SCS CONSULTING
make your future happen

# Overview dei principali impatti del Regolamento DORA in materia di ICT Third Party Risk Management

make your future happen

21 febbraio 2023

# Chi siamo

Siamo una società di consulenza di direzione, nata a **Bologna** nel 2001 dalla fusione di tre società presenti sul mercato da **oltre 20 anni** nel campo dei servizi professionali di **consulenza**, **formazione** e **valorizzazione** delle risorse umane

Il nostro obiettivo è **valorizzare** il capitale di **competenze** e di **relazioni** che oggi abbiamo, diventando sempre più un riferimento e un centro di **eccellenza** nel nostro ambito.

## La nostra **Mission**

"***Supportare*** *imprese e territori offrendo servizi e* ***soluzioni*** *per la creazione di* ***valore*** *e la realizzazione di una* ***crescita sostenibile***"


**22**
Anni

**150+**
Dipendenti

**185**
Clienti nel 2022

**417**
Progetti nel 2022

**MERCATI DI RIFERIMENTO**

| AREE DI COMPETENZA | FINANCE | INDUSTRIA E SERVIZI | P.A. & UTILITIES |
|---|---|---|---|
| CONSULENZA STRATEGICA E ORGANIZZATIVA | | | |
| PEOPLE & CHANGE MANAGEMENT | | | |
| SOSTENIBILITÀ | | | |

SCS CONSULTING

SCS CONSULTING

Un modello di consulenza **integrata** focalizzato su creazione di **valore** e realizzazione di una crescita **sostenibile**

Utilizziamo un modello di business in cui team di **professionisti** con competenze specifiche nei diversi settori agiscono in maniera integrata per **valorizzare** le più innovative esperienze e metodologie in grado di generare valore per i **nostri clienti**

# Il nostro DNA

## Visione & strategia
..dall'elaborazione delle **strategie**, alla riprogettazione del **business model e dell'offerta**

## Proattività commerciale
Supportiamo i nostri clienti nel migliorare la **proposizione**, le **organizzazioni** ed i **processi di vendita** in un contesto di continua evoluzione e crescita della **digital experience**

## Process Transformation
Accompagniamo i nostri clienti nella **gestione** profittevole dei **processi complessi**, volti a sviluppare **innovazione** ed **efficienza**

## Supporto alle persone & Change Management
Lavoriamo per le **persone** e con le persone, perché solo attraverso di loro si possono realizzare **strategie aziendali**, incrementi di performance, cambiamenti organizzativi e innovazione

## Audit, Risk & Compliance
Aiutiamo i nostri clienti nel disegno, implementazione, verifica e revisione dei modelli di **governance aziendale**: dal presidio dell'evoluzione regolamentare, alla definizione ed implementazione di modelli di Enterprise Risk Management e di Sistemi di Controllo Interno

## Digital Transformation
**Supportiamo** i nostri clienti nell'affrontare le **sfide** strategiche e implementative legate alla digital transformation: **tecnologiche**, **culturali**, **organizzative** e **manageriali**.

## Sostenibilità
Forbes Consulting Speciale 100 Responsibility 2020

La lunga tradizione sulle tematiche della sostenibilità ci consente di lavorare a partire dalle **strategie**, sui modelli di **governance** nonché sui **prodotti** e sui **processi**, ovviamente presidiando le tematiche più tradizionali come la **rendicontazione** ed i processi ad essa correlati.

SCS CONSULTING

# AGENDA WEBINAR

- Apertura evento
- Overview dei principali impatti del Regolamento DORA in materia di ICT Third Party Risk Management
- Intervista ad opinion leader di settore
- Q&A e chiusura evento

# Il Regolamento DORA (1/2)

L'iter approvativo del Regolamento DORA ha avuto avvio il 24 settembre 2020, quando la Commissione europea ha presentato la proposta in materia di resilienza operativa digitale (DORA), come parte integrante del più ampio **pacchetto sulla finanza digitale**, inteso a:

- sviluppare un **approccio comune allo sviluppo tecnologico;**
- garantire la **stabilità finanziaria**;
- promuovere la **protezione dei consumatori**.

### *Qual è l'obiettivo del Regolamento DORA?*

Definire un **quadro normativo uniforme e standardizzato** che consenta al settore finanziario di garantire la **resilienza operativa digitale**, ossia la capacità di creare, assicurare e riesaminare la propria integrità operativa da un punto di vista tecnologico, garantendo, direttamente o indirettamente, l'intera gamma delle capacità connesse alle ICT necessarie per garantire la sicurezza delle reti e dei sistemi informativi impiegati dall'entità finanziaria

### *Tempistiche*


## … contesto normativo assicurativo

**Framework EU**

- Direttiva Solvency II
- Regolamento GDPR
- Direttiva NIS / NIS II
- Direttiva CER
- EIOPA Guidelines(*)
- Framework TIBER EU

**Framework Nazionale**

- Reg. IVASS 38/2018
- Lettera al mercato 5/2018
- Framework & Strategia Nazionale di Cybersicurezza
- Guida nazionale TIBER-IT

**Principali framework Internazionali**

- Standard ISO
- Standard NIST
- Standard CIS-CSC
- Standard CSA-CCM

(*) Orientamenti EIOPA sulla sicurezza e sulla governance della tecnologia dell'informazione e comunicazione
Orientamenti in materia di esternalizzazione a fornitori di servizi cloud

# Il Regolamento DORA (2/2)

## *Quali gli ambiti di applicazione della DORA?*


## A chi si applica la DORA?

**Art.2 (Ambito di applicazione)**

- **(a) enti creditizi**
- **(b) istituti di pagamento**
- **(c) prestatori di servizi di informazione sui conti**
- **(d) istituti di moneta elettronica**
- **(e) imprese di investimento**
- (f) fornitori di servizi per le cripto-attività ed emittenti di token collegati ad attività
- (g) depositari centrali di titoli
- (h) controparti centrali
- (i) sedi di negoziazione
- (j) repertori di dati sulle negoziazioni
- (k) gestori di fondi di investimento alternativi
- (l) società di gestione
- **(m) fornitori di servizi di comunicazione dati**
- **(n) imprese di assicurazione e di riassicurazione**
- **(o) intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio**
- **(p) enti pensionistici aziendali o professionali**
- (q) agenzie di rating del credito
- (r) amministratori degli indici di riferimento critici
- (s) fornitori di servizi di crowdfunding
- (t) repertori di dati sulle cartolarizzazioni
- **(u) fornitori terzi di servizi di TIC**



SCS CONSULTING

# Perché l'attenzione sulla catena di fornitura? (1/5)

*[27] La dipendenza delle entità finanziarie dall'uso dei servizi TIC è causata in parte dalla loro necessità di adattarsi all'emergere di* ***un'economia mondiale digitale sempre più competitiva****, di accrescere la propria efficienza commerciale e di soddisfare la domanda dei consumatori. La* ***natura e la portata di tale dipendenza ha conosciuto negli ultimi anni un'evoluzione costante,*** *che ha prodotto una riduzione dei costi dell'intermediazione finanziaria, ha favorito l'espansione e la scalabilità delle imprese nello sviluppo delle attività finanziarie, offrendo d'altra parte un'ampia gamma di strumenti TIC per la gestione di complessi processi interni*

*[34] Oggi è evidente* ***una certa carenza di omogeneità e convergenza per quanto riguarda il monitoraggio delle dipendenze da terzi nel settore delle TIC e dei rischi informatici derivanti da terzi****. Nonostante gli sforzi per trattare l'esternalizzazione, come gli orientamenti dell'ABE in materia di esternalizzazione del 2019 e degli orientamenti dell'ESMA in materia di esternalizzazione a fornitori di servizi cloud del 2021, la* ***questione più ampia del contrasto del rischio sistemico potenzialmente derivante dall'esposizione del settore finanziario*** *a un ristretto numero di fornitori terzi critici di servizi TIC* ***non è adeguatamente affrontata dal diritto dell'Unione****. La carenza di norme a livello dell'Unione è* ***aggravata dall'assenza di norme nazionali su strumenti*** *e mandati che consentano alle autorità di vigilanza finanziaria di acquisire una valida comprensione delle dipendenze da terzi nel settore delle TIC e di* ***monitorare adeguatamente i rischi provocati dalla concentrazione di tali dipendenze***



SCS CONSULTING

# Perché l'attenzione sulla catena di fornitura? (2/5)


Il Regolamento DORA rimarca la necessità per gli enti di **definire chiari ruoli e responsabilità per la gestione del rischio ICT,** anche con riferimento al rischio ICT derivante da fornitori terzi. In particolare richiede:

Presenza di **canali di comunicazione verso l'Organo di Gestione**, per informarlo in merito a:
- **i) gli accordi conclusi con i fornitori terzi** di servizi ICT sull'uso di tali servizi;
- ii) le **eventuali modifiche importanti** riguardo ai fornitori terzi di servizi ICT;
- **iii) il potenziale impatto di tali modiche sulle funzioni essenziali o importanti soggette agli accordi** (incl. sintesi dell'analisi del rischio per valutare l'impatto di tali modifiche)

Istituzione di un ruolo al fine di **monitorare gli accordi conclusi con i fornitori terzi di servizi ICT**

Definizione di una **strategia olistica per le ICT** basata su una varietà di fornitori, che **indichi le principali dipendenze da fornitori terzi di servizi ICT**

**Mappatura dei processi dipendenti da fornitori terzi di servizi ICT,** anche identificando le interconnessioni con i fornitori che offrono servizi a supporto di funzioni essenziali o importanti

Predisposizione e test di **piani di continuità operativa delle ICT**, in particolare **per quanto riguarda le funzioni essenziali o importanti esternalizzate o appaltate** a fornitori terzi

Inclusione **nei programmi di sensibilizzazione sulla sicurezza delle ICT e di formazione** sulla resilienza operativa digitale **anche dei fornitori terzi di servizi ICT**



SCS CONSULTING

# Perché l'attenzione sulla catena di fornitura? (3/5)


Il Regolamento DORA definisce requisiti comuni in materia di **processo di gestione** degli incidenti ICT, **classificazione degli incidenti ICT e delle minacce informatiche** e modalità e contenuti per la **segnalazione** di gravi incidenti ICT all'Autorità

Obbligo per il fornitore terzo di servizi ICT di **prestare assistenza all'entità finanziaria senza costi aggiuntivi o a un costo stabilito ex ante**, qualora si verifichi un incidente connesso alle ICT relativo al servizio fornito all'entità finanziaria

Definizione da parte dei fornitori terzi critici di servizi ICT di processi per:

- **l'identificazione, il monitoraggio e la tempestiva segnalazione** alle entità finanziarie di incidenti significativi
- la **gestione e la risoluzione di tali incidenti**, in particolare con riferimento ad attacchi informatici

# Perché l'attenzione sulla catena di fornitura? (4/5)


Agli enti finanziari è richiesto di adottare un **approccio risk based nella definizione di un programma di test sui sistemi e strumenti ICT**, che includa test avanzati sotto forma di test di penetrazione basati su minacce **(TLPT)** con cadenza almeno triennale

I **TLPT riguardano alcune o tutte le funzioni essenziali o importanti** dell'entità finanziaria ed è effettuato sui sistemi attivi di produzione a supporto di tali funzioni. Le entità finanziarie **identificano tutti i sistemi, i processi e le tecnologie ICT sottostanti a supporto delle funzioni essenziali o importanti**, **compresi quelli sono stati esternalizzate o appaltate a fornitori terzi** di servizi ICT

Nel caso in cui i **fornitori di servizi ICT rientrino nell'ambito di applicazione dei Test di penetrazione basati su minaccia (TLPT),** l'entità finanziaria adotta le **misure necessarie per garantire la loro partecipazione** ai TLPT ed è responsabile per il rispetto del Regolamento DORA

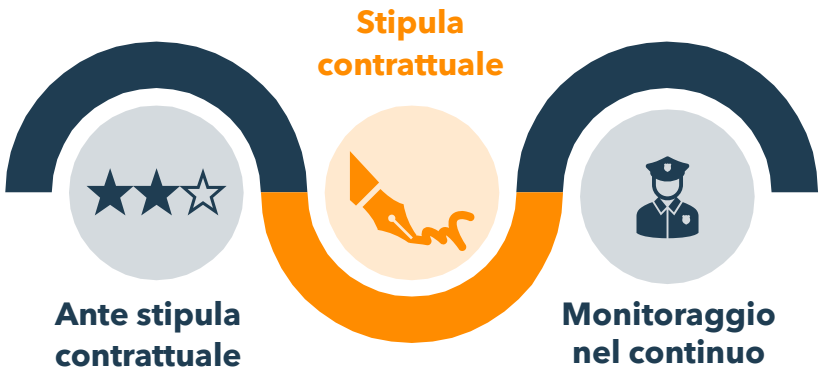
# Perché l'attenzione sulla catena di fornitura? (5/5)


Il Regolamento DORA chiede agli enti finanziari di dotarsