

# Normativa DORA e gestione delle Terze Parti

# Agenda

- 1 Aggiornamento del Quadro Normativo
- 2 Il Quadro Sanzionatorio e impatti organizzativi
- 3 PwC View: Benchmark di mercato
- 4 Focus on: Gestione delle Terze Parti



# Aggiornamento del Quadro Normativo

# Aggiornamento del quadro normativo



**EBA dichiara**  
Futuro aggiornamento delle  
EBA Guidelines on outsourcing  
*Commentario RTS Terze Parti*

**Le ESA** sottolineano che le Guidelines emanate a livello EU  
vengono superate da DORA per i temi di competenza, per cui le  
FSI si devono concentrare sui requisiti mandatori di DORA (e non  
delle Guidelines)

**ECB** nella lettera agli AD delle Banche SI

- stesso regime esternalizzazioni e terze parti per i servizi ICT (registro delle informazioni)
- unico meccanismo segnalatorio incidenti
- Allineamento SREP con DORA

**ECB adegua** il  
framework **TIBER-  
EU** per  
armonizzazione  
con DORA

**EIOPA abroga**

- "Guidelines on ICT Security and Governance"
- "Guidelines on Cloud Outsourcing"

**EBA abroga**  
Il reporting  
degli incidenti  
PSD2

**EBA adegua**  
Le "Guidelines on  
ICT and Security"  
per armonizzazione  
con DORA



Adozione e  
pubblicazione  
di **DORA**

Entrata in  
vigore  
**DORA**

**DORA  
Go Live**



**Banca d'Italia anticipa** il  
recepimento delle disposizioni **DORA**  
in ambito Governance, dettagliando  
per il **settore Bancario (Circolare  
285) le modalità operative e le  
attività** per creazione della **funzione  
di Il livello dedicata ai Rischi ICT e  
Sicurezza**, oltre ad un avvicinamento  
in termini di requisiti (e.g. terze parti,  
BCM) ad alcuni dei principi di DORA

**Banca d'Italia (30/12/2024):**

- Linee guide in ambito governance per soggetti non Bancari
- Decadimento regime outsourcing per esternalizzazioni e terze parti di Servizi ICT
- Univoche modalità di reporting incident e relative canali
- Futuro aggiornamento normativa Nazionale

**IVASS:**

- modalità di reporting incident e relativi canali (**14/02**)

**COVIP**

- Applicazione e modalità di reporting (**27/02**)

**Decreto Legislativo 23/2025** «Disposizioni  
per l'adeguamento della normativa nazionale  
al Regolamento DORA» (**10/03**)

**IVASS:**

- Modalità e tempistiche Rol (**07/03**)
- Aspettative in ambito esternalizzazioni (**11/03**)

**BankIT**

- Modalità e tempistiche Rol (**14/03**)

# Adeguamento Nazionale al DORA (DL 23/2025)

## Novità Normative

### 1. Autorità Competenti

- Determinazione Autorità per ciascun Settore FS
- Determinazione Autorità per la vigilanza sulle Terze Parti
- Ruoli all'interno del Framework Sorveglianza EU

### 2. Estensione Applicazione

- Applicazione Regolamento DORA e per intermediari finanziari (e.g. ex 106) e Bancoposta
- Tempistiche: 2 anni per gli Intermediari Finanziari (gennaio 2027)

### 3. Major Incident Reporting

- Attuazione Processi di reporting Major Incident in Italia
- Relazione con CSIRT (perimetro NIS2)

### 4. Regime Sanzionatorio

- Dettaglio dello schema regime sanzionatorio per le diverse tipologie di Entità FS, differenziato per requisiti DORA
- Introduzione sanzioni per persone giuridiche - BoD member o con ruolo di amministrazione o controllo

## Takeaways

- Autorità DORA in Italia: BankIT; CONSOB; COVIP; **IVASS** (Imprese di assicurazione; Imprese di riassicurazione; Intermediari assicurativi; Intermediari riassicurativi; Intermediari assicurativi a titolo accessori)
- Vigilanza sulle 3 Parti: Ciascuna autorità per settore di competenza
- Partecipazione al Framework di Sorveglianza EU: BankIT

- Gap analysis e valutazione dell'estensione del Programma DORA e dei presidi implementati anche agli Intermediari Finanziari finora non in scope (in caso di Gruppi)

- Criteri e report di segnalazione previsti da DORA
- Segnalazione, processi di reporting e follow up incidente con l'Autorità DORA (IVASS)
- In caso si sia stati nominati Entità Essenziali o Importanti ai fini NIS2, Informativa verso CSIRT nazionale con report e criteri previsti da DORA  
- la vigilanza è in carico all'Autorità DORA

