SUPPLY CHAIN E FORNITORI: IL VALORE DEL MONITORAGGIO

Gli adempimenti e gli impatti legali della sicurezza informatica

Il Regolamento DORA impatterà su diverse categorie di attori

Obblighi Art. 1	Entità finanziarie	Fornitori ICT	Fornitori ICT critici
Gestione dei rischi ICT	IMPATTO DIRETTO	IMPATTO INDIRETTO	IMPATTO INDIRETTO
Gestione e reporting incidenti ICT	IMPATTO DIRETTO	IMPATTO INDIRETTO	IMPATTO INDIRETTO
Test di resilienza operativa digitale	IMPATTO DIRETTO	IMPATTO INDIRETTO	IMPATTO INDIRETTO
Condivisione delle informazioni	IMPATTO DIRETTO	IMPATTO INDIRETTO	IMPATTO INDIRETTO
Rischi ICT derivanti da terze parti	IMPATTO DIRETTO	IMPATTO DIRETTO	IMPATTO DIRETTO
Quadro di sorveglianza dei fornitori terzi di servizi di TIC Critici	NESSUN IMPATTO	NESSUN IMPATTO	IMPATTO DIRETTO

N.B.: Art. 28 c. 5 Le entità finanziarie possono stipulare accordi contrattuali soltanto con fornitori terzi di servizi TIC che soddisfano standard appropriati in materia di sicurezza delle informazioni

Gli adempimenti e gli impatti legali della sicurezza informatica

TENDER STRATEGY
Individuazione delle logiche e dei modelli delle specifiche esigenza d'acquisto, in coerenza con la strategia IT e di Sourcing

REQUEST FOR PROPOSAL
Definizione delle strategie di gara e redazione di documenti di richiesta di offerta che rispettino, oltre che le esigenze tecnico-funzionali aziendali, i requisiti normativi bancari

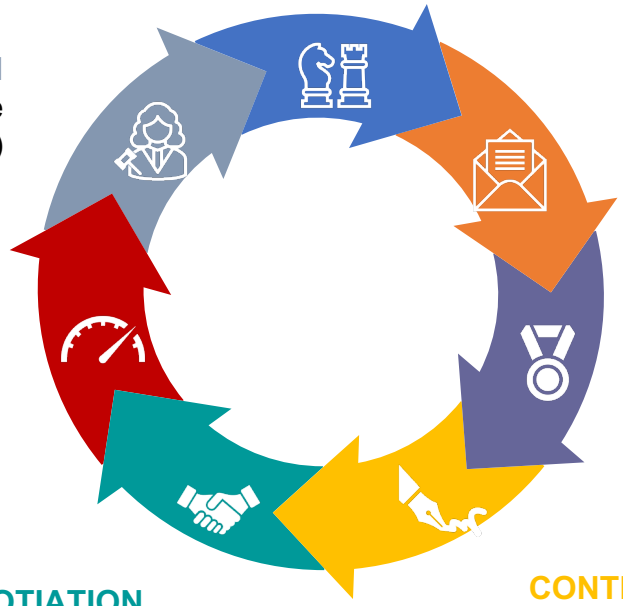
VENDOR SELECTION
Assegnazione dei livelli di rischio delle forniture e definizione di modelli di scoring su aspetti tecnici, economici e legali per la valutazione dell'accordo e le attività di *due diligence* sul fornitore

CONTRACT DRAFTING
Redazione di template contrattuali (o di singoli contratti) e dei relativi allegati che siano conformi alla normativa bancaria e che riducano al minimo i rischi della fornitura

NEGOTIATION
Negoziazione attenta del contratto e degli allegati tecnici, che garantisca la compliance normativa e la minimizzazione del rischio

VENDOR & CONTRACT MANAGEMENT
Adozione di sistemi efficaci di monitoraggio sulle performance del fornitore (KPI/SLA), predisposizione di piani di audit sulla compliance del fornitore, processo di gestione delle variazioni contrattuali

