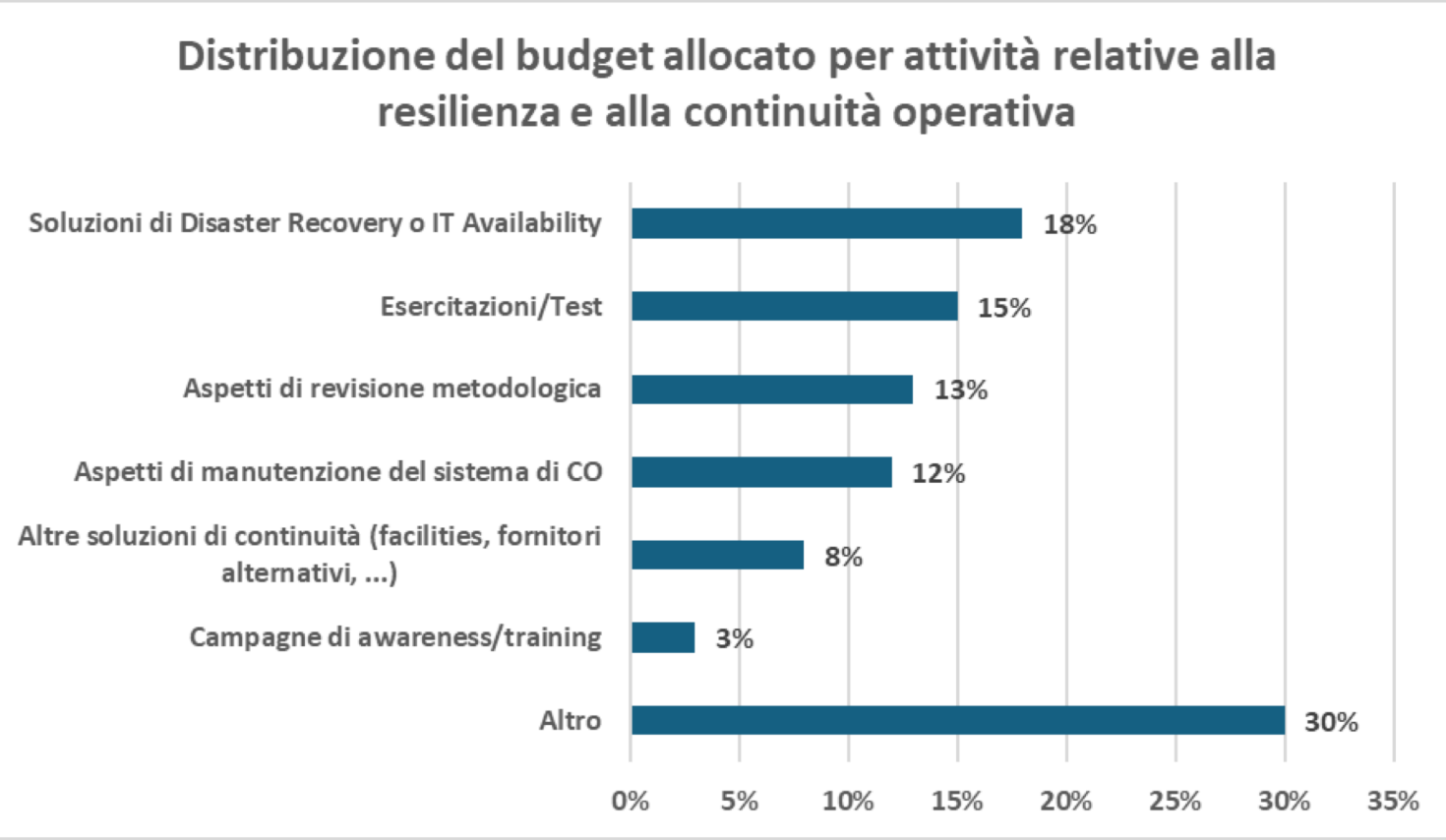
Si rilevano molteplici iniziative nell'ambito della Resilienza Operativa:

- ***Buona parte dei rispondenti ha definito un ruolo di responsabile per la Resilienza Operativa o sta valutando questa opzione.***
- ***Il 43% dei rispondenti ha attivato iniziative di awareness e programmi di training.***
- ***Revisione/Evoluzione dei ruoli e delle responsabilità per supportare la Resilienza Operativa.***