- Analisi organizzativa per l'identificazione di tutti i soggetti che svolgono compiti di amministrazione, direzione o controllo e che quindi sono potenzialmente oggetto del nuovo regime sanzionatorio
- Gap Analysis rispetto alle tutele ad oggi esistenti per tali soggetti/funzioni allo scopo di identificare eventuali nuove coperture da attivare per tutti i soggetti identificati

# 2

## Il Quadro Sanzionatorio e impatti organizzativi

# Schema sanzionatorio

## Applicazione

### Quali sono le Sanzioni previste?

- Le sanzioni sono differenziate per **tipologia di requisito DORA e relativi RTS** oggetto di inosservanza:
  - **Caso 1 Sanzioni di maggiore entità** per inosservanza dei requisiti DORA ed RTS che riguardano i temi di **Governance; Risk Management & Digital Strategy**; Individuazione (minacce, vulnerabilità, eventi); **Backup; Incident Management & Reporting**; Regime Semplificato (ove applicabile)
  - **Caso 2 Sanzioni di minore entità** per inosservanza dei requisiti DORA ed RTS che riguardano i temi di **Processi e tecnologie di Sicurezza / ICT**; Identificazione, Protezione, Risposta, Ripristino, Comunicazione e Follow Up; Incident Classification; TPRM; **Test e TLPT** (ove applicabile)
- Le Sanzioni possono essere applicate anche alle relative **Terze Parti** coinvolte
- Sono previste sanzioni sia per le **Entità Finanziarie** che per le **Persone Fisiche**. Per le persone fisiche, sono inoltre previste:
  - Inasprimento della sanzione nel caso in cui il vantaggio ottenuto dall'autore della violazione sia maggiore della sanzione massima prevista;
  - Possibilità di interdizione dalle funzioni ricoperte da 6 mesi a 3 anni (in tutte le Entità Finanziarie nazionali)

### Quando si applicano alle Entità Finanziarie?

- Mancata attuazione dei requisiti DORA ed RTS
- Omessa collaborazione o mancato seguito dato nell'ambito di un'indagine, un'ispezione o una richiesta da parte delle Autorità

### Quando si applicano alle persone fisiche?

- Quando svolgono compiti di amministrazione, direzione o controllo
- Quando l'oggetto della sanzione costituisce reato
- Se l'inosservanza è conseguenza della violazione di doveri propri o dell'organo di appartenenza e la condotta ha inciso in modo rilevante sulla complessiva organizzazione o sui profili di rischio aziendali o ha contribuito a determinare la mancata ottemperanza della società
- In caso di comportamento reiterato\*

\*Articolo 50 del Regolamento (UE) 2022/2554 (DORA): «Gli Stati membri conferiscono alle autorità competenti il potere di applicare almeno le sanzioni amministrative o misure di riparazione seguenti per le violazioni del presente regolamento: a) emanare un ordine che imponga alla persona fisica o giuridica di porre termine al comportamento in violazione del presente regolamento e di astenersi dal ripeterlo;»

# Schema sanzionatorio

## Dettaglio

### Tipologia di Entità\*

Tipologia di Entità*	Requisiti DORA oggetto di sanzione (inclusi relativi RTS)			
	<div>• Governance</div> <div>• Risk Management &amp; Digital Strategy</div> <div>• Individuazione</div>	<div>• Backup</div> <div>• Incident Management &amp; Reporting</div> <div>• Regime Semplificato <i>(ove applicabile)</i></div>	<div>• Processi e tecnologie di Sicurezza / ICT</div> <div>• Identificazione, Protezione, Risposta, Ripristino, Comunicazione e Follow Up</div>	<div>• Incident Classification</div> <div>• TPRM</div> <div>• Test e TLPT <i>(ove applicabile)</i></div>
	Sanzioni per l'Entità Finanziaria	Sanzioni per i soggetti che svolgono compiti di amministrazione, direzione o controllo**	Sanzioni per l'Entità Finanziaria	Sanzioni per i soggetti che svolgono compiti di amministrazione, direzione o controllo**
Enti Creditizi ed Intermediari Finanziari	min: 30.000 € max: 10% del fatturato	min: 5.000 € max: 5 mil €	min: 30.000 € max: 7% del fatturato	min: 5.000 € max: 3,5 mil €
Istituti di Pagamento ed IMEL	min: 30.000 € max: 5 mil € o 10% del fatturato (se > 5 mil €)	min: 5.000 € max: 5 mil €	min: 30.000 € max: 3,5 mil € o 7% del fatturato (se > 3,5 mil €)	min: 5.000 € max: 3,5 mil €
SIM, SGR, SICAV, SICAF, controparti centrali, gestori mercati regolamentati	min: 30.000 € max: 5 mil € o 10% del fatturato (se > 5 mil €)	min: 5.000 € max: 5 mil €	min: 30.000 € max: 3,5 mil € o 7% del fatturato (se > 3,5 mil €)	min: 5.000 € max: 3,5 mil €
Depositari centrali di titoli	min: 30.000 € max: 20 mil € o 10% del fatturato (se > 20 mil €)	min: 5.000 € max: 5 mil €	min: 30.000 € max: 14 mil € o 7% del fatturato (se > 14 mil €)	min: 5.000 € max: 3,5 mil €
Servizi di crowdfunding	min: 500 € max: 500.000 € o 5% del fatturato (se > 500.000 €)	min: 500 € max: 500.000 €	min: 500 € max: 350.000 € o 3,5% del fatturato (se > 350.000 €)	min: 500 € max: 350.000 €
Amministratori di indici di riferimento	min: 10.000 € max: 1 mil € o 10% del fatturato (se > 1 mil €)	min: 5.000 € max: 500.000 €	min: 10.000 € max: 700.000 € o 7% del fatturato (se > 700.000 €)	min: 5.000 € max: 350.000 €
Imprese di assicurazione e riassicurazione	min: 30.000 € max: 10% del fatturato	min: 5.000 € max: 5 mil €	min: 30.000 € max: 7% del fatturato	min: 5.000 € max: 3,5 mil €
intermediari assicurativi e riassicurativi, int. assicurativi a titolo accessorio	min: 5.000 € max: 5 mil € o 5% del fatturato (se > 5 mil €)	min: 1.000 € max: 700.000 €	min: 5.000 € max: 3,5 mil € o 7% del fatturato (se > 3,5 mil €)	min: 1.000 € max: 500.000 €
Previdenza (fondi e casse)	min: 5.000 € max: 25.000 € <div>• Per il settore della previdenza, rispondono i componenti degli organi di amministrazione e di controllo, i direttori generali, i titolari delle funzioni fondamentali i responsabili delle forme pensionistiche complementari, i liquidatori e i commissari nominati.</div> <div>• Nei casi di maggiore gravità, la COVIP può dichiarare decaduti dall'incarico i componenti degli organi collegiali, il direttore generale, il responsabile della forma pensionistica e i titolari delle funzioni fondamentali.</div> <div>• In caso di più violazioni della stessa disposizione, soggiace alla sanzione prevista per la violazione più grave, aumentata sino al triplo.</div>			
Emittenti di token; Servizi di cripto-attività	min: 30.000 € max: 5 mil € <div>o 12,5% del fatturato (se &gt; 5 mil €) per token</div> <div>o 5% del fatturato (se &gt; 5 mil €) per crypto</div>	min: 5.000 € max: 700.000 €	min: 30.000 € max: 3,5 mil € <div>o 9% del fatturato (se &gt; 3,5 mil €) per token</div> <div>o 3,5% del fatturato (se &gt; 3,5 mil €) per crypto</div>	min: 5.000 € max: 550.000 €

\* Include sanzioni per le relative terze parti  
\*\* Includono la possibilità di interdizione dalle funzioni ricoperte da 6 mesi a 3 anni (in tutte le Entità Finanziarie nazionali)





# PwC View: Benchmark di mercato

# Profilo della Survey

**300+** clienti DORA a livello EMEA

- Banking & Capital Markets
- Insurance
- Asset & Wealth Management
- Payment Institutions
- Altre entità (SGR, IMEL, ICT Service provider,...)

## Obiettivo



Identificare il livello di maturità del mercato EMEA rispetto ai requisiti DORA, coerentemente alle attività ritenute essenziali rispetto alle fasi di adeguamento riconducibili ai piani di remediation tipicamente realizzati dalle istituzioni finanziarie

## Ambiti oggetto di indagine

**1**

### **Gli Essenziali al 17/01/2025**

Attività con effetti a partire dall'applicazione del Regolamento (es. Reporting verso le Autorità) o di scoping delle attività operative e tecnologiche

**2**

### **Processi, Metodologie e Procedure DORA**

Attività di definizione ed implementazione delle metodologie, processi e procedure previste ed in carico alla singola Banca, anche valorizzando e monitorando quanto eseguito dai fornitori ICT laddove applicabile

**3**

### **Operazionalizzazione DORA (2025+)**

Attività per la messa a terra ed automatizzazione tanto dei processi quanto dei requisiti tecnologici previsti da DORA per le Banche (oltre ai fornitori ICT)

# Le peculiarità di una vista per Settori (1/3)

## 1. Gli Essenziali al 17/01/2025

Attività con effetti a partire dall'applicazione del Regolamento (es. Reporting verso le Autorità) o di scoping delle attività operative e tecnologiche



### FUNZIONI ESSENZIALI O IMPORTANTI (Scoping)

**Definizione, implementazione e manutenzione** di un framework che identifichi e classifichi tutte le funzioni aziendali, nonché quelle essenziali o importanti (FEI), con relativo modello per la mappatura.



### IMPATTI ORGANIZZATIVI & CAPACITY MANAGEMENT

Definizione delle ricadute operative (effort e staffing) a seguito della ripartizione delle responsabilità per il controllo dei rischi ICT e di Sicurezza e dell'avvio delle azioni d'intervento prioritarie.



### REGISTRO TERZE PARTI

Creazione di un registro relativo alle informazioni degli accordi contrattuali con fornitori di servizi ICT (incluse le quarte parti) e di un **processo (accountability, manutenzione)** volto alla condivisione annuale del contenuto di tale registro alle Autorità di Vigilanza.



### GESTIONE DEGLI INCIDENTI

Rafforzamento nella gestione end-to-end del processo di Incident Management mediante l'adozione di una metodologia strutturata per la classificazione e la quantificazione degli impatti derivanti dagli incidenti ICT e delle minacce informatiche.



**FSI:** Effettua la segnalazione degli incidenti ICT in base alle informazioni condivise dal/i fornitori ICT ed aggregate con le proprie.

Banking	INS	AWM	Payment	Altri Soggetti FS
✓	✓	✓	✓	✓
✓	✓	▶	▶	⏸
▶	▶	▶	▶	▶
✓	✓	✓	✓	✓



# Le peculiarità di una vista per Settori (2/3)

## 2. Processi, Metodologie e Procedure DORA

Attività di definizione ed implementazione delle metodologie, processi e procedure previste ed in carico alla singola Banca, anche valorizzando e monitorando quanto eseguito dai fornitori ICT laddove applicabile



### FRAMEWORK PER LA GESTIONE DEL RISCHIO ICT

Definizione/Evoluzione del framework per la gestione dei rischi ICT, processi e flussi informativi. Messa in opera e manutenzione dello stesso



### CONTINUITÀ OPERATIVA E ICT CONTINUITY

Definizione/aggiornamento della politica di continuità operativa e dei relativi modelli operativi (ad es. BIA evoluta), messa in opera e manutenzione dello stesso



### MONITORAGGIO CONTRATTUALISTICA DELLE TERZE PARTI

Definizione di procedure e controlli per il monitoraggio dei Fornitori ICT. Analisi e revisione delle clausole contrattuali



### TEST DI RESILIENZA OPERATIVA DIGITALE

Definizione della metodologia e del Piano di Test di Resilienza, includendo tutte le tipologie di test e le attività di lessons learned.

**FSI:** Prevede ed effettua un programma di test completo, verificando eventuali report di test condivisi dal/i fornitori ICT e facendo monitoraggio degli stessi



### FORMAZIONE E TRAINING ICT

Definizione/aggiornamento di un piano di formazione in ambito ICT



### IT SERVICE MANAGEMENT

Definizione dei processi e procedure di Sicurezza e IT Service Management (ad esempio acquisto, sviluppo e maintenance dei sistemi ICT, ICT change management)



### ANALISI DEL LANDSCAPE TECNOLOGICO

Analisi di soluzioni tecnologiche, processi e procedure in essere, identificare e definire le priorità di intervento in ambito tecnologico

**FSI:** Identifica la lista completa delle soluzioni tecnologiche, anche in base a quanto condiviso dal/i fornitori ICT per quanto oggetto di contratto. Identificazione e definizione degli interventi tecnologici di ownership della FSI

Banking	INS	AWM	Payment	Altri Soggetti FS
✓	✓	▶	▶	▶
▶	▶	▶	▶	▶
▶	▶	▶	▶	▶
✓	✓	▶	▶	▶
✓	✓	✓	✓	✓
✓	✓	▶	▶	▶
✓	✓	▶	▶	▶









































































# Le peculiarità di una vista per Settori (3/3)

## 3. Operazionalizzazione DORA (2025+)

Attività per la messa a terra ed automatizzazione tanto dei processi quanto dei requisiti tecnologici previsti da DORA per le Banche (oltre ai fornitori ICT)

**Punti di Attenzione**  
Valutazione di strategie di Technology portfolio rationalization

	<b>DORA Integrated Controls</b> (anche tramite Managed Services).
	<b>ICT &amp; Cyber Risk Management End-to-End</b> RAF, Scenari, impact tolerance, integrazione con BCM outcomes.
	<b>TPRM operationalization</b> Finalizzazione contratti, workflow, definizione use case, controlli I e II linea verifica SLA, automatizzazione tramite tool (anche tramite Managed Services).
	<b>Threat Intelligence</b> Funzionale a definizione scenari, formazione CdA, event detection & early warning, incident response & follow up (anche tramite Managed Services).
	<b>Manutenzione mappatura FEI</b> Tramite processi e tecnologie Asset Management & Visibility, orchestratori, manutenzione 3 e 4 parti.
	<b>Incident Management</b> Includendo skill , capability, capacity e adozione / evoluzione tecnologie per tutte le fasi di processo, da early warning a follow up (Integrazione log, SIEM; SOC).
	<b>Identity Governance, Access Management, Privileged Access Management</b> Inclusa Ricertificazione Profili Abilitativi, rivisitazione modelli operativi, ruoli, con di visibilità, adozione/estensione di tool (anche tramite Managed Services)
	<b>Secure Endpoint Management</b> Inclusa visibility, vulnerability, patching (anche tramite Managed Services)
	<b>Digital Operational Resilience Testing</b> Esecuzione dei test di resilienza operativa, coinvolgendo i fornitori laddove applicabile ed integrando gli stessi nei processi BAU (anche tramite Managed Services)
	<b>Technologies evolution</b> Estensione di scope / nuove funzionalità / ulteriori soluzioni tecnologiche a presidio degli scenari di rischio (Data Security, Network, Application Security)

Banking	INS	AWM	Payment	Altri Soggetti FS
				
				
				
				
				
				
				
				
				
				
				
				
				
				



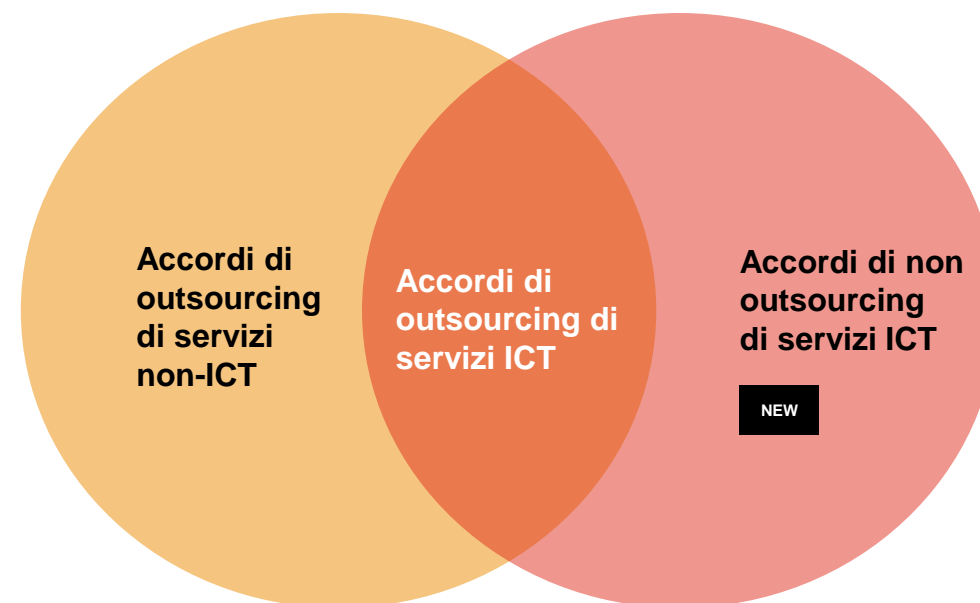
# 4

## Focus on: Gestione delle Terze Parti

# *Non solo DORA: Orientarsi nei requisiti normativi in ambito Terze Parti*

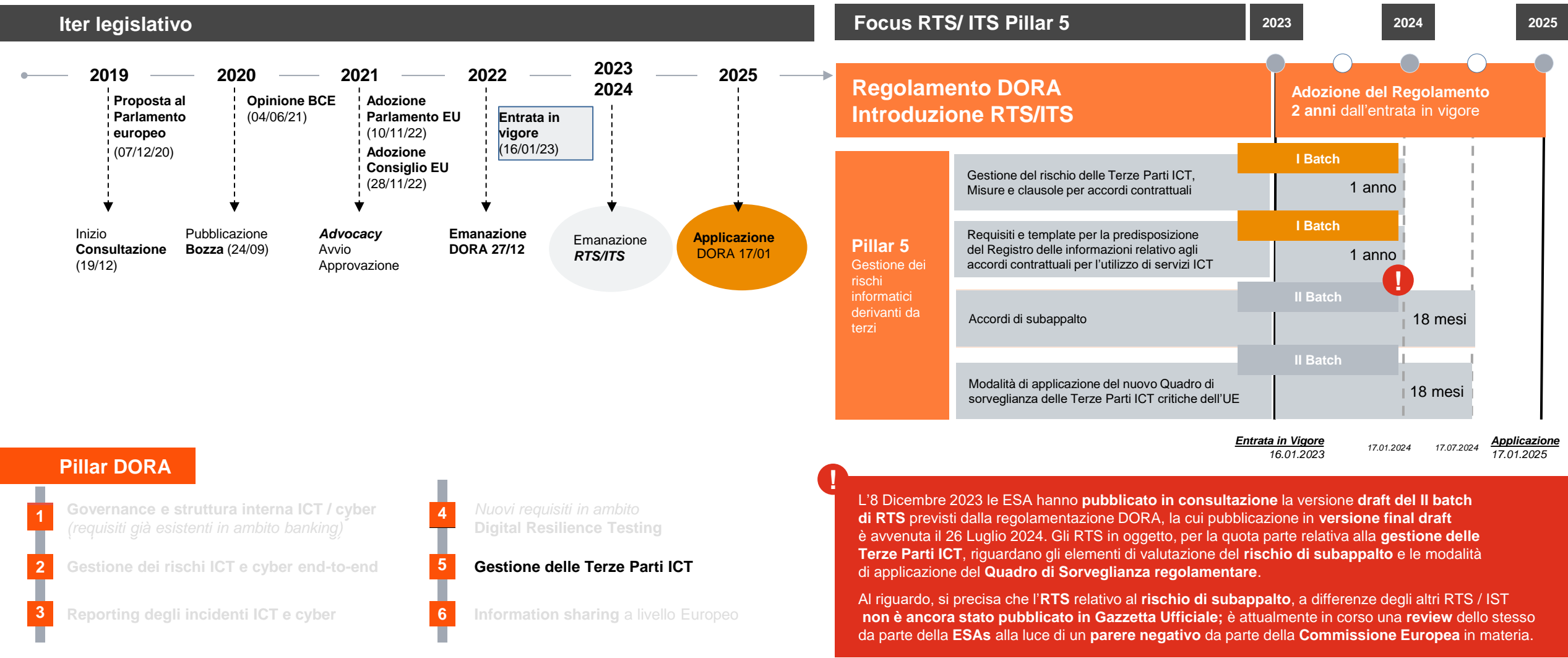
Il **Regolamento DORA**, nell'ambito del **Capo V «Gestione dei rischi informatici derivanti da terzi»**, introduce **requisiti normativi** per la gestione delle **Terze Parti** che forniscono **servizi ICT**.

Una delle  **differenze principali**  tra le **EBA Guidelines e le regolamentazioni nazionali** ed il **Regolamento DORA** è rappresentata dal **perimetro** di riferimento: il **Regolamento DORA** regola **tutti gli accordi contrattuali per l'utilizzo di servizi ICT** prestati da fornitori terzi, senza distinzione tra accordi di **esternalizzazione** e **non esternalizzazione**.



Si specifica che, alla luce dell'introduzione del Regolamento DORA, la volontà dell' **AdV** sembrerebbe essere quella di **armonizzare il quadro normativo in ambito Terze Parti**, con una **progressiva prevalenze dei requisiti DORA** su altre normative

# Normative per la gestione delle forniture di servizi ICT (1/2)





# Normative per la gestione delle forniture di servizi ICT (2/2)

## I Batch

Consultazione conclusa in data 11.09.23, pubblicazione RTS/ITS finale in Gazzetta Ufficiale **avvenuta** il 17.01.24



### REGOLAMENTO DELEGATO (UE) 2024/1773

del 13 marzo 2024 che integra il regolamento (UE) 2022/2554 per le norme tecniche di regolamentazione che precisano il contenuto dettagliato della politica relativa agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC

- Ruoli, responsabilità e requisiti per le diverse fasi del **ciclo di vita dei fornitori terzi di servizi ICT**
- Maggiore specificazione di ulteriori requisiti in merito a:
  - **Risk Assessment**
  - **Due diligence**
  - Valutazione dei **conflitti di interesse**
  - **Elementi contrattuali minimi**
  - **Controlli e Monitoraggio** durante il rapporto contrattuale
  - **Strategia d'uscita**



### REGOLAMENTO DI ESECUZIONE (UE) 2024/2956

del 29 novembre 2024 che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) 2022/2554 del parlamento europeo e del consiglio per quanto riguarda i modelli standard in relazione al registro delle informazioni

- Struttura del **registro delle Terze Parti ICT e requisiti di compilazione**
- Ruoli, responsabilità e processi di **manutenzione/aggiornamento** per LE, subappalto e holding
- Template del **registro delle Terze Parti ICT, chiavi relazionali e descrizione dettagliata** dei singoli campi

## II Batch

Consultazione conclusa in data 04.03.24, pubblicazione RTS in versione *final draft* **avvenuta** il 26.07.24. RTS non ancora pubblicato in Gazzetta Ufficiale



**Final Report - Draft RTS** to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554

- Condizioni per il **subappalto di servizi ICT a supporto di Funzioni essenziali o importanti** o di parti materiali di esse da parte di fornitori terzi
- **Requisiti di dettaglio per la valutazione del subappalto** in termini di:
  - **Due diligence**
  - **Risk Assessment**
  - **Monitoraggio**
  - **Elementi contrattuali minimi**

# Gestione delle Terze Parti: organizzazione, processi e tooling e reporting (1/3)

## Organizzazione

Per garantire il corretto funzionamento del framework di gestione delle Terze Parti, è necessario il **coinvolgimento di diverse Funzioni e attori** con ruoli e responsabilità, tra cui:

### Prima linea di difesa

#### Business Owner

- Manifesta la **necessità** di attivare una **nuova esternalizzazione / fornitura** ed **avvia** il processo di **valutazione del rischio**

#### Acquisti

- Presidia l'**approvvigionamento di servizi** e la **negoiazione contrattuale** con la Terza Parte

#### (Entry point)

- Presidia il **processo** di gestione delle Terze Parti ICT, facilitando la **comunicazione** tra **Business Owner**, la **funzione Risk Management** e le **Funzioni Esperte**

#### Funzioni esperte

- Definiscono i **controlli** e le **misure tecniche** di **gestione del rischio** da applicare per la **valutazione dei propri ambiti di competenza**
- Sono **coinvolti** nelle **valutazioni di rischio** per la formulazione di **opinion**

### Seconda linea di difesa

#### Risk Management

- Definisce il **Framework metodologico** per la gestione del rischio Terze Parti
- Definisce e applica i **controlli di II livello**
- Rivede le **valutazioni** effettuate dalle Funzioni di I livello, in particolare in caso di un livello di **rischiosità elevato** associato al servizio (i.e., rischio inerente) e alla Terza Parte (i.e., *add-on*)

#### Compliance

- È coinvolta ove opportuno nell'analisi di **Due Diligence** sui **fornitori**
- Esprime eventuali **compliance opinion** in fase di **valutazione di esternalizzazioni / forniture più rilevanti**
- Effettua **valutazioni** su **ambiti di rischio** specifici, tra cui la **valutazione dei conflitti di interesse**
- Effettua ove opportuno **controlli di II livello** sugli **ambiti di rischio presidiati**

# Gestione delle Terze Parti: organizzazione, processi e tooling e reporting (2/3)

## Processi

Il framework di gestione delle Terze Parti comprende un **processo E2E di gestione delle Terze Parti** («Processo TPRM») si compone di **5 macro-fasi: Identificazione e Selezione** del servizio, **Risk Assessment** e Due Diligence della Terza Parte, **Ingaggio** del Provider, **Monitoraggio** delle condizioni di performance/ rischio del contratto e fase conclusiva di **Fuoriuscita dagli accordi contrattuali**.



La **mappatura Servizio – Processo – Funzione** rappresenta un **elemento di input** al framework TPRM

## Identificazione e Selezione

Valutazione della rischiosità intrinseca del servizio

- Classificazione dell'accordo in **ICT/ Non ICT**
- Classificazione dell'accordo in **outsourcing/ non outsourcing**
- **Collegamento** tra il **servizio ICT** fornito dalla Terza Parte e **processo/ funzione** secondo la tassonomia interna dell'istituto
- Identificazione degli **attributi di servizio rilevanti** (i.e., perimetro rischi / aree di indagine) e **calcolo del rischio inerente**

## Ingaggio

Stesura del contratto

- Identificazione delle **clausole contrattuali** e delle **misure tecniche di sicurezza** da porre in essere per il presidio del rischio
- Stesura del **Main body contrattuale** quale documento per la formalizzazione dell'accordo tra le parti
- Identificazione degli **indicatori chiave** e della relativa **frequenza/ profondità per il monitoraggio** delle performance del Provider

## Fuoriuscita dagli accordi contrattuali

Cessazione dell'accordo

- **Esecuzione dell'exit strategy** per la fuoriuscita dagli accordi con la Terza Parte
- **Minimizzazione degli impatti** sui clienti dell'Istituto e sugli obblighi normativi

## Risk Assessment

Due Diligence e valutazione dei controlli

- **Due diligence del fornitore** sulla base di informazioni finanziarie/ reputazionali/ di compliance a disposizione dell'istituto
- **Valutazione del Control Resilience Rating della Terza Parte** basato sulla capacità del Provider di mitigare il rischio associato al servizio
- Calcolo del **rischio residuo dell'accordo** contrattuale
- **Predisposizione dell'exit strategy** per la fuoriuscita dagli accordi contrattuali

## Monitoraggio

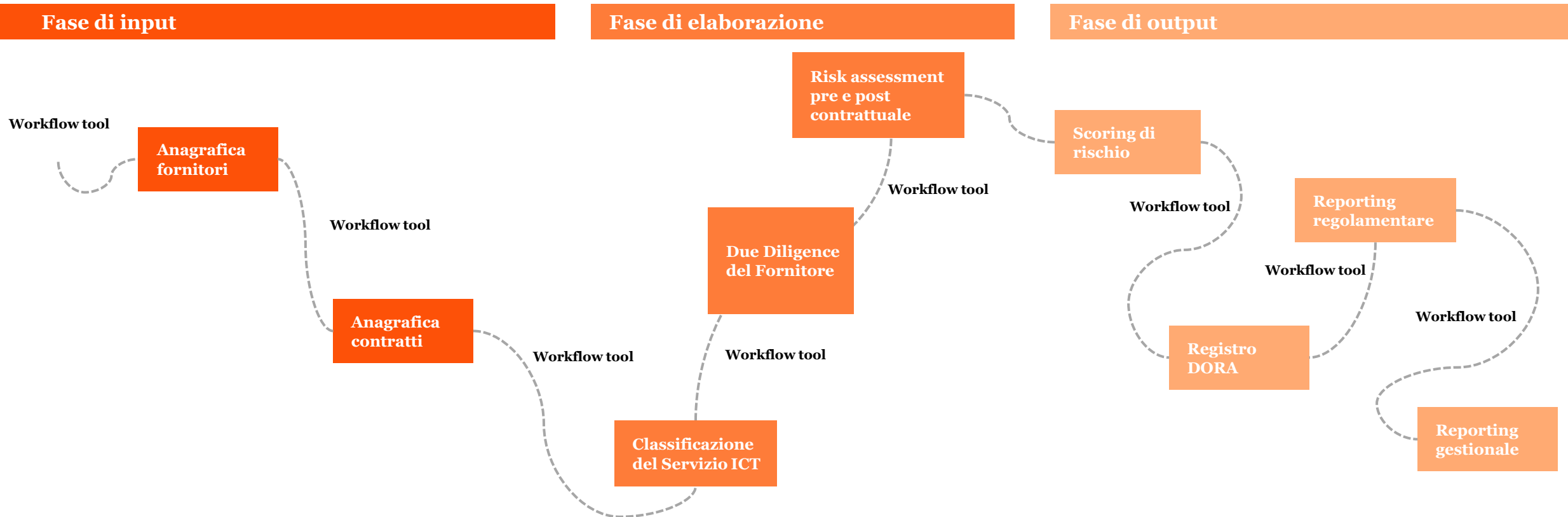
Valutazione nel continuo della Terza Parte

- **Valutazione di performance e rischio** associato alla Terza Parte durante tutta la vita del contratto
- Capacità di **intercettare eventuali controversie** tra le parti (e.g., mancato rispetto degli SLA del contratto, *breach* contrattuale)
- Esecuzione del **processo di Escalation** in presenza di controversie insorte tra il Gruppo e la Terza Parte
- **Reperforming periodico** del Risk Assessment sulla base degli esiti del monitoraggio

# Gestione delle Terze Parti: organizzazione, processi e tooling e reporting (3/3)

## Tooling e Reporting

Considerando la **complessità** del **processo di gestione delle Terze Parti**, una **best practice** è dotarsi di un **workflow tool** che permetta la gestione delle informazioni da raccogliere / produrre durante il processo. Il tool dovrebbe essere in grado di recuperare in **input informazioni presenti negli attuali processi** / strumenti aziendali, ed utilizzarle per alimentare processi quali la **valutazione del rischio Terze Parti**, la gestione del **Registro delle informazioni** e la **produzione di reportistica**:



# Thank you

# *PwC Cybersecurity&Resilience - Contatti*



**Paolo Carcano**  
**Partner**

+39 334 6896335  
[paolo.carcano@pwc.com](mailto:paolo.carcano@pwc.com)



**Samantha Trama**  
**Director**

+39 349 3360414  
[samantha.trama@pwc.com](mailto:samantha.trama@pwc.com)



**Cesare Cervini**  
**Manager**

+39 340 8687914  
[cesare.cervini@pwc.com](mailto:cesare.cervini@pwc.com)