# Rischio Terze Parti e Outsourcing: L'implementazione di un framework di risk management

## Adeguamento alle Linee guida in materia di accordi di outsourcing

Settembre 2020

# Esternalizzazione – Contesto Normativo

## *Normativa esterna*

European Banking Authority (EBA) ha pubblicato il 25 Febbraio 2019 il Final Report relativo alle **«Linee guida in materia di accordi di outsourcing»**, fissando la data di adozione negli ordinamenti nazionali e di entrata in vigore entro il 30 Settembre 2019.

Banca d'Italia il 12 Novembre **2019** ha informato EBA di volersi conformare agli orientamenti sull'outsourcing a far data dal **30 settembre 2020.**

**Precedentemente, con il 28° Aggiornamento Circ. 285 del Luglio 2019,** aveva adottato le Linee Guida limitatamente «all'esternalizzazione del sistema informativo e di risorse ICT a fornitori di servizi cloud: «*all'esternalizzazione del sistema informativo e di risorse ICT a fornitori di servizi cloud, gli intermediari applicano, le raccomandazioni in materia di esternalizzazione a fornitori di servizi cloud, emanate dall'EBA*»**.**

**BdI non ha previsto ulteriori proroghe**

## *Normativa interna*

*Normativa interna attualmente in vigore*

«***Policy di Gruppo in materia di esternalizzazione di funzioni aziendali***»

«***Procedura di valutazione delle esternalizzazioni di processi/funzioni aziendali e successivo monitoraggio degli outsourcers***»

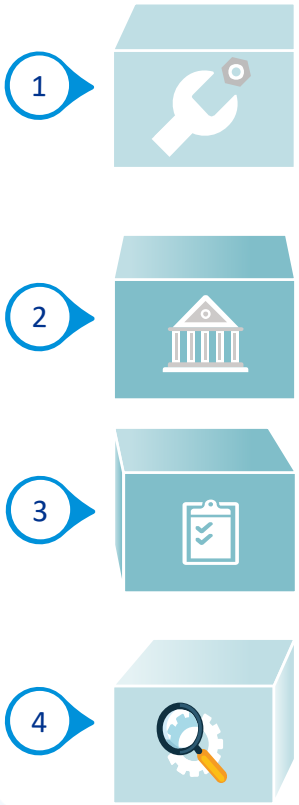
# Executive summary (1/2)

- A partire da 30 settembre 2019 le banche avranno **2 anni di tempo** (Dicembre 2021) per adeguare i contratti già sottoscritti
- La banche devono implementare un efficace "**Outsourcing framework**" che permetta al **Consiglio di Amministrazione** di essere **consapevole** della rilevanza degli accordi di outsourcing e del conseguente livello di dipendenza da terze parti e dei rischi ad essi associati.
- Il nuovo outsourcing framework presenta **elementi di novità** quale il registro delle esternalizzazioni ed elementi per i quali è richiesto un **maggior livello di dettaglio**, normativa interna, processo di esternalizzazione, governance e monitoraggio continuo dei fornitori di servizi
- Le banche hanno l'obbligo di **monitorate la qualità e le performance** di attività, processi e servizi esternalizzati "nel continuo" ed effettuare dei risk assessment lungo tutto il processo di outsourcing.
- Per una valutazione **di tutti i rischi di outsourcing** (operational risk, reputational risk, step-in risk e concentration risk) le banche dovranno dettagliare maggiormente e svolgere risk assessment lungo tutto il ciclo di vita dell'outsourcer

# Executive summary (2/2)

- A loro volta le funzioni coinvolte e soprattutto le funzioni di controllo dovranno prevedere attività di controllo e monitoraggio nel continuo secondo un **approccio risk based**
- Le banche devono scegliere se attribuire la responsabilità di supervisione dei service provider ad una struttura dedicata "**Outsourcing function**" oppure ad un "senior staff member"
- Per la compilazione del nuovo "**registro delle esternalizzazioni**" richiesto dall'EBA, le banche devono analizzare e ricercare, sia nei **contratti** in essere sia nella documentazione interna le informazioni richieste per la compilazione dei campi obbligatori.
- Tutti i nuovi contratti dopo l'entrata in vigore dovranno contenere le clausole previste dalla normativa e quelli esistenti dovranno essere aggiornati in occasione della prima revisione (i.e sub-outsourcing, diritti di accesso ed audit, reporting ed assicurazione)

# Outsourcing framework (1/2)




### Policy di esternalizzazione

FOCUS 1

- La Politica deve contenere le principali fasi del ciclo di vita dell'accordo di outsourcing e definire i principi, le responsabilità e i processi in relazione all'outsourcing
- Il documento deve contenere almeno: (i) ruoli e responsabilità; (ii) pianificazione degli accordi di outsourcing; (iii) implementazione, monitoraggio e gestione degli accordi di outsourcing; (iv) documentazione e tenuta del registro; (v) exit strategy e processi di risoluzione del contratto

### Governance

- Best option: le Banche dovrebbero introdurre una "Funzione Outsourcing" direttamente responsabile nei confronti del management per il monitoraggio dei singoli accordi di outsourcing
- Il senior management e l'Outsourcing Officer/senior staff member devono assicurare la presenza di risorse, interne o esterne, sufficienti per assicurare la conformità alle Guidelines EBA

### Registro delle "outsourcing activities"

FOCUS 2

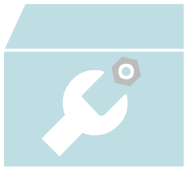
- Le Banche devono mantenere un registro (a livello di singola Legal Entity e a livello di Gruppo) di tutti gli accordi di outsourcing, e documentare e registrare tutti gli accordi di outsourcing, distinguendo tra l'outsourcing di funzioni critiche o importanti e altri accordi di outsourcing

### Conflitti di interesse

- Le Banche devono identificare, valutare e gestire i conflitti di interesse con riferimento agli accordi di outsourcing
- Nel momento in cui l'accordo di outsourcing crea un rilevante conflitto di interesse, inclusi quelli stipulati all'interno dello stesso Gruppo, le Banche devono intraprendere misure appropriate al fine di gestire tali conflitti

# Outsourcing framework (2/2)

5



## Business continuity planning

- Le Banche devono avere in essere, mantenere e periodicamente testare piani di business continuity appropriati con riferimento all'outsourcing di funzioni critiche o importanti
- I piani di business continuity predisposti a livello accentrato possono essere applicati a tutte le Entità del Gruppo
- I piani di business continuity devono considerare l'eventualità che la qualità del servizio relativa alla funzione critica o importante esternalizzata si deteriori o venga meno completamente

6

## Third-party risk management

- Le Banche devono valutare tutti i rischi prima dell'esternalizzazione e, come parte del monitoraggio, focalizzarsi sui rischi operativi, reputazionali e di concentrazione (outsourcing multipli in un'unica area o verso un unico provider)
- Inoltre, le Banche devono considerare il rischio risultante da sub-outsourcing delle attività sottostanti l'accordo o parte di esse

7

## Internal audit

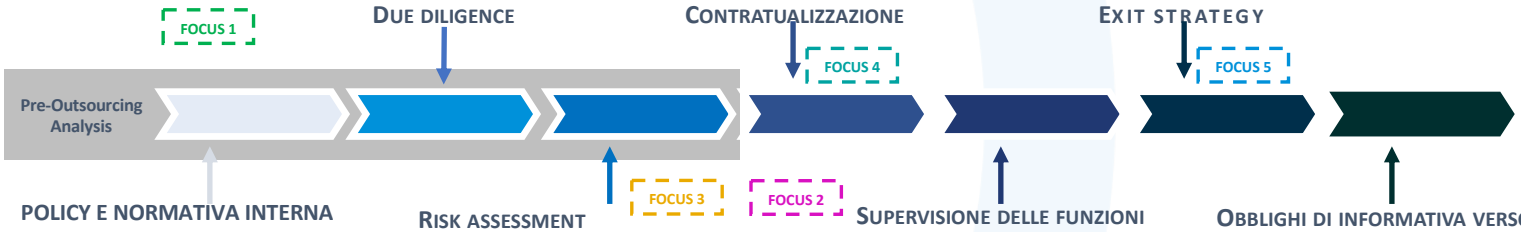
- Nel piano annuale di audit deve essere inclusa la revisione indipendente dell'efficacia del framework di outsourcing, effettuata seguendo un approccio risk based
- L'internal audit deve assicurarsi che il framework di outsourcing sia in linea con la strategia della Banca e che sia efficacemente implementato, assicurando l'adeguatezza, la qualità e l'efficacia della valutazione dei rischi sulle funzioni esternalizzate

# Il «nuovo» processo di outsourcing

- Verifica che il service provider abbia le appropriate e sufficienti competenze, capacità, risorse, struttura organizzativa e, ove applicabile, autorizzazione regolamentare a svolgere la funzione critica o importante in maniera affidabile e professionale

- Solidi accordi che assegnino diritti e obblighi
- Sub-esternalizzazioni delle funzioni critiche o importanti
- Sicurezza IT e dei dati
- Diritti di accesso, informazione e revisione
- Obblighi di reporting
- Target di performance
- Diritti di risoluzione del contratto

- Definire all'interno della Politica una chiara exit strategy per tutti gli accordi di outsourcing di funzioni critiche o importanti, che prenda in considerazione tutti i potenziali rischi e che preveda almeno la possibilità di risoluzione dell'accordo di outsourcing nel caso di fallimento del service provider e/o deterioramento rilevante del servizio prestato




**POLICY E NORMATIVA INTERNA**

- Criteri e processi definiti allo scopo di identificare le funzioni critiche o importanti
- Creazione del registro e definizione degli attributi
- Definizione dei controlli di rischio e performance
- Definizione di esternalizzazione vs acquisto di bene
- Definizione di FEI/FOI

**RISK ASSESSMENT**

- Valutare i rischi operativi derivanti dagli accordi di outsourcing
- La valutazione dei rischi deve includere specifici scenari, regolarmente aggiornati e adeguatamente riportati al management, nel momento in cui qualsiasi rischio venga identificato in relazione all'outsourcing di funzioni critiche o importanti

**SUPERVISIONE DELLE FUNZIONI ESTERNALIZZATE**

- Monitoraggio continuo dell'outsourcer secondo un approccio risk based e prevalentemente su CIF
- La Banca deve applicare la dovuta competenza, cura e diligenza nelle attività di monitoraggio
- La valutazione dei rischi deve essere regolarmente aggiornata e riportata al management
- Performance e qualità devono essere quantificate e stabilite attraverso KPI, KRI, auto certificazioni e verifiche indipendenti

**OBBLIGHI DI INFORMATIVA VERSO IL REGULATOR**

- La Banca deve fornire alle autorità competenti il registro di tutti gli accordi di outsourcing esistenti secondo un formato dati comune
- La Banca deve informare le autorità competenti in modo tempestivo riguardo agli outsourcing pianificati su funzioni importanti o critiche

mediolanum BANCA

# Policy e normativa interna

Focus 1

Le Politiche devono includere un maggior livello di granularità e dettaglio, in particolare:

| Tipo | Requisiti minimi |
|---|---|
| Nuovi | ▪ Criteri e processi definiti allo scopo di identificare le funzioni critiche o importanti<br>▪ Business Continuity Plan operativo in caso di malfunzionamento delle attività svolte dal service provider<br>▪ Exit strategy<br>▪ Documentazione e tenuta del registro |
| Più specifici | ▪ Identificazione e valutazione dei rischi connessi all'outsourcing<br>▪ Procedure per l'identificazione, valutazione, gestione e mitigazione dei potenziali conflitti di interesse dei service provider<br>▪ Valutazione e verifica su base continuativa delle performance dell'outsourcer |
| Già in essere | ▪ Responsabilità del management, linee di business, funzioni di controllo e chiunque svolga un ruolo all'interno dell'accordo di outsourcing<br>▪ Criteri adottati per la selezione dei service provider e la due diligence effettuata sui potenziali service provider<br>▪ Coinvolgimento del management nell'esternalizzazione del processo decisionale |

**Obbligjhi della banca**

Le Banche devono formalizzare normativa interna di dettaglio che descriva le principali fasi del **processo di esternalizzazione**, comprese le valutazioni iniziali, i principi base e le responsabilità delle singole attività all'interno del processo stesso

mediolanum BANCA

# "Registro" di tutti gli accordi di outsourcing

Focus 2

Deve essere istituito e aggiornato un registro di tutti gli accordi di outsourcing con le informazioni sotto riportate che sono **già presenti nei contratti** in essere, o possono essere recuperate da **documentazione interna** esistente, **responsabili di processo** o **funzioni di controllo**

## Requisiti comuni

- Identificativo univoco
- Descrizione delle attività in outsourcing (processi/ funzioni/ attività)
- Sottocategorie di attività in outsourcing
- Critica o importante?
- Accesso a dati sensibili da terze parti
- Beneficiario di servizi di terze parti
- Approvazione finale
- Sub-contraente?
- Nome
- Indirizzo del service provider
- Paese in cui il service provider è registrato
- LEI o numero di registro del service provider
- Capogruppo
- Service provider è parte del gruppo bancario?
- Paesi in cui il servizio è fornito
- Paesi in cui i dati sono archiviati
- Legge applicabile
- Costo stimato
- Operazione in cui le tempistiche sono cruciali

## Requisiti specifici per FEI/FOI

- Inizio del servizio/ultima data di rinnovo contrattuale
- Data di scadenza del servizio o prossima data di rinnovo contrattuale
- Ultimo audit
- Prossimo audit
- Data dell'ultimo risk assessment
- Breve riassunto dei risultati del risk assessment
- Sostenibilità
- Esempi di service provider alternativi
- Natura specifica dei dati da mantenere
- Operazione in cui le tempistiche sono cruciali

## Obblighi della banca

- **Fornire su richiesta** delle autorità di supervisione, l'**intero registro** degli accordi di outsourcing **o sezioni specifiche**.
- **Definire e aggiornare regolarmente** il registro degli accordi di outsourcing, tenendo traccia delle valutazioni e registrando i relativi esiti
- Le autorità di supervisione devono essere **prontamente informate** sui cambiamenti sostanziali/eventi significativi che possono impattare le attività

mediolanum BANCA

# Il risk assessment sul ciclo di vita dell'outsourcing (1/2)

Focus 3

- La componente chiave è il risk assessment che permette di selezionare, monitorare e decommissionare potenziali service provider


| Obblighi della banca |
|---|
| ▪ Valutazione dei rischi relativi al service provider proposto (i.e. rischio reputazionale, rischio operativo, rischio di concentrazione, potenziale sub-outsourcer e i rischi ad esso associati)<br>▪ Valutazione delle attività proposte (FOI vs non FOI) e impatto della definizione stessa<br>▪ Definizione di un nuovo insieme di controlli da implementare prima dell'approvazione dell'outsourcing (funzione di controllo integrata e funzione di outsourcing) |
| ▪ Effettuare una valutazione dei rischi continuativa sugli outsourcer<br>▪ Definizione di un framework di gestione del rischio di outsourcing con lo scopo di supervisionare le attività utilizzando approcci qualitativi/quantitativi (KRI e KPI) integrati tra le funzioni in capo al responsabile del processo, alle funzioni di controllo e al Data Protection Officer (DPO)<br>▪ Attività di evoluzione di valutazione del rischio (up / down grade rischio) |
| ▪ La valutazione dei rischi della exit strategy deve essere effettuata prima dell'avvio dell'attività in outsourcing:<br>o Valutazione ex-ante dei rischi delle potenziali opzioni di exit strategy (re-integrazione, identificazione di altre parti)<br>o Valutazione ex-ante dei piani di business continuity dei potenziali outsourcer |

mediolanum BANCA

# Il risk assessment sul ciclo di vita dell'outsourcing (2/2)

Focus 3

- Per valutare correttamente tutti I rischi connessi all'esternalizzazione è necessario sviluppare:

| | |
|---|---|
| 1 **Sviluppo di scenari di rischio** | Definizione di **plausibili scenari di rischio sull'outsourcing** considerando: (i) possibili eventi ad alto impatto e (ii) dati interni/esterni (i.e. perdite operative passate, raccomandazioni delle funzioni legali/audit) |
| 2 **Analisi di scenario** | **Sviluppo di *case study* per le analisi di scenario all'interno di un ampio perimetro di rischi da valutare*** inclusi, tra gli altri:<br>▪ Fattori sottostanti il verificarsi di potenziali rischi (i.e. processi, sistemi)<br>▪ Rischi associati alla concentrazione dell'outsourcing in termini di servizi erogati dallo stesso fornitore o fornitori correlati<br>▪ Funzioni interne, dati e sistemi coinvolti nell'accordo di outsourcing<br>▪ Contesto esterno relativo al fornitore dell'esternalizzazione (i.e. posizionamento geografico, normativa in vigore)<br>▪ Misure e controlli implementati dalla Banca e dal service provider per finalità di risk management, vigilanza e mitigazione (i.e. sicurezza, misure di *compliance*) |
| 3 **Assessment degli impatti** | **Valutazione qualitativa o quantitativa degli impatti legali, di compliance, informatici e reputazionali** legati agli scenari di rischio di outsourcing, sulla base del perimetro definito all'interno della valutazione del rischio |
| 4 **Validazione e monitoraggio dei rischi** | Validazione del framework di valutazione dei rischi e monitoraggio delle performance degli accordi di outsourcing al fine di eventuali **aggiornamenti e/o revisioni delle stime di rischio** per indirizzare l'implementazione di misure di mitigazione |

** Depending on the governance structure of the bank, the risk assessment should involve Risk Management (ops. risk + IT units) and expert functions (e.g. legal, compliance, security)*

mediolanum BANCA

# Contratti di outsourcing

Focus 4

- A partire dal 30 settembre 2019, i nuovi contratti o quelli soggetti a modifiche dovranno subire una completa revisione in accordo con le nuove *guidelines,* **con un periodo di transizione fino al 31 dicembre 2021**

- Main Areas

| CONDIZIONI GENERALI | SUB-OUTSOURCING | SICUREZZA DEI DATI | DIRITTI DI ACCESSO | RISOLUZIONE DEL CONTRATTO | EXIT STRATEGY |
|---|---|---|---|---|---|
| • Livelli di servizio<br>• Piani di contingency<br>• Assicurazione obbligatoria | • Dati<br>• Limiti<br>• Supervisione<br>• Diritti di risoluzione | • Compliance<br>• Monitoraggio<br>• Privacy | • Accessi della banca<br>• Accessi dell'autorità di supervisione | • Trasferimento della funzione<br>• Impegni del provider<br>• Periodo di transizione | • Strategie<br>• Soluzioni |

**Obblighi della Banca**

- Con l'entrata in vigore delle *guideline*, la Banca **dovrà aggiornare i contratti di outsourcing** tenendo in considerazione i nuovi requisiti, i quali verranno riportati all'interno dei contratti attualmente in essere, non oltre **Dicembre 2021**
- L'unità legale deve **cooperare con le funzioni rilevanti** (funzioni di controllo e responsabili di processo) **al fine includere tutti i dettagli dell'accordo** nei contratti o nei relativi documenti di supporto

mediolanum BANCA

# Exit strategies

Focus 5

- Nel caso di outsourcing di funzioni critiche o importanti, la Banca deve **sviluppare exit strategy adeguate** che siano in linea con la Politica e i piani di continuità aziendale.
- Tali exit strategy devono essere opportunatamente **documentate e testate.**

| Tipo | Requisiti minimi |
|---|---|
| BRAND NEW | ▪ Almeno per l'outsourcing di funzioni critiche o importanti, la documentazione delle exit strategy deve essere in grado di evitare la mancata conformità con la normativa tecnica e la sospensione delle attività di business<br>▪ All'interno della exit strategy devono essere assegnati i ruoli, le responsabilità e le risorse per gestire la risoluzione e il periodo di transizione<br>▪ La Banca deve testare e attuare analisi di impatto sull'exit strategy (i.e. costi potenziali, impatti, risorse umane, tempistiche)<br>▪ È necessario sviluppare un piano di transizione tra la fine di una fornitura e l'inizio di una nuova o la re-internalizzazione |
| EXISTING | ▪ Per l'outsourcing dei sistemi IT, la Banca è tenuta ad avere una exit strategy<br>▪ I contratti devono includere i dettagli relativi ai diritti di risoluzione in caso di fallimento del fornitore o in caso di deterioramento della qualità della servizio fornito dallo stesso |

**Obbligjhi della banca**

Al fine **di assicurare la continuità** delle proprie attività, la Banca deve valutare ex-ante le possibilità di:

1. **Reintegrare** le attività esternalizzate
2. **Trasferire** le attività verso un diverso fornitore
3. **Identificare accordi alternativi**

mediolanum BANCA

# Principali Impatti / Cantieri progettuali

***Deadline Normativa***

## 1. GOVERNANCE:

- ❑ Definizione del modello di governance — **30/09/2020**
- ❑ Aggiornamento Policy di Gruppo in materia di esternalizzazione di funzioni aziendali — **30/09/2020**

## 2. ADEGUAMENTO CONTRATTI:

- ❑ Mappatura e censimento nuovi attributi contratti (e adeguamenti informatici) — **30/09/2020**
- ❑ Definizione modello contrattuale per nuovi accordi di outsourcing — **30/09/2020**
- ❑ Adeguamenti degli accordi di outsourcing esistenti nel rispetto dei principi delle nuove linee guida — **31/12/2021**

## 3. REGISTRO DEI SERVIZI ESTERNALIZZATI:

- ❑ Registro che mappi tutti i servizi esternalizzati con un set di informazioni necessarie — **30/09/2020**

## 4. VALUTAZIONE RISCHI TERZE PARTI:

- ❑ Valutazione di tutti i rischi prima dell'esternalizzazione e, come parte del monitoraggio, focalizzarsi sui rischi operativi, reputazionali e di concentrazione — **30/09/2020**
- ❑ Exit plan (ex-ante) e formalizzazione contrattuale — **30/09/2020**
- ❑ Impatti sulla Business Continuity — **30/09/2020**

# Focus cantiere Governance

## 1. Funzione di Esternalizzazione

*«istituire **una funzione di esternalizzazione** o designare un membro del personale di grado superiore (senior staff member) che risponda direttamente all'organo di amministrazione (ad esempio, una persona che riveste un ruolo chiave nell'ambito di una funzione di controllo) e che sia **responsabile della gestione e supervisione dei rischi connessi agli accordi di esternalizzazione** nell'ambito del sistema dei controlli interni dell'ente **e della supervisione della documentazione degli accordi di esternalizzazione**»*

## 2. Modello di interazione

La costituzione della «funzione di esternalizzazione» sarebbe comunque integrata **nel contesto dell'attuale modello**, che prevede una **responsabilità distribuita tra diversi attori coinvolti in base alle relative competenze funzionali**:

- **Referenti contrattuali/operativi:** definizione dei termini operativi / SLA e monitoraggio performance
  - esp: ICT Governance, Cost&Services Governance
- **Divisione Acquisti**: standardizzazione dei processi di selezione, negoziazione e formalizzazione accordi
- **Risk Management** (con IT Risk & Security)**:** valutazione e gestione del **rischio di terze parti** (valutazione **FOI**)
- **Organizzazione:** valutazione **make/buy** e gestione **intercompany**, impatti **Business Continuity**
- **Compliance:** valutazione **FOI** e **controlli di secondo livello** (attualmente owner del processo)

# Modello di Governance – possibili soluzioni

| | *Principali Driver* | *Peso* | Funzione Risk Management<br>*Operational Risk Management* | Procurement, Safety & Corporate Services<br>Acquisti<br>Contract Management | Portafoglio Progetti & Sviluppo Organizzativo<br>Organizzazione<br>Business Continuity e Esternalizzazione |
|---|---|---|---|---|---|
| CORE | Supervisione dei processi / attori distribuiti (Policy/Procedure, monitoraggio, rendicontazione) | ++ | ✓ | | ✓ |
| | Aderenza normativa | + | ✓ | | |
| AMBITI DI SINERGIE e COMPETENZE | Contenuti Contrattuali | ++ | | ✓ | |
| | Valutazioni di rischio<br>Valutazione FOI | | ✓ | | |
| | Business Continuity | + | | | ✓ |
| | Registro repository (CMT) | | | ✓ | |
| | Governo della spesa – make/buy | | | | ✓ |

mediolanum BANCA

# Conclusioni

- Il tema outsourcing è diventato prioritario nell'agenda di BCE/Bankit
- Gli aspetti di governance e organizzativi non sono secondari. Al Risk Management è richiesto di partecipare in modo attivo nella gestione del rischio terze parti. Gestione che deve necessariamente contemplare un modello «diffuso» con il supporto di altre unità della banca.
- Il tema dell'exit strategy va affrontato con molta attenzione. Se può essere relativamente facile definirlo per un piccolo fornitore, diventa estremamente critico per un grosso fornitore (es: IT o Banca depositaria, etc.)
- Le nuove linee guida EBA ci danno la possibilità di rivedere criticamente e riconsiderare la definizione di FOI (o meglio FEI come si chiamano oggi)