LITIGATION & DISPUTE RESOLUTION
Adozione di strategie di risoluzione delle controversie (giudiziali o stragiudiziali)



Il contenuto degli accordi contrattuali: clausole e negoziazione con i fornitori

Prima del 40° aggiornamento, le banche che ricorrevano all'esternalizzazione di servizi, processi e attività applicavano la Circolare 285/13 che, a sua volta, rinviava la disciplina contrattuale agli «Orientamenti in materia di outsourcing dell'EBA»

Con il 40° aggiornamento si distingue tra:

i. **Accordi di esternalizzazione del sistema informativo**
   i. **si applicano le clausole previste dal capitolo 3 e 4 del Titolo IV della Circ. 285/13 (per le FEI) e le clausole previste dagli «Orientamenti in materia di *outsourcing* dell'EBA». In aggiunta si applicano le due clausole relative «le misure e gli obiettivi in materia di sicurezza dell'informazione» e «le procedure di gestione degli incidenti operativi e di sicurezza»** (così come previsto dagli «Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza»)

ii. **Accordi stipulati con soggetti terzi al di fuori delle esternalizzazioni**
   i. **si applica la sezione 1.2.3 prevista dagli «Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza» e perciò le condizioni contrattuali relative «le misure e gli obiettivi in materia di sicurezza dell'informazione» e « le procedure di gestione degli incidenti operativi e di sicurezza»**

<u>Con il Reg. DORA agli accordi contrattuali per l'utilizzo dei servizi ICT si applicheranno le clausole contrattuali previste dall'art. 30 e quanto previsto dagli Orientamenti EBA in materia di outsourcing.</u>

In altri termini il Reg. Dora armonizza i principi relativi ai diritti contrattuali nell'ambito della catena di fornitura ICT al fine di fornire alcune garanzie minime per rafforzare la capacità delle entità finanziarie di monitorare efficacemente tutti i rischi informatici che insorgano a livello di fornitori di servizi terzi.
Tali principi sono complementari alla normativa <u>settoriale</u> applicabile all'esternalizzazione (Cons. 29) (ergo: il DORA si aggiunge, ma non si sostituisce alle normative settoriali quali quelle afferenti al mondo bancario e assicurativo)

Il contenuto degli accordi contrattuali: clausole e negoziazione con i fornitori

Le clausole contrattuali da applicare secondo le normative bancarie in vigore sono:

SERVIZI ICT (285/EBA ICT/DORA) (diversi dall'esternalizzazione)

- **Accordo con soggetto terzo**
- **Normativa:** Circ. 285/13 40°agg., **Sez. VI, Par. 3** che rimanda a *Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza.* Si aggiunge il Reg. DORA.

- **Clausole da prevedere**:
  - *EBA ICT (misure di sicurezza e di integrità e procedure sugli incidenti di sicurezza) E*
  - *DORA (Art. 30, par. 2 e/o 3)*

Non si applicano le clausole previste dalle Linee Guida EBA sull'esternalizzazione.

ESTERNALIZZAZIONE (EBA EST/DORA)

- **Accordo con fornitore di servizi ICT esternalizzati**
- **Normativa:** Orientamenti *in materia di outsourcing* (solo in parte, ovvero gli orientamenti che disciplinano tutti gli accordi di esternalizzazione). Si aggiunge il Reg. DORA.

- **Clausole da prevedere**:
  - *EBA EST (limitatamente alle clausole applicabili a tutti gli accordi esternalizzati (es. diritti di cessazione del contratto)*
  - *DORA (Art. 30, par. 2)*

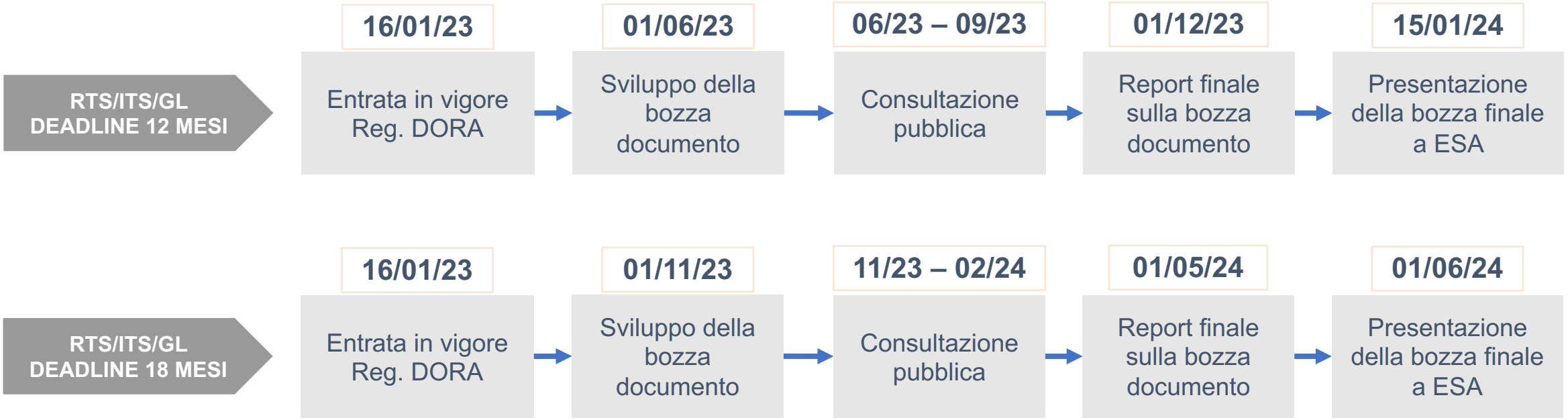
Non si applicano le altre previsioni contrattuali previste dalla Circolare 285/13 per le FEI.

ESTERNALIZZAZIONE FEI (285/EBA EST/DORA)

- **Accordo con fornitore di servizi ICT esternalizzati a supporto delle FEI**
- **Normativa: Circolare 285/13, Cap. 3 e 4** e **EBA** Orientamenti *in materia di outsourcing.* Si aggiunge il Reg. DORA.

- **Clausole da prevedere**:
  - *Clausole Cap. 3 e 4 della Circ. 285/13*
  - *EBA EST (tutte quelle previste dall'Orientamento 13 e quelle previste per tutti gli accordi di esternalizzazione)*
  - *DORA (Art. 30 par. 2 e 3)*

La regolamentazione tecnica standard (RTS) che sarà emessa nei prossimi mesi per dare attuazione ai principi contenuti nel Regolamento Dora



Le mosse e le aspettative del legislatore nazionale ed europeo

EBA EUROPEAN BANKING AUTHORITY

RTS su procedure di classificazione degli incidenti ICT e minacce informatiche
deadline 12 mesi

RTS sulla segnalazione di gravi incidenti informatici e TIC alle autorità
deadline 18 mesi

ITS sui dettagli da riportare nella segnalazione degli incidenti

GL sulla *stima dei costi/perdite derivanti da incidenti ICT gravi*

Studio di fattibilità di un Hub UE per la segnalazione degli incidenti
deadline 24 mesi

N.B.: EBA dirigerà la consultazione pubblica in materia di Incident Response

Le mosse e le aspettative del legislatore nazionale ed europeo

ESMA
European Securities and Markets Authority

RTS sugli elementi del quadro di gestione del rischio ICT
deadline 12 mesi

RTS sul livello di dettaglio richiesto nelle strategie di gestione dei fornitori terzi (TPP)
deadline 12 mesi

RTS sugli accordi contrattuali chiave per il subappalto di funzioni/servizi a supporto di funzioni critiche o importanti
deadline 18 mesi

RTS sulle informazioni che un fornitore terzo critico (CTPP) deve fornire alle autorità di vigilanza
deadline 18 mesi

RTS sulla nomina dei membri del Comitato congiunto
deadline 18 mesi

N.B.: ESMA dirigerà la consultazione pubblica in materia di ICT Risk management

Le mosse e le aspettative del legislatore nazionale ed europeo

ITS sul Registro delle informazioni relative agli accordi contrattuali con i fornitori nel settore delle TIC
deadline 12 mesi

GL sulla cooperazione nelle attività di sorveglianza dell'ESA
deadline 18 mesi

RTS sulla conduzione della supervisione
deadline 18 mesi

Consultazione per la designazione dei Fornitori terzi critici (CTPP)

N.B.: EIOPA dirigerà la consultazione pubblica in materia di Supervisione

Come cambia il ruolo del fornitore: l'integrazione del rischio informatico

Le entità finanziarie gestiscono i rischi informatici derivanti da terzi quali componenti integranti dei rischi informatici nel contesto del proprio quadro per la gestione di detti rischi ICT.

Il Regolamento DORA si propone l'obiettivo di realizzare un pieno e costante coinvolgimento delle persone che gestione i rischi ICT all'interno dell'azienda al fine di conseguire un elevato livello di resilienza operativa digitale.

In particolare, ai sensi **del Regolamento DORA**, l'organo di gestione deve adottare un approccio di sistema riguardante complessivamente:

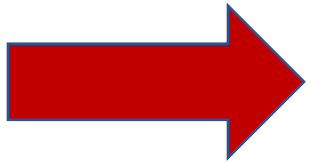
- tanto i mezzi per assicurare la resilienza dei sistemi di TIC;
- le persone (considerando 45 – art. 13 par. 6);
- i fornitori di servizi ICT (art. 30 – art. 13 par. 6),

e deve

predisporre strategie che promuovano, per ciascun livello dell'azienda e per tutto il personale, un forte senso di consapevolezza dei rischi informatici e l'impegno a osservare, a tutti, i livelli un una rigorosa igiene informatica.

Come cambia il ruolo del fornitore: l'integrazione del rischio informatico

- Tutti gli accordi con fornitori di servizi ICT devono essere **documentati in un registro** che deve essere aggiornato e messo a disposizione dell'autorità;
- Nella fase pre-negoziale è necessario:



identificare la **tipologia di servizio** (tassonomia)
effettuare ***due diligence*** dei fornitori
effettuare ***risk assessment*** sulla fornitura e sul fornitore
identificare eventuali **conflitti di interesse**
assicurarsi che il fornitore rispetti gli **standard ICT security**
esaminare rischi di **concentrazione**

- Le entità devono **adottare e riesaminare periodicamente la strategia per i rischi ICT** derivanti da terzi (inclusi subappalti, soprattutto extra UE);
- Le entità devono predisporre **strategie e piani di controllo, ispezioni e audit** in base alle tipologie di forniture di servizi ICT di cui si avvalgono;
- Le entità devono adottare ***exit strategy*** **e piani di transizione** che non compromettano la propria compliance normativa, la propria Business Continuity e i servizi forniti ai clienti, in particolare in caso di servizi ICT a supporto di FEI.

Come cambia il ruolo del fornitore: l'integrazione del rischio informatico

Le entità finanziarie elaborano programmi di sensibilizzazione sulla sicurezza delle TIC nonché attività di formazione sulla resilienza operativa digitale. **Tali programmi e attività di formazione riguardano i dipendenti e gli organi o ruoli coinvolti nella gestione dei rischi** (DORA)

Le entità finanziare **assegnano e riesaminano periodicamente le risorse finanziarie adeguate per programmi** di sensibilizzazione sulla sicurezza delle TIC e le attività di formazione sulla resilienza operativa digitale

Gli accordi contrattuali per l'utilizzo di servizi TIC **comprendono** le condizioni riguardanti **la partecipazione dei fornitori terzi di servizi TIC ai programmi di sensibilizzazione sulla sicurezza delle TIC e alle attività di formazione** sulla resilienza operativa digitale delle entità finanziarie