Priorità di investimento

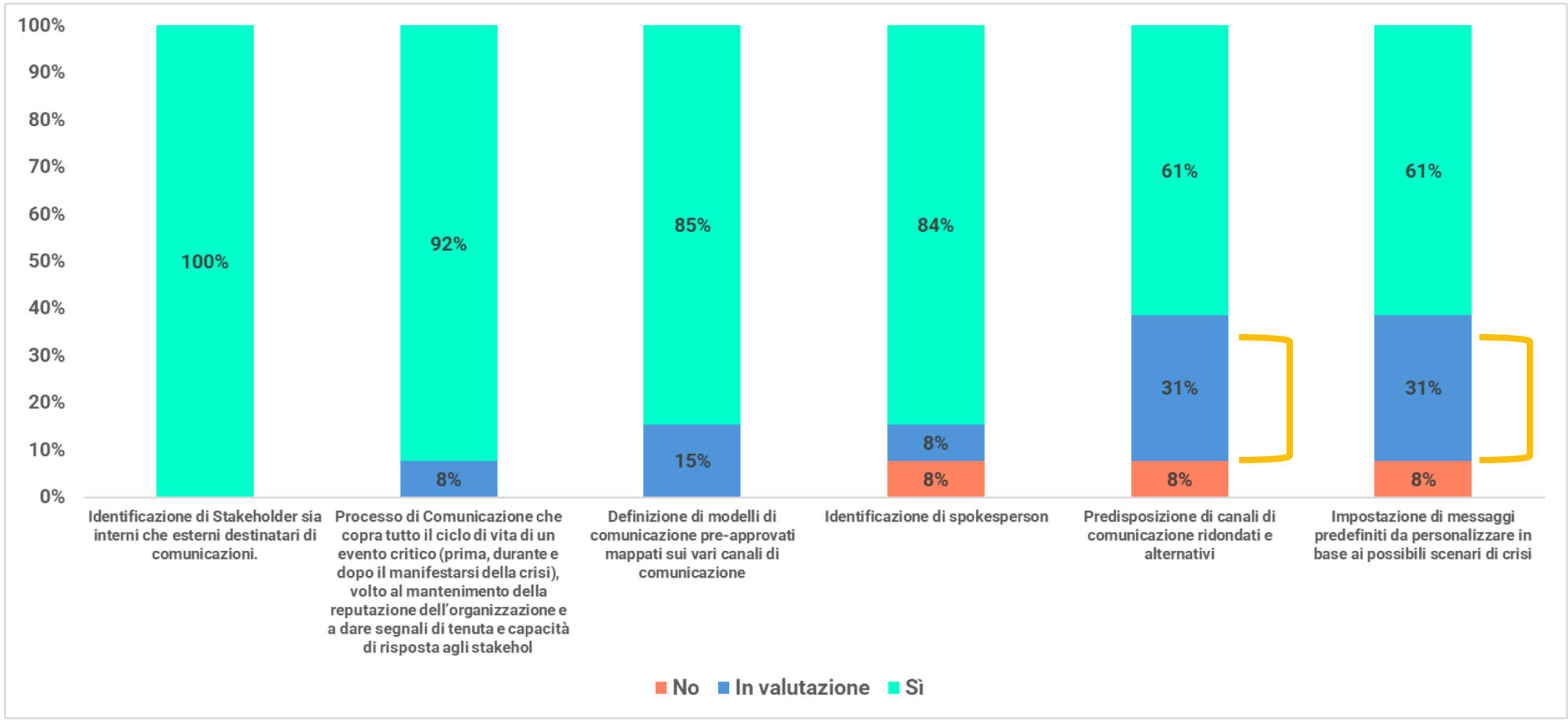
- **Nessuna organizzazione rispondente ha evidenziato una diminuzione del budget dedicato alla resilienza e alla continuità operativa rispetto allo scorso anno (18% nella scorsa rilevazione).**
- L'implementazione di soluzioni di **Disaster Recovery o Disponibilità IT** e l'**esecuzione di esercitazioni o test**, sembrano essere in termini assoluti le aree verso cui sono state convogliate maggiormente le risorse.
- **Ma nella distribuzione percentuale dei diversi ambiti di investimento è diminuità la quota % dedicata al Disaster Recovery e Disponibilità IT (-12%).**



