14:00-15:30
Sessione parallela 1.2

Il governo della resilienza esterna: valutazione, monitoraggio e presidio del rischio ICT delle terze parti nel framework DORA

Il radar della resilienza esterna

Strategia TPRM (Art.28)

Integrazione totale del rischio TIC nel framework globale di risk management dell'entità

Principio di inalienabilità: l'entità finanziaria mantiene sempre la responsabilità normativa assoluta delle attività esternalizzate.

Registro informazioni

Mappatura esaustiva e tracciamento rigoroso di tutti gli accordi contrattuali di servizi TIC (Art. 28(3))

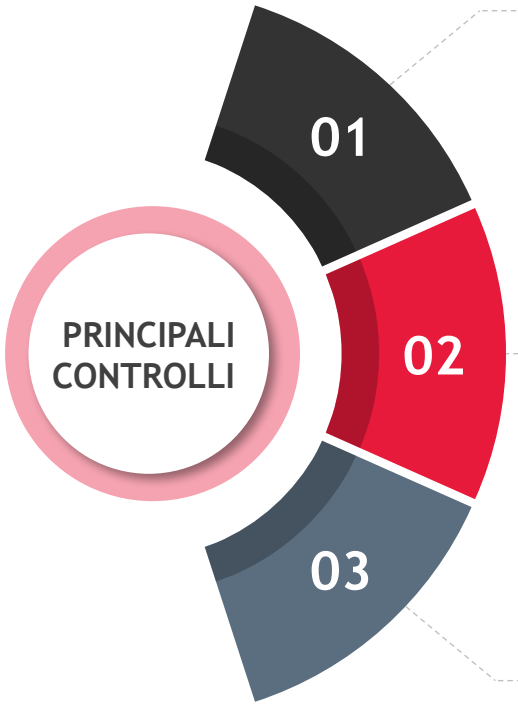
Richiede la distinzione netta tra fornitori generici e fornitori che supportano **funzioni essenziali o importanti (FEI)**.

Concentrazione (Art. 29)

Valutazione sistematica della dipendenza critica da singoli fornitori chiave

Focus sulle reali difficoltà di **sostituibilità** nel mercato e sull'aggregazione di contratti multipli su un singolo nodo tecnologico critico.

Controllo catena di sub-fornitura



CRITERI DI SELEZIONE (ART. 28(4))

Ingaggio limitato a fornitori in grado di garantire standard di sicurezza elevati e costantemente aggiornati.

RISCHIO 'QUARTA PARTE' (RTS SUBAPPALTO)

Mappatura estesa oltre il primo livello. Monitoraggio attivo dei subappaltatori che supportano funzioni FEI.

SECURITY GATES OBBLIGATORI

Analisi geopolitica per i paesi terzi e controllo a cascata per garantire policy di sicurezza inalterate su ogni livello.

Presidio contrattuale & gestione In-Life

DISPOSIZIONI OBBLIGATORIE (Art. 30)

La definizione dei requisiti minimi contrattuali rappresenta la prima barriera di difesa operativa:

- ✓ **SLA precisi:** inclusione di metriche sia quantitative (es. disponibilità dei sistemi) sia qualitative per valutare oggettivamente il servizio.
- ✓ **Localizzazione dati:** indicazione chiara dei paesi di transito e di memorizzazione dei dati sensibili.
- ✓ **Assistenza incidenti:** obbligo per il fornitore di cooperazione immediata e tempestiva in caso di emergenza informatica.

DIRITTI DI AUDIT E ACCESSO

Nessuna limitazione è tollerata per le attività ispettive e di vigilanza delle entità finanziarie:

- ✓ **Diritto incondizionato (Art. 30(3)(e)):** possibilità di programmare ispezioni on-site e audit fisici senza precondizioni ostative del fornitore.
- ✓ **Trasparenza totale:** cooperazione obbligatoria per garantire l'accesso ai log di sicurezza, ai sistemi operativi e alle infrastrutture di rete correlate al servizio.

Exit strategy & gestione End-of-Life

EXIT STRATEGY (ART. 28(8))

La dismissione programmata o improvvisa di un servizio TIC deve avvenire senza rischi operativi per l'entità:

- ✓ **Pianificazione ex-ante:** strategie di uscita codificate e pronte all'uso fin dal momento della firma del contratto.
- ✓ **No vendor lock-in:** proibizione di dipendenze tecnologiche esclusive che impediscono la sostituzione del fornitore per le funzioni essenziali.

TRANSIZIONE E RISOLUZIONE

Fattori di mitigazione e continuità aziendale durante la migrazione o risoluzione del servizio:

- ✓ **Periodi di transizione:** definizione contrattuale di tempi di preavviso prolungati e supporto proattivo del fornitore uscente.
- ✓ **Resilienza in risoluzione:** clausole che inibiscono l'interruzione dei servizi anche in pendenza di controversie o ristrutturazioni del fornitore.

Grazie per l'attenzione

✉ CONTATTI

federico.temporiti@bdo.it

marcello.fumagalli@bdo.it