BPER Factor

DORA: Gestione dei rischi da terze parti

L’approccio del Gruppo BPER per BPER Factor

29.05.2025

Il Gruppo BPER

Perimetro di applicabilità del DORA alle Legal Entity

Perimetro di applicazione

Il **perimetro di applicazione DORA ricomprende le entità del settore finanziario tradizionale**, come istituti di credito, borse e stanze di compensazione, gestori di fondi alternativi, società di gestione, imprese di assicurazione, istituti di pagamento, istituti di monetica elettronica, nonché fornitori di servizi di cripto-valuta, emittenti di cripto-asset ed emittenti di token.

LEs ricomprese nel perimetro di applicabilità del Regolamento DORA (art. 2)

Les, attualmente non ricomprese nel perimetro dell'art. 2 del Regolamento DORA, che saranno, alla luce dell'art. 15 della Legge 28 giugno 2024, n.90 «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici», soggette in futuro a un'estensione dei requisiti analoghi a quelli previsti dal DORA.

Il Gruppo BPER

Approccio progettuale complessivo all'adeguamento a DORA

Data l'entrata in vigore del Regolamento **Digital Operational Resilience Act (DORA)** dal **17/01/2025**, nel 2023 BPER Banca ha eseguito un'attività di assessment e successiva gap analysis, volta ad individuare eventuali scoperture. BPER Banca ha così predisposto una roadmap di dettaglio degli interventi necessari all'adeguamento al nuovo Regolamento europeo.

Questa progettualità ha previsto l'**esecuzione di attività specifiche di adeguamento alle previsioni della normativa DORA** su diversi ambiti, suddivise in **sette Stream principali:**

Security & Business Continuity

Risk Management

Gestione Terze Parti

Acquisti

Data Quality / Data Governance

IT

IT Governance

Il Gruppo BPER

Approccio progettuale complessivo all'adeguamento a DORA

- **A.1** Definizione della Strategia di Resilienza Operativa Digitale
- **A.2** Identificazione delle funzioni essenziali o importanti ai fini DORA
- **A.3** Revisione del piano di continuità operativa, dei piani di test e dei piani di risposta e ripristino
- **A.4** Aggiornamento del Piano di Comunicazione interna ed esterna
- **A.5** Revisione dei processi di abilitazione e ricertificazione
- **A.6** Attivazione del modello di ricertificazione
- **A.7** Evoluzione Training Sicurezza
- **A.8** Definizione del programma di Operational Resilience Testing
- **A.9** Evoluzione del processo di gestione degli incidenti di sicurezza
- **A.10** Evoluzione Threat Intelligence
- **A.11** Framework dei Threat Led Penetration Test in linea con TIBER-IT
- **A.12** Processo di prioritizzazione delle vulnerabilità
- **A.13** Revisione del framework di crittografia

Security & Business Continuity

Risk Management

Gestione Terze Parti

Acquisti

Data Quality / Data Governance

IT

IT Governance

Il Gruppo BPER

Approccio progettuale complessivo all'adeguamento a DORA

B.1 Revisione e aggiornamento della Metodologia di Analisi del Rischio ICT e di Sicurezza
B.2 Definizione di nuovi flussi informativi tra funzione di controllo e funzioni di primo livello
B.3 Revisione degli indicatori relativi al rischio ICT e Sicurezza (KRI) e identificazione delle soglie di tolleranza
B.4 Formazione degli Organi Aziendali
B.5 Formazione del personale
B.6 Integrazione della metodologia di valutazione del rischio fornitori
B.7 Controlli di secondo livello & indicatori del rischio sul TPRM

Security & Business Continuity

Risk Management

Gestione Terze Parti

Acquisti

Data Quality / Data Governance

IT

IT Governance

Il Gruppo BPER

Approccio progettuale complessivo all'adeguamento a DORA

C.1 Analisi sui processi di gestione Terze Parti, inclusi interventi sui template di reportistica
- Sintesi degli impatti di processo
- Template di reportistica verso organi apicali o autorità di vigilanza

C.2 Definizione del registro Terze Parti

C.3 Identificazione SLA standard per categoria merceologica e report di monitoraggio

C.4 Mappatura Funzioni CIF e applicativi a supporto
- Criteri per l'identificazione dei contratti critici a supporto delle Funzioni Essenziali o Importanti
- Mappatura Funzioni Essenziali o Importanti e applicativi a supporto
- Procedura per la manutenzione della mappatura delle Funzioni e relativi applicativi

C.5 Interventi di adeguamento dell'attuale modello di Exit Strategy (ES)

Security & Business Continuity

Risk Management

Gestione Terze Parti

Acquisti

Data Quality / Data Governance

IT

IT Governance

Il Gruppo BPER

Approccio progettuale complessivo all'adeguamento a DORA

D.1 Revisione dei processi di gestione delle Terze Parti e ruolo della Funzione Acquisti

Procedure aggiornate di accreditamento, valutazione e monitoraggio periodico dei Fornitori
Nuove procedure di accreditamento e valutazione dei subappaltatori
Modello di collaborazione tra le diverse funzioni coinvolte
Report per il rafforzamento della Funzione Acquisti

D.2 Revisione dei template contrattuali (clausole), in linea con le indicazioni DORA

Template contrattuali aggiornati rispetto ai requisiti previsti dal DORA

Security & Business Continuity

Risk Management

Gestione Terze Parti

Acquisti

Data Quality / Data Governance

IT

IT Governance

Il Gruppo BPER

Approccio progettuale complessivo all'adeguamento a DORA

E.1 **Modello di Data Quality in base al Rischio**

E.2 **Integrazione del Modello RID nella metodologia ICT Risk**

Security & Business Continuity

Risk Management

Gestione Terze Parti

Acquisti

Data Quality / Data Governance

IT

IT Governance

Il Gruppo BPER

Approccio progettuale complessivo all'adeguamento a DORA

F.1 Modello test di resilienza
F.2 Piani di Contingency
F.3 Modello di ripristino dei dati
F.4 Mappatura sistemi legacy
F.5 Change Management
F.6 Evoluzione incidenti operativi
F.7 Indicatori di allerta precoce
F.8 Valutazione costi annuali degli incidenti

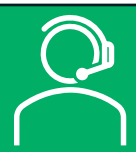
Security & Business Continuity

Risk Management

Gestione Terze Parti

Acquisti

Data Quality / Data Governance



IT

IT Governance

Il Gruppo BPER

Approccio progettuale complessivo all'adeguamento a DORA

G.1 Supporto integrazione dipendenze dei fornitori

Modello olistico per la gestione delle forniture ICT

Aggiornamento dell'attuale piano strategico IT di BPER in relazione alla gestione dei fornitori di terze parti

G.2 Supporto all'aggiornamento dei webinar relativi ai processi IT

Descrizione dei contenuti di dettaglio relativi ai processi IT da inserire all'interno dei webinar attuali al fine di consentire il loro aggiornamento

Security & Business Continuity

Risk Management

Gestione Terze Parti

Acquisti

Data Quality / Data Governance

IT

IT Governance

Focus su: Classificazione ai fini DORA

Rilevanza DORA e classificazione DORA COI del servizio di TP

1. Identificazione e definizione dell'ambito del servizio di Terza Parte | Criteri per identificare la rilevanza DORA

DORA, Art.3 – Definizioni | «Servizi ICT»: **servizi digitali e di dati forniti attraverso sistemi di TIC** a uno o più utenti interni o esterni su **base continuativa**, inclusi l'hardware come servizio e i servizi hardware, comprendenti la fornitura di assistenza tecnica mediante aggiornamenti di software e firmware da parte del fornitore dell'hardware, esclusi i servizi telefonici analogici tradizionali

Criteri

1 Categorie di servizio ICT [1]

1. *ICT project management*
2. *ICT Development*
3. *ICT help desk and first level support*
4. *ICT security management services*
5. *Provision of data*
6. *Data analysis*
7. *ICT, facilities and hosting services*
8. *Computation*
9. *Non-Cloud Data storage*
10. *Telecom carrier*
11. *Network infrastructure*
12. *Hardware and physical devices*
13. *Software licensing (excluding SaaS)*
14. *ICT operation management (including maintenance)*
15. *ICT Consulting*
16. *ICT Risk management*
17. *Cloud services: IaaS*
18. *Cloud services: PaaS*
19. *Cloud services: SaaS*

2 Base continuativa

Il Regolamento DORA non esplicita la dimensione di "base continuativa", dunque si rimanda all'interpretazione dell'entità finanziaria per declinare il requisito stesso

Quanto riportato sotto risponde all'interpretazione del requisito «su base continuativa» da parte di BPER:

- Servizi ICT erogati sulla base di un contratto con una durata maggiore di 12 mesi
- Servizi ICT erogati sulla base di un contratto con una durata inferiore a 12 mesi ma con possibilità di rinnovo (inteso come tacito o espresso contrattualmente)

Un servizio è un **servizio ICT nell'ambito del Regolamento DORA** nei seguenti casi:

- **Servizi ICT** che rientrano in una delle categorie DORA e che sono **su base continuativa**

Note	*Selezionare più di una voce in caso di diversi servizi ICT all'interno del medesimo contratto*	*Valutare la base continuativa per ogni servizi ICT all'interno del medesimo contratto*
Owner compilazione	*Il proponente è supportato da Sicurezza e IT*	*Il proponente è supportato da Esternalizzazioni*

[1] *L'elenco deriva dalle categorie di servizi ICT declinate in Annex III – ITS on the standard templates for the purposes of the register of information*

Rilevanza DORA e classificazione DORA COI del servizio di TP

1. Identificazione e definizione dell'ambito del servizio di Terza Parte | Criteri per identificare la classificazione DORA COI

Il Regolamento DORA introduce il perimetro di **servizi ICT a supporto delle CIF - Critical or Important Functions**, normando previsioni aggiuntive rispetto ai soli servizi DORA relevant (es. clausole contrattuali aggiuntive, compilazione di specifici campi all'interno del Registro delle Informazioni DORA)

Criteri

1 Elenco delle CIF che il servizio potrebbe supportare

Si rimanda allo Stream A – Security & Business Continuity per la lista delle Critical or Important Functions - CIF identificate

*Risulta necessario prevedere un **flusso informativo sempre aggiornato** fra il **CMDB che censisce le CIF** e lo **strumento target** che verrà utilizzato ai fini della **valutazione del servizio** di Terza Parte in **ottica DORA***

2 Livello di dipendenza dal servizio ICT della funzione/funzioni supportate [1]

- ***Not significant***
- ***Low reliance**: in case of disruption of the services, the supported functions would not be significantly impacted (no interruption, no important damage) or disruption can be resolved quickly and with minimal impact on the function/s supported*
- ***Material reliance**: in case of disruption of the services, the supported functions would be significantly impacted if the disruption lasts more than few minutes/few hours, and the disruption may engender damages, but still manageable*
- ***Full reliance**: in case of disruption of the services, the supported functions would be immediately and severely interrupted/damaged, for a long period*

Un servizio è un **servizio DORA COI – Critical or Important** nei seguenti casi:

- Servizio ICT che supporta **almeno una CIF** e il **livello di dipendenza** del servizio ICT è **«Material» o «Full»**

Note

Selezionare il processo prevalente oppure, nel caso in cui non sia possibile identificarlo, selezionare l'opzione «Cross» specificandone il razionale

Valutare il livello di reliance per il processo prevalente, oppure in ottica worst-case in caso di opzione «Cross»

Owner compilazione

Il proponente è supportato da Continuità operativa

[1] *L'elenco deriva dalle categorie di servizi ICT declinate in Annex III – ITS on the standard templates for the purposes of the register of information*

Focus Stream C (Gestione Terze Parti) e D (Acquisti)

Cosa prevedevano i processi interni in caso di affidamento a soggetti Terzi di servizi ICT (1/2)

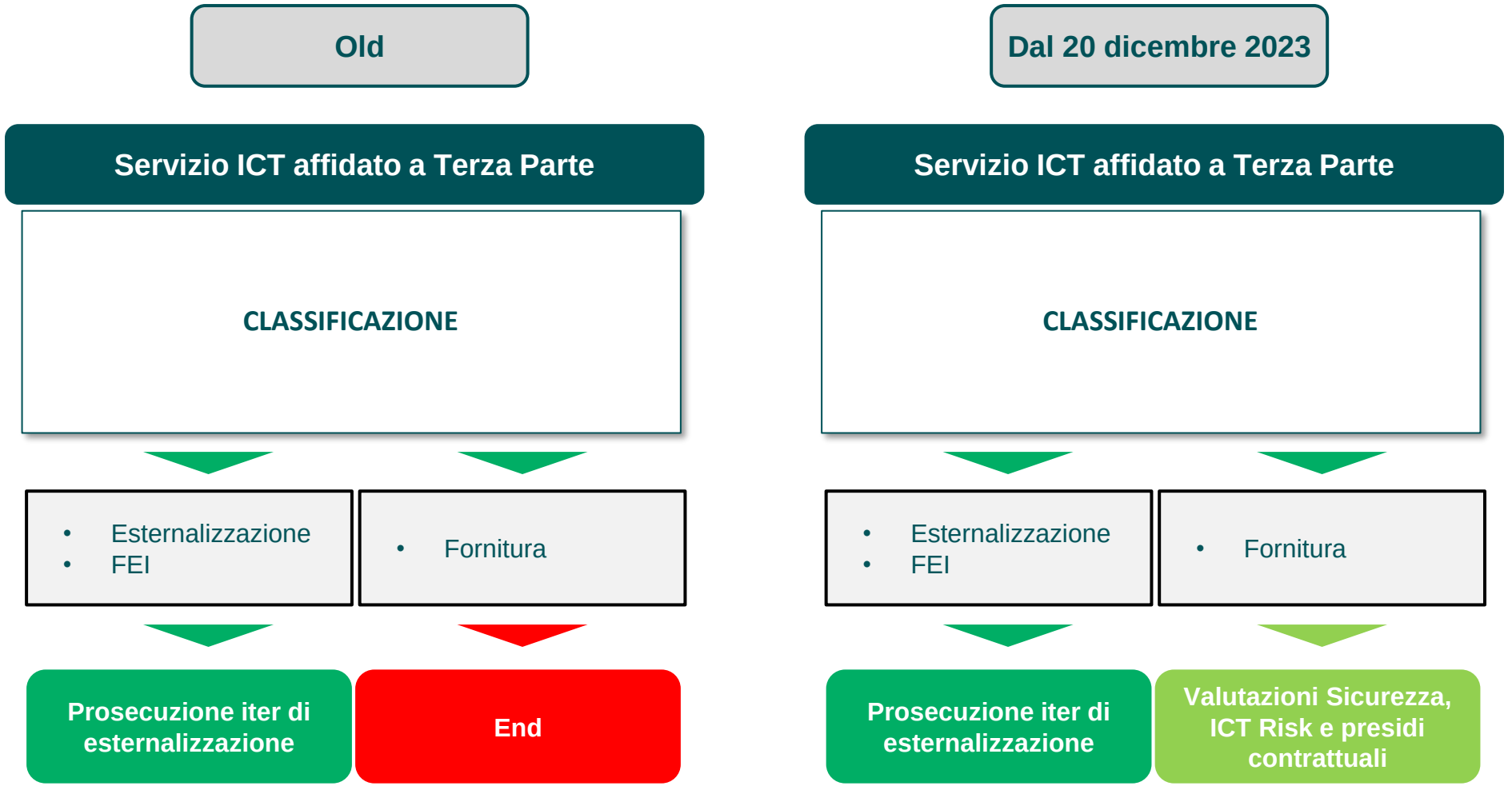
40° Aggiornamento Circolare 285

Il ricorso a soggetti terzi

Le banche che ricorrono a soggetti terzi per la prestazione di servizi ICT al di fuori di un rapporto di esternalizzazione applicano la Sezione 1.2.3 degli Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza.

Con l'emanazione del Regolamento del Processo di Esternalizzazione di Funzioni Aziendali approvato dal C.d.A. del 20 dicembre 2023 il ricorso a soggetti terzi in ambito ICT deve essere sottoposto a specifiche valutazioni, anche in caso di classificazione come fornitura, nell'ambito del Processo di Esternalizzazione.

Cosa prevedevano i processi interni in caso di affidamento a soggetti Terzi di servizi ICT (2/2)

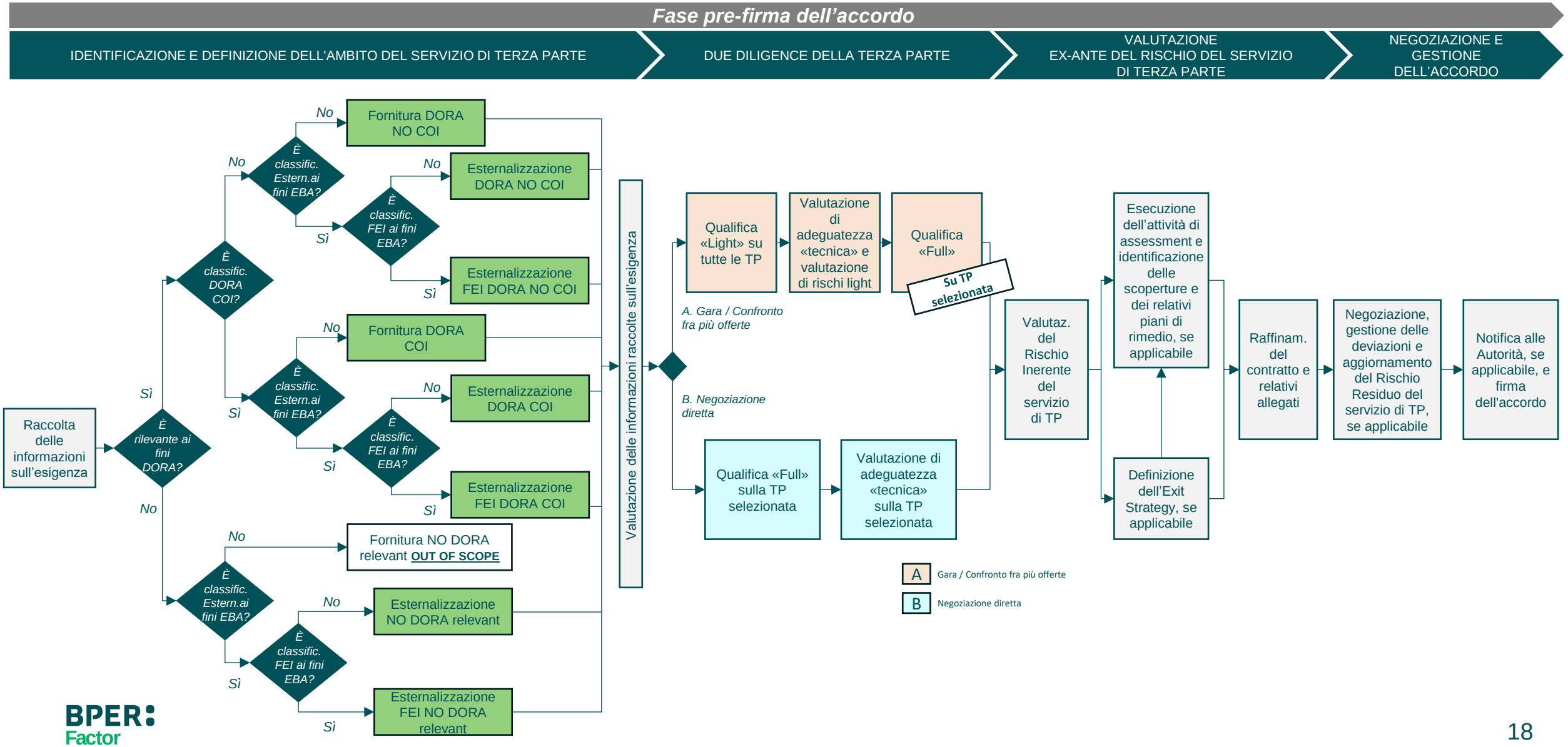


BPER: Factor

Sintesi nuovo processo DORA

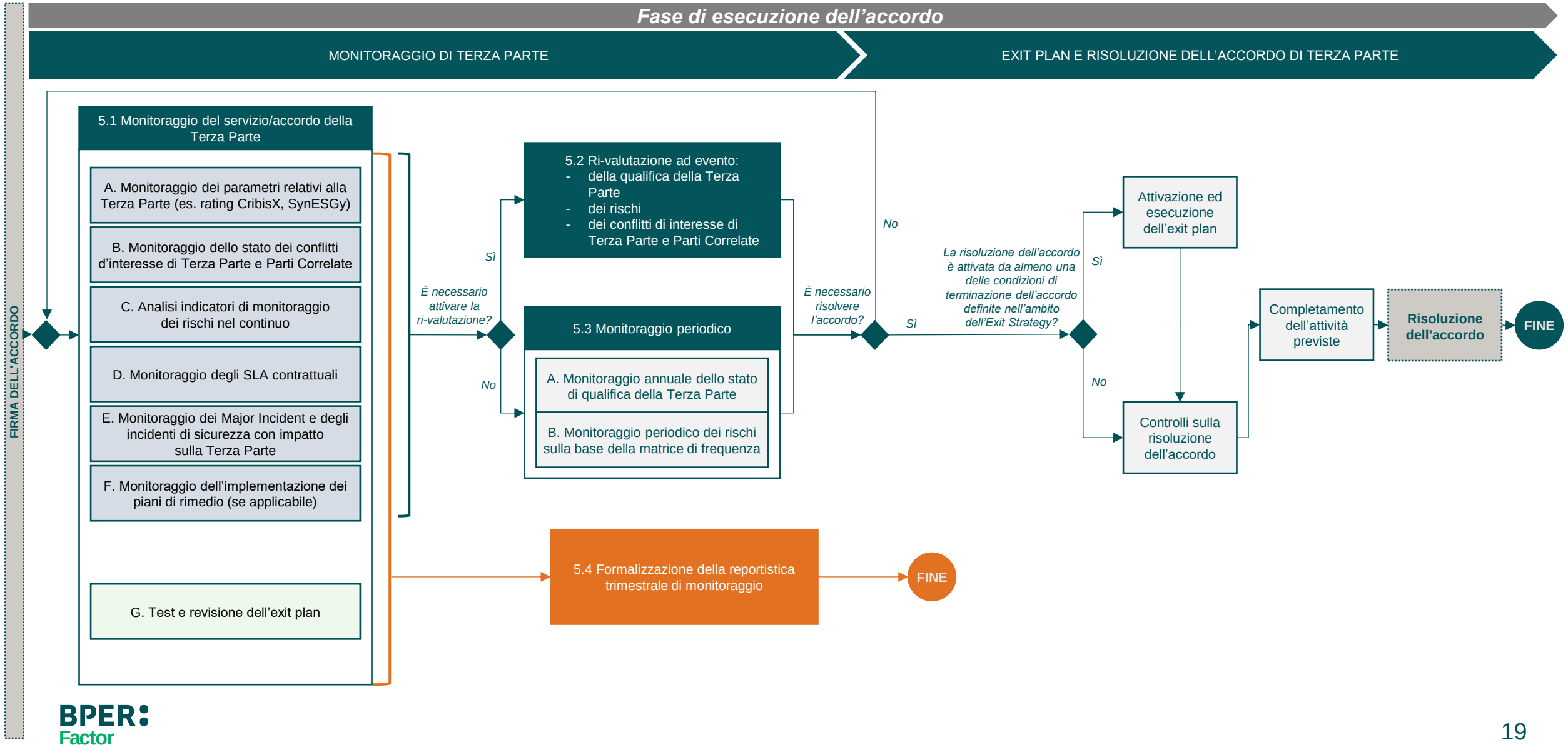
Live dal 17 gennaio 2025 - Integrato con il processo di esternalizzazione di funzioni aziendali

Overview del processo target DORA di gestione delle Terze Parti



BPER Factor

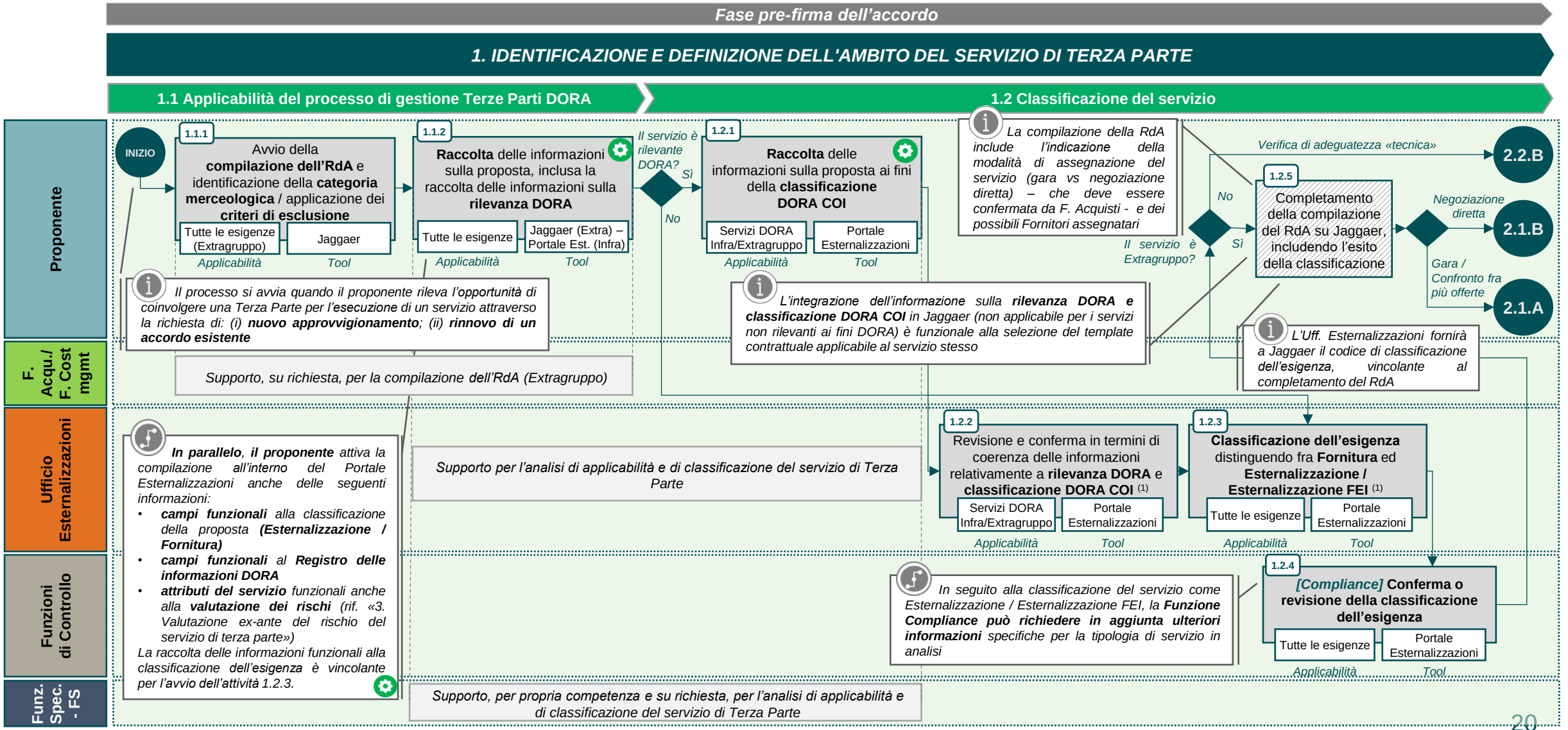
Overview del processo target DORA di gestione delle Terze Parti



Processo target DORA di gestione Terze Parti

ESTRATTO

1. Identificazione e definizione dell'ambito del servizio di Terza Parte



(1) A valle del completamento dell'attività 1.2.3, **per tutti i servizi non rilevanti ai fini DORA** si rimanda ai **processi attuali** secondo il "Regolamento del processo di acquisto e ciclo passivo" e il "Regolamento del processo di Esternalizzazione di funzioni aziendali"

Focus su: Specifiche per BPER Factor

Specifiche per BPER Factor

Aspetti già operativi anche per le Legal Entity del Gruppo attualmente escluse dal perimetro DORA

Società ex 106 TUB	▪ Allo stato attuale queste Legal Entity sono fuori dal perimetro di applicazione DORA. Tuttavia, alla luce dell'art. 15 della Legge 28 giugno 2024, n.90 «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici», saranno soggette in futuro a un'estensione dei requisiti analoghi a quelli previsti dal DORA. Rimangono invece applicabili, come ad oggi, le componenti di processo relative alle Linee Guida EBA sull'Outsourcing.
Tutte le società del Gruppo in Perimetro DORA	▪ Sarà necessario che tutte le società attualmente o prospetticamente in perimetro DORA pianifichino una verifica degli accordi in essere in ambito ICT e programmino gli interventi necessari per sottoporre tali contratti al processo con lo scopo di regolarizzare classificazioni e contratti ai fini DORA.
Società del Gruppo non allineate informaticamente che non hanno la Funzione Acquisti accentrata in Capogruppo	▪ Per le società che non hanno accentrato in Capogruppo la Gestione degli Acquisti, le attività di **raccolta delle informazioni necessarie ai fini della qualifica dei fornitori** (Light e Full), della valutazione di adeguatezza e dei rischi Light dovranno essere effettuate in autonomia; ▪ L'innesco del processo valutativo DORA, come avvenuto fino ad ora per EBA, sarà di tipo Organizzativo; ▪ Verrà predisposto un template dove dovranno essere raccolte, in una fase preliminare alla conclusione dell'RDA, tutte le informazioni necessarie per le **classificazioni** ai fini DORA e EBA; ▪ Il Proponente della Legal Entity dovrà farsi parte attiva per il recupero e la gestione di tali informazioni; ▪ Il template verrà processato dagli applicativi di Capogruppo. ▪ Sono in corso verifiche per consentire l'accesso al Portale Esternalizzazioni della Capogruppo anche alle Società Non allineate Informaticamente per consentire il data entry delle informazioni richieste anche ai fini DORA

BPER:
Factor

Grazie per l’attenzione