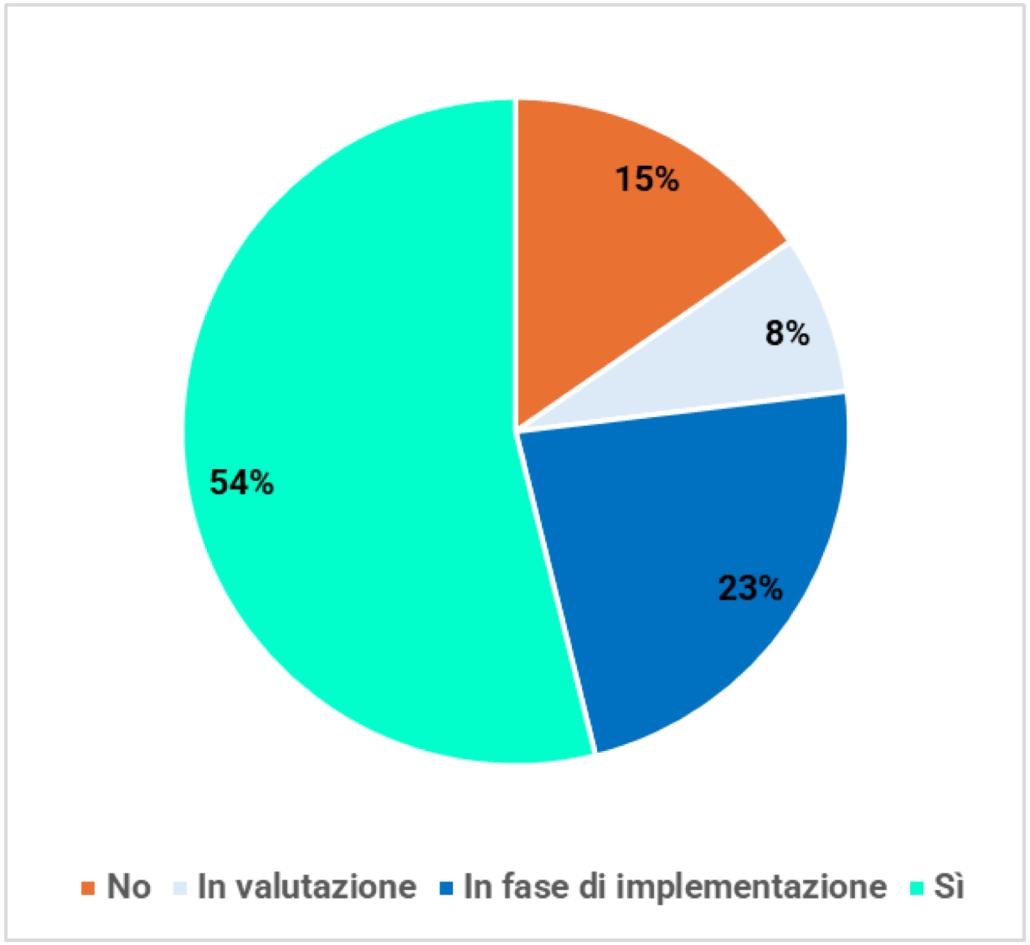
Piano di comunicazione: analisi dei dettagli implementativi

Alcuni elementi dei piani di comunicazione non risultano ancora pienamente implementati.

La **predisposizione dei canali di comunicazione ridondanti** e **l'impostazione di messaggi predefiniti da utilizzare in caso di possibili scenari di crisi** sembrano essere i due ambiti meno sviluppati.



Impiego di fonti di intelligence nell'ambito dell'Analisi dei Rischi



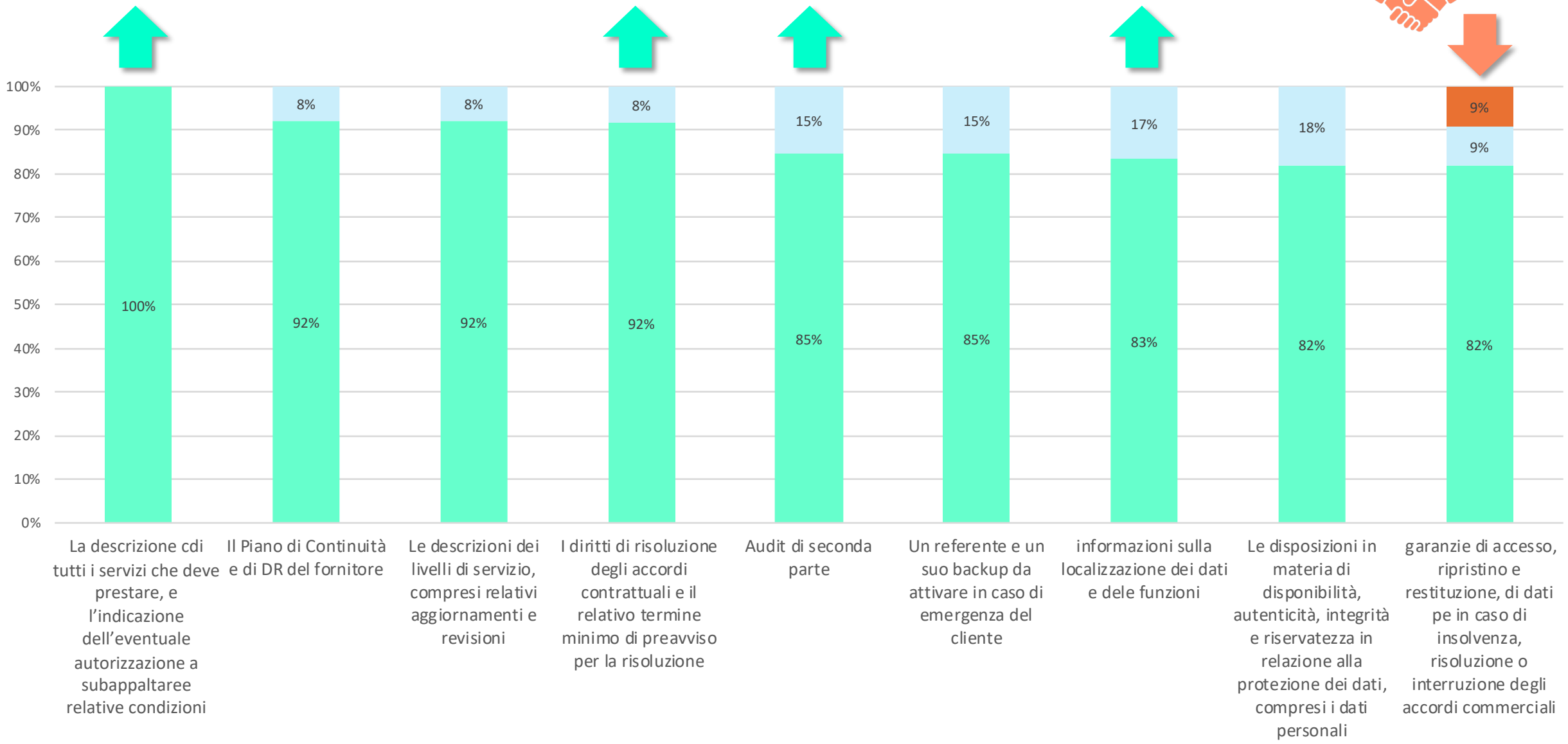
L'impiego delle fonti di intelligence è un ulteriore elemento chiave per costruire un sistema di **resilienza digitale proattivo**.

Le istituzioni finanziarie sono incoraggiate **a valutare regolarmente il proprio livello di esposizione alle minacce cibernetiche e alle vulnerabilità emergenti, basandosi anche su dati di intelligence.**

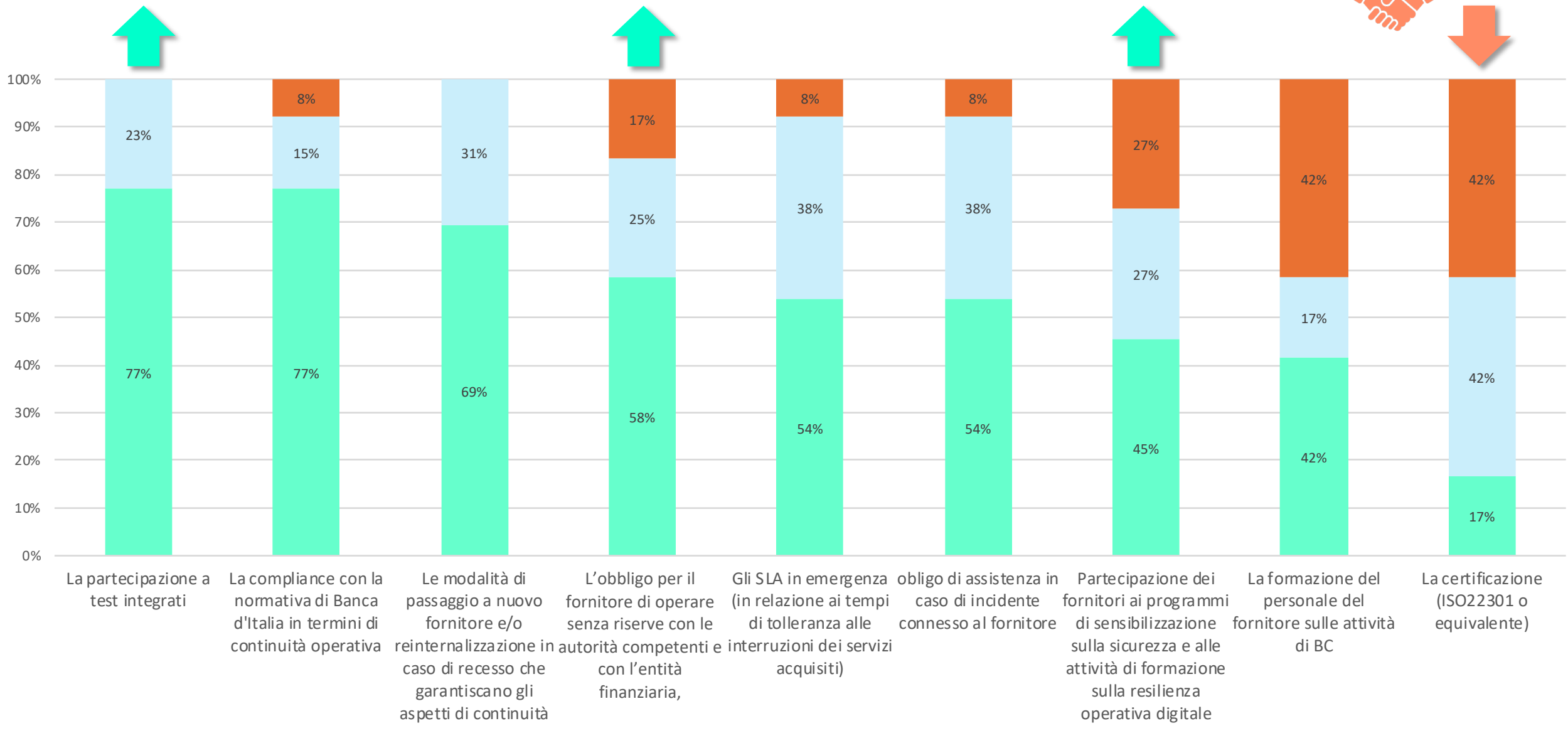
Dai dati raccolti nell'ambito, emerge un aumento rilevante delle organizzazioni che dichiarano di impiegare, o stanno implementando, fonti di intelligence (77%):

- Nell'edizione precedente, nessun rispondente aveva dichiarato di utilizzare tali fonti ma solo il 33% dichiarava che fossero in fase di implementazione.
- Tra gli strumenti utilizzati sono stati indicati: **strumenti di Threat Intelligence e la fruizione di contenuti da report specifici.**

Adeguamento al DORA: Articolazione dei contratti con i fornitori critici (1/2)



Adeguamento al DORA: Articolazione dei contratti con i fornitori critici: (2/2)



Punti di attenzione

LE BANCHE, NEL COMPLETARE LE NECESSARIE IMPLEMENTAZIONI, SEGNALANO PARTICOLARE COMPLESSITÀ RIGUARDO A:

- Indisponibilità delle versioni finali approvate di alcuni RTS/ITS
- Dubbi sulla interpretazione ed applicazione di alcuni requisiti in assenza di esperienza ed indicazioni di vigilanza
- Sviluppi metodologici per l'Individuazione delle CIF/FEI
- Integrazioni sulle analisi dei rischi e nella classificazione delle minacce
- Adeguamento degli strumenti per la raccolta delle informazioni per la Mappatura delle interdipendenze fra funzioni/processi/servizi/asset tecnologici
- Evoluzioni delle architetture di DR
- Adeguamento dei processi di classificazione e segnalazione indicenti
  (per i quali Le banche stimano un aumento della segnalazioni a fronte dei criteri introdotti dal DORA)
- Sviluppo delle modalità, degli obiettivi e e degli ambiti dei test, e dei relativi scenari delle minacce
- **Evoluzione della relazione tecnico contrattuale con i fornitori dei servizi**
  - *Modalità di classificazione e selezione degli accordi contrattuali da includere nel registro delle terze parti (anche a fronte del recente Dry Run)*
    - *Se un servizio (ad esempio di progettazione o di supporto) rientra o meno fra quelli da includere*
    - *Come classificare un servizio che rientra fra più categorie fra le 19 definite dall'ITS*
  - *Complessità nel negoziare clausole contrattuali con i grandi fornitori*
  - *Inesperienze e resistenze da parte di fornitori "minori"*
  - *numerosità dei contratti da aggiornare*