# *Rules and principles of risk management, beyond the fragmentation of operational risk*

**ABI – Supervision Risks&Profitability 2026**

**Milano, 10/06/2026**

BAPS

*Chief Risk Officer*

# Agenda

- 01 | *Context*
- 02 | *Operational Risk Fragmentation: A Further Source of Risk?*
- 03 | *Transversality with DORA, Third-Party ICT, and ESG Risks*
- 04 | *Transversality between DORA, ICT, and ESG for LSIs*
- 05 | *Outsourcers and Operational Risk: Problems and Solutions*
- 06 | *ICT Risk Control: Evolving Functions and Roles*
- 07 | *Case study: Data breach ai danni di un fornitore ICT di BAPS*
- 08 | *Operational Resilience Integration Framework - ORIF*
- 09 | *Wrap-up*

# Context

- ✓ In un contesto operativo in continua evoluzione, con crescente attenzione ai rischi **ICT, ESG e di terze parti**, BAPS ha avviato una **revisione organizzativa** per rafforzare presìdi e specializzazione sulle diverse tipologie di rischio.
- ✓ Sono state introdotte **unità indipendenti dedicate** ai singoli rischi, per rafforzare le competenze specialistiche mantenendo **coordinamento e visione integrata** del framework di Risk Management.
- ✓ Il framework è in evoluzione verso un modello integrato di **Operational Resilience**, orientato alla gestione oltre che alla misurazione integrata del rischio.

BAPS

# Operational Risk Fragmentation: A Further Source of Risk? *(1/2)*

**Rischio di frammentazione**

- La crescente specializzazione del **rischio operativo** è una naturale evoluzione del sistema Bancario, guidata dalla **digitalizzazione**, dall'aumento delle **minacce cyber**, dalla maggiore dipendenza da **terze parti** e dalla crescente rilevanza dei fattori **ESG**
- In questo contesto, la sfida consiste nel bilanciare competenze sempre più verticali con una **visione olistica**, in grado di cogliere e governare le **interdipendenze** tra i diversi profili di rischio

**Key concepts**

| Fonte di rischio | Impatti sull'operatività | Complessità reporting |
|---|---|---|
| *Specializzazione verticale* | *Tassonomia non unificate* | *Erosione dell'efficacia* |
| *Interdipendenze inespresse* | *Classificazione disomogenea* | *Deterioramento decisionale* |
| *Effetti Knock-on* | *Output non sintetizzato* | *Proliferazione KPI* |
| *Opacità decisionale* | *Aumento cost of control* | *Deficit di sintesi strategica* |

**BAPS** *Framework*

**Soluzioni per gestire il trade off tra specializzazione e integrazione**

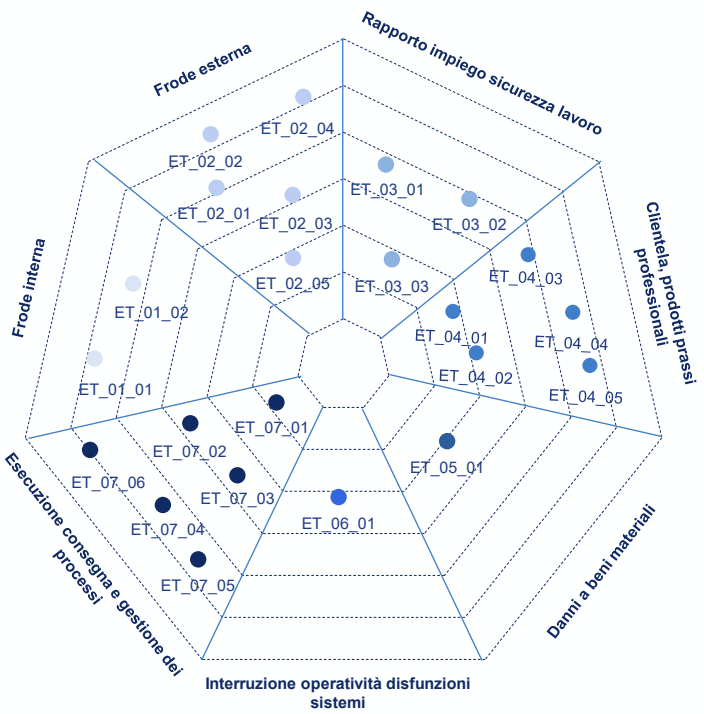
- Sviluppo di un **framework integrato** che faccia evolvere il modello di mappatura dei rischi, con focus sugli eventi boundary e articoli in modo coordinato e omogeneo tra le diverse fattispecie di rischio le diverse fasi del lifecycle risk management
- Tale impostazione permette di **evidenziare** le **correlazioni** tra il **rischio operativo** e gli altri **profili di rischio**, ricondotto in modo omogeneo gli eventi a impatto trasversale all'interno del framework
- Il **framework** consente di **rafforzare** il **coordinamento** tra **funzioni**, **uniformare** le **logiche** di **analisi** e favorire una maggiore **coerenza** nella produzione degli output, contribuendo a una lettura più trasversale e complessiva dei fattori di rischio aziendali

# Operational Risk Fragmentation: A Further Source of Risk? *(2/2)*

## Declinazione degli eventi

- In BAPS gli scenari di **Pillar 1 di Basilea** sono stati evoluti e contestualizzati nel più ampio **scenario operativo e tecnologico della Banca**, con l'obiettivo di **sviluppare** una **lettura integrata** dei rischi coerente con il paradigma della **resilienza operativa** introdotto da **DORA** e da altre normative di settore
- Tale approccio consente di valorizzare le interdipendenze tra rischi **operativi**, **ICT**, **cyber**, **terze parti** e continuità dei servizi critici e/o essenziali, rafforzando la **capacità del framework di Risk Management** di **rappresentare** in **modo unitario** le **esposizioni** di BAPS

## Event Type




## Boundary Events

a) Credit Risk
b) Market Risk
c) ICT e Cyber Risk
d) Misconduct Risk
e) Strategic Risk
f) Compliance Risk
g) Reputational Risk
h) ESG Risk
i) Third Party
j) Business Continuity
k) Data Management
l) Model
m) Statutory Reporting,Tax

## Dimensione di analisi

**Effetto boundary**

- Adozione di una **lettura trasversale** e **integrata** dei **diversi risk domain**,
- Rappresentazione **coerente** delle esposizioni e dei **relativi impatti**
- Diventa quindi essenziale distinguere:
  - *causa originaria dell'evento*
  - *meccanismo di propagazione del rischio*
  - *natura finale dell'impatto economico*

**Business Resilience**

- In questa prospettiva, la **business resilience** assume una **dimensione trasversale** rispetto ai diversi risk domain e richiede una **lettura sempre più end-to-end** dei processi, delle relative dipendenze operative e delle componenti tecnologiche

# Transversality with DORA, Third-Party ICT, and ESG Risks

**Dal rischio frammentato alla resilienza integrata**

- La risposta alla **frammentazione** del settore si è tradotta in un'**evoluzione regolamentare** e **metodologica** orientata a **rafforzare l'integrazione dei modelli** e a **contenere la variabilità delle scelte** metodologiche tra intermediari
- In tale contesto, il **framework implementato** da **BAPS** supporta il **passaggio** a un **approccio** di **governance** del **rischio strutturato** e **multidimensionale**, in grado di superare logiche per funzione e abilitare una resilienza operativa effettivamente integrata

**Key concepts**

| **Spinta visione olistica** | **DORA** (NIS2, …) | **ICT & Third Party** | **Fattori ESG** |
|---|---|---|---|
| • *Riduzione discrezionalità metodologica* | • *Lex specialis* | • *Concentrazione* | • *Loss events ESG-driven* |
| • *Integrazione dati di rischio* | • *Armonizzazione requisiti* | • *Trasparenza della catena del valore* | • *Canali di trasmissione* |
| • *Passaggio da logica di calcolo a una di gestione* | • *Framework documentato* | • *Supervisione sistemica diretta* | • *Moltiplicatori di severità* |
| | • *Scenari interconnessi Operational – ICT - Third Party* | | |

**BAPS** *Framework*

## Visione olistica

- Le interconnessioni tra DORA, rischio terze parti e ESG Risk hanno condotto all'avvio di progettualità ad hoc sviluppate con partecipazioni interfunzionali, revisioni organizzative ed evoluzioni in chiave organica degli approcci e delle metodologie.
  - Progetto DORA avviato nel 2024 e autovalutazione condotta nel 2025;
  - Costituzione di una Funzione di Controllo Rischi ICT e Sicurezza nel luglio del 2023 e definizione del framework metodologico a supporto; revisione processo di gestione delle terze parti e identificazione di una Unità organizzativa a presidio; revisione integrale della struttura della Funzione IT con unità specialistiche e unità di coordinamento con altre funzioni (governance, terze parti, etc.)
  - Costituzione di un Servizio Sostenibilità, ampliamento delle attribuzioni del Comitato endo-consiliare dedicato ai rischi (Comitato Rischi e Sostenibilità) ed elaborazione di piani di azione volte ad integrare i rischi ESG nella gestione dei rischi; politiche di diversity; certificazione parità di genere Uni/PdR 125:2022; diversificazione per competenze, età e genere del board e degli altri Organi aziendali.
  - Sessioni di RCSA, ampliamento della raccolta dei dati (LDC), implementazione di un GRC
  - Creazione di meccanismi di integrazione orizzontale (C-Suite, Comitati manageriali, etc.)

# Transversality between DORA, ICT, and ESG for LSIs *(1/3)*

**Equilibrio tra robustezza del controllo e proporzionalità**

- Per le **LSIs** l'implementazione dei diversi **framework** di **resilienza** e **risk management** non può basarsi sulla mera replica dei modelli più complessi, ma richiede un **adattamento proporzionato** e **sostenibile** al proprio **perimetro operativo**
- Un **approccio eccessivamente traspositivo**, infatti, rischia di generare **complessità** non gestibile rispetto alle risorse disponibili, **riducendo l'efficacia dei presidi**
- Ne deriva la necessità di un **equilibrio** tra **robustezza** del **controllo**, **proporzionalità** e **sostenibilità del modello** di **governo del rischio**

**Key concepts**

| Criteri guida | Multi - fattorialità | Sana e prudente gestione |
|---|---|---|
| • *Proporzionalità* | • *Integrazione fattoriale degli scenari* | • *Presidio unitario della resilienza* |
| • *Modello lean* | • *Capital planning vs silos informativi* | • *Traduzione dei tecnicismi in valore* |
| • *Risk comunity* | • *Effetti combinati* | • *Governance integrata* |
| • *Risk Culture* | | • *Reporting olistico* |

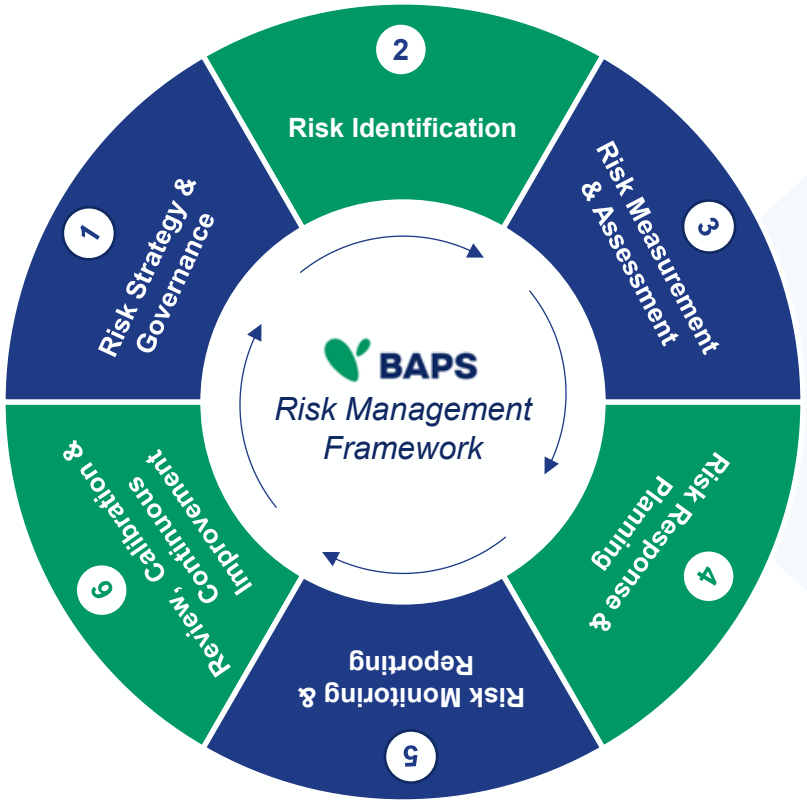
**BAPS** *Framework*

**Trasversalità nelle funzioni**

- L'**applicazione** di **criteri** di **materialità** e **proporzionalità** ha consentito di superare **logiche per silos e micro-funzioni**, favorendo modelli organizzativi più snelli e una lettura end-to-end dei processi e delle esposizioni
- **BAPS**, facendo leva sulla propria struttura organizzativa ha potuto disegnare **modelli** in linea con i **requisiti di vigilanza e coerenti con le esigenze di censimento**, in termini di attributi, modalità di classificazione e integrazione nei sistemi aziendali, garantendo una gestione complessiva delle fattispecie di rischio
- Tale impostazione è stata supportata da un **modello** di **governance** basato su **coordinamento centralizzato delle attività** e sviluppo decentrato presso i managers dei diversi ambiti di riferimento, con l'obiettivo di assicurare una visione il più possibile completa e coerente degli eventi di rischio
- Il tutto si inserisce nello sviluppo di un **framework integrato** e **circolare**, articolato in **fasi** tra loro **interconnesse**, applicate in modo omogeneo alle diverse fattispecie di rischio e supportate da un processo continuo di monitoraggio

# Transversality between DORA, ICT, and ESG for LSIs *(2/3)*

Il **BAPS Risk Management** framework evolve da una logica di sola **loss event collection** a un modello integrato di **Operational Risk, Operational Resilience** e **ICT Risk**, orientato non solo alla misurazione ma alla **gestione attiva del rischio**, per assicurare **resilienza** e **continuità operativa** nel rispetto dei principi di sana e prudente gestione




1. **Disciplina governance**, **ruoli**, **metriche**, **soglie**, **escalation** e **priorità di rischio**, definendo gli indirizzi per l'intero **processo risk management**. Gli output delle attività di monitoring, assessment e review alimentano l'aggiornamento del framework, garantendone l'evoluzione rispetto al profilo di rischio

2. **Identificazione** nel **continum** dei **rischi** che possono **impattare obiettivi strategici**, **operativi** e **regolamentari**. La fase comprende la mappatura dei rischi per processi, business unit, prodotti e servizi, integrando database e rilievi audit

3. Valutazione del **livello** di **esposizione** ai rischi identificati tramite analisi del **rischio inerente** e **residuo**, **efficacia dei controlli**. La fase consente di prioritizzare i rischi, identificare vulnerabilità e supportare decisioni risk-based

4. **Definizione** delle **azioni necessarie** per riportare il **rischio** entro i **livelli** di **tolleranza** definiti da BAPS. La fase include **remediation plan**, **strategie di mitigazione** e il **monitoraggio continuo** delle **azioni implementate** che alimenta eventuali interventi correttivi o recalibration

5. **Monitoraggio continuo** del **profilo** di **rischio attraverso KRI**, soglie **RAF** ed **early warning indicators**. La fase supporta **reporting direzionale**, **escalation** e **processi decisionali tempestivi**. Gli output del monitoring alimentano reassessment e revisione del Risk Management Framework

6. **Revisione periodica** del **Risk Management Framework** finalizzata ad **aggiornarne metodologie**, **metriche** e **processi** rispetto all'evoluzione del contesto interno ed esterno. La fase integra feedback provenienti da monitoring, audit, eventi operativi ed evoluzioni normative

# Transversality between DORA, ICT, and ESG for LSIs *(3/3)*

**Framework integrato cross-risk**, applicato in modo omogeneo alle diverse fattispecie e supportato da un **monitoraggio continuo**, che ci consente di **rafforzare il coordinamento** tra le funzioni di controllo e di garantire una **lettura più coerente e trasversale** dei profili di rischio di BAPS

| *BAPS Risk Management* \ *Risk categories* | 1 *Operational risk* | 2 *ICT risk* | 3 *Third-party risk* | 4 *ESG risk* | *…* |
|---|---|---|---|---|---|
| 1 *Risk Strategy & Governance* | **Definizione** ruoli e responsabilità, perimetro analisi, processi, Risk Control Map, controlli e soglie RAF | **Definizione** ruoli e responsabilità, soglie RAF, perimetro, processi, asset ICT e controlli | **Definizione** ruoli, perimetro, criteri di criticità delle terze parti ICT e soglie RAF | **Integrata** con strategie business e RAF, modello ibrido che combina coordinamento centrale e funzioni specialistiche | … |
| 2 *Risk Identification* | **Mappatura** tassonomia dei processi, Risk Control Map e scenari di rischio *(event type e fattori di rischio)* | **Mappatura** perimetro oggetto di analisi, scenari di rischio e minacce | **Mappatura** terze parti ICT, servizi erogati, processi supportati e scenari di rischio applicabili | **Mappatura** enti e potenziali rischi rispetto ai canali di trasmissione in coerenza con ICAAP con coinvolgimento stakeholder | … |
| 3 *Risk Measurement & Assessment* | Rischio lordo, efficacia dei presidi di mitigazione e rischio netto tramite **analisi** dei driver verticali di ogni grandezza | Rischio inerente e residuo tramite **analisi** degli impatti, probabilità e dell'efficacia dei controlli | Rischio residuo per terze parti tramite **analisi** degli impatti, probabilità e dell'efficacia dei controlli | **Rilevanza** rischi ESG con wokshop verticali, driver valutativi e data point integrati, declinati sulle specificità dei singoli ambiti operativi | … |
| 4 *Risk Response & Planning* | **Remediation plan** per rischi che superano soglie critiche e **azioni di efficientamento** per rischi sotto soglie critiche | **Remediation plan** e **azioni di mitigazione** per i rischi superiori alla soglia RAF | **Remediation** e **azioni di mitigazione**, revisione contrattuale, exit strategy o sostituzione del fornitore | **Cambio** di **indirizzi gestionali** coerenti con le evidenze emerse negli assessment che riflettono l'obiettivo strategico di business | … |
| 5 *Risk Monitoring & Reporting* | **Nel continuum** tramite KRI integrati nel RAF e reporting periodico verso gli Organi aziendali | **Nel continuum** tramite KRI, incidenti e reporting periodico verso gli Organi aziendali | **On-going** delle terze parti ICT, delle FEI, dei presidi del fornitore e reporting verso gli Organi aziendali | **Nel continuum** tramite KRI integrati nel RAF e altri KRI di natura gestionale monitorati dagli stakeholder | … |
| 6 *Review, Calibration & Continuous Improvement* | **Nel continuum** del framework in funzione di evoluzioni normative, tecnologiche e operative | **Nel continuum** del framework in funzione di evoluzioni normative, tecnologiche e operative | **Nel continuum** di metodologia, scenari, controlli e valutazioni in funzione di eventi, criticità e variazioni del fornitore | **Nel continuum** in linea con le strategie di business finalizzate all'identificazione della rilevanza dei fattori ESG | … |

BAPS

# Outsourcers and Operational Risk: Problems and Solutions

**Interdipendenze supply chain consortile e non**

- La **crescente dipendenza** da **fornitori esterni** rappresenta un ambito di **particolare criticità**, in cui l'intersezione tra **requisiti normativi**, **presidi** di **rischio** e **modelli operativi** genera le principali **aree di complessità gestionale**
- Tale evidenza risulta rilevante per le **LSI fortemente integrate** in **catene di fornitura** di tipo consortile, dove le **interdipendenze operative** amplificano le **esigenze** di **governo** del **rischio** e di **presidio della continuità dei servizi**

**Key concepts**

| Esternalizzazione | Dipendenza sistemica | Relazioni contrattuali | Controllo diretto |
|---|---|---|---|
| • *Trasferimento della responsabilità prudenziale* | • *Rischio di concentrazione* | • *Catene di Sub-fornitura* | • *Auditabilità* |
| • *Da Outsourcing a Third-Party Arrangements* | • *Single point of failure* | • *N-th Party Risk* | • *Portabilità dati* |
| • *Mappatura Critical or Important Functions* | • *Effetto contagio sistemico* | • *Due diligence avanzata* | • *Exit Strategies* |
| | | • *Monitoraggio continuo e testing congiunto* | |

**BAPS** ***Framework***

## Third Party Risk

- **Trade off concentrazione vs integrazione:** analisi costi/benefici facilitata dalla ricerca di logiche omogenee tra BAPS e il principale fornitore:
  - Coerenza delle strategie;
  - Moduli di raccordo e coordinamento;
  - Rafforzamento sensibilità del provider verso tematiche di gestione dei rischi
- **Processi strutturati di assessment** del rischio di terze parti e delle performance che coinvolgono più unità, investono tutti i rischi e sono coordinati da una Direzione specializzata
- **Metodologia interna di valutazione delle terze parti ICT** (15 scenari, scale omogenee con il rischio ICT); third party register unico; tracciabilità dell'intero ciclo di relazione: a partire dall'identificazione delle terze parti, dei servizi erogati, dei processi supportati e degli scenari di rischio applicabili, fino a un testing nel continum (con particolare attenzione alle FEI), basato su analisi di impatto e probabilità e sulla valutazione dell'efficacia dei controlli, a supporto delle decisioni su mitigazioni ed eventuale exit strategy e dell'aggiornamento nel tempo di metodologie e presidi.

# ICT Risk Control: Evolving Functions and Roles

**Nuove interconnessioni di rischio**

- La **crescente interconnessione** tra **rischio ICT** e di **sicurezza**, **terze parti**, **resilienza operativa** ed **ESG** sta modificando profondamente gli **assetti di governance** delle banche
- Le **nuove aspettative regolamentari** richiedono il superamento dei **silos organizzativi** e una **lettura integrata** dell'**esposizione** al **rischio**
- In questo contesto, il **CRO** assume un **ruolo centrale** nel **garantire coerenza**, **visione olistica** e **capacità decisionale** al vertice aziendale

**Key concepts**

| ICT risk management | Evoluzione strategica | Risk data aggregation | Governance |
|---|---|---|---|
| • *Superamento del Back-office operativo* | • *Superamento dei silos metodologici* | • *Superamento dei silos informativi* | • *KRI sintetici* |
| • *Ruoli e responsabilità* | • *Integrazione forward-looking* | • *Viste uniche di classificazione* | • *Inquadramento nel RAF* |
| • *Integrazione delle analisi nel prospetto ICAAP* | • *Mandato strategico* | • *Data Quality come prerequisito* | • *Reporting Olistico* |
| | | | • *Business resilience* |

**BAPS** *Framework*

**ICT Risk**

- Framework di ICT&Security risk management modellato sui requirements DORA
- Strategia di resilienza operativa e digitale in chiave olistica, normative specifiche a presidio delle diverse fasi, strumenti e protocolli di sicurezza integralmente rivisitati
- Funzione di Rischio ICT e Sicurezza: specializzazione vs integrazione
- Approccio strutturato alla gestione del rischio ICT, allineato con quello adottato per il rischio operativo sia in termini di dimensioni di analisi sia di scala di valutazione quantitativa, per garantire un linguaggio di valutazione unico e una lettura integrata delle esposizioni tecnologiche e operative, coerente lungo i cinque livelli previsti dal framework interno
- Questa impostazione si traduce in una metodologia che presidia l'intero ciclo di gestione del rischio ICT: dalla definizione di governance, perimetro, processi, asset ICT, controlli e soglie RAF, all'identificazione del perimetro oggetto di analisi, degli scenari di rischio e delle principali minacce. La valutazione del rischio inerente e residuo è basata su analisi di impatto, probabilità ed efficacia dei controlli e su queste basi vengono definiti i remediation plan e le azioni di mitigazione per le esposizioni oltre obiettivo RAF
- monitoraggio continuo tramite KRI e reporting verso gli Organi aziendali e continuous improvement
- Ricerca di collaborazione trasversale tra funzioni nella definizione della metodologia e nella gestione di incidents e progettualità

# Case study: Data breach ai danni di un fornitore ICT di BAPS *(2/2)*

**Descrizione dello scenario:** una terza parte ICT di BAPS, che fornisce un applicativo in modalità SaaS a supporto dei processi di credito, è stata vittima di un attacco informatico che avrebbe potuto determinare una potenziale esfiltrazione di dati di proprietà di BAPS. Le verifiche con il fornitore hanno confermato che l'attacco non ha interessato i dati della Banca. Il CRO e la Funzione ICT Risk hanno valutato la variazione del profilo di rischio e gli impatti sul BAPS Risk Management Framework. Di seguito un estratto della mappatura dei rischi e dei canali di trasmissione attivata a seguito dell'evento

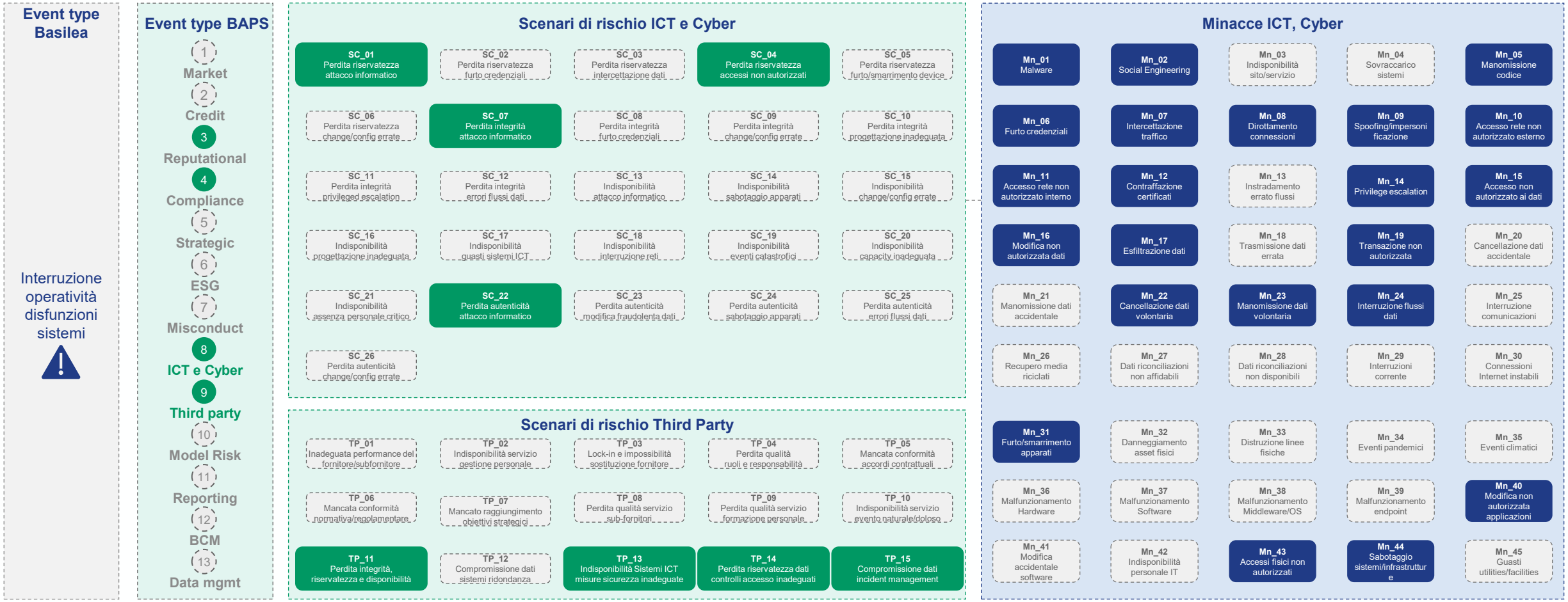
| | Rilevazione evento | Analisi rischi IT, Cyber e Third Party | Analisi controlli IT, Cyber e Third Party | Analisi rischi operativi | Remediation plan | Monitoring program |
|---|---|---|---|---|---|---|
| **Descrizione attività** | • Il **fornitore di BAPS** ha tempestivamente comunicato il possibile coinvolgimento in un **data breach**<br>• La **Banca** ha attivato un **canale di scambio continuo** con il fornitore per ricevere **aggiornamenti costanti** | • Il **CRO** e la **Funzione IT Risk** hanno avviato un'analisi tramite il **BAPS Risk Management Framework** al fine di valutare gli **scenari di rischio** impattati dall'evento<br>• Più in generale, il **framework** viene applicato **on going** e/o **ad evento** | • Sono stati identificati i **controlli a presidio** degli **scenari di rischio** impattati e, sulla base delle prime informazioni trasmesse dal fornitore, i controlli inizialmente classificati come **«falliti»** sono stati rivalutati come **«non efficaci»** | • Sono stati identificati i **processi correlati** allo **scenario** in questione ed è stato rivalutato il **profilo di rischio (probabilità)** | • La **Banca**, pur non avendo subito conseguenze dall'attacco, ha richiesto al **fornitore** un **remediation plan** al fine di tutelarsi da **eventi futuri** | • La **Banca** (Funzioni **Information Security** e **IT Risk**) ha avviato un **programma di monitoraggio** sull'implementazione delle **misure di rimedio**<br>• In parallelo sono stati rivalutati i **presìdi di controllo in place** e sono state condotte attività di **set up delle metriche** e di **review del framework** |

*Timeline: 9 mesi*

| BAPS Risk Management Framework | | | | | | |
|---|---|---|---|---|---|---|
| | Risk Identification | Risk Measurement & Assessment | Risk Measurement & Assessment | Risk Measurement & Assessment | Risk Response & Planning | Review, Calibration & Continuous Improvement<br>Risk Strategy e Governance |

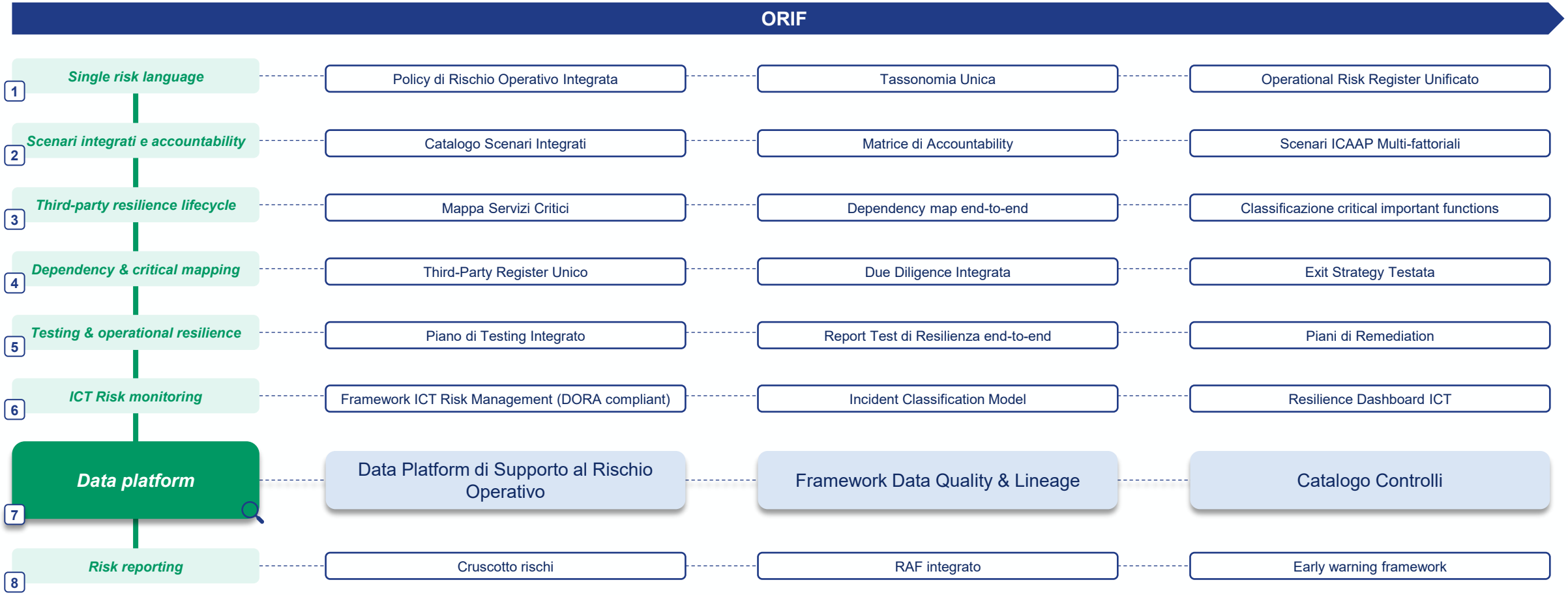
# Case study: Data breach ai danni di un fornitore ICT di BAPS *(1/2)*

**Descrizione dello scenario:** una terza parte ICT di BAPS, che fornisce un applicativo in modalità SaaS a supporto dei processi di credito, è stata vittima di un attacco informatico che avrebbe potuto determinare una potenziale esfiltrazione di dati di proprietà di BAPS. Le verifiche con il fornitore hanno confermato che l'attacco non ha interessato i dati della Banca. Il CRO e la Funzione ICT Risk hanno valutato la variazione del profilo di rischio e gli impatti sul BAPS Risk Management Framework. Di seguito un estratto della mappatura dei rischi e dei canali di trasmissione attivata a seguito dell'evento



# Operational Resilience Integration Framework - ORIF

**Modello target** che integra i principali ambiti della gestione del rischio operativo in un'unica **architettura coerente**, raccogliendo le considerazioni critiche su governance, dependency mapping, testing della resilienza e monitoraggio dei dati, e fornendo una **base strutturata per il presidio operativo** della resilienza



# Wrap-up

## 1

### Valore della resilienza

Leva di sostenibilità del modello di business

- Gestione di scenari **multifattoriali** (ICT, ESG, terze parti, continuità) con una lettura integrata degli impatti
- **Stress test** e piani di **Business Continuity** a supporto della tempestività decisionale in condizioni di stress
- Integrazione della resilienza operativa nei **processi strategici** e nei cicli di pianificazione della Banca

## 2

### Responsabilità trasversale

Governance integrata

- **Coinvolgimento coordinato** delle funzioni specialistiche su rischi ICT, ESG, terze parti e continuità operativa
- Tassonomie, processi e **linguaggi comuni** per una **lettura unitaria** delle esposizioni e dei canali di trasmissione del rischio
- Chiarezza di **ruoli** e **responsabilità** per assicurare presidio end-to-end lungo i processi critici

## 3

### Risk data aggregation, risk reporting

Prerequisito per decisioni uniformi

- Framework informativi strutturati per garantire **qualità del dato**, coerenza tassonomica e tracciabilità
- **Dashboard direzionali integrate** che aggregano i principali indicatori di rischio a livello aziendale
- Informativa sintetica e **azionabile** a supporto degli Organi di governo nei processi di indirizzo e controllo

# BAPS

Una nuova Banca. Fondata a Ragusa nel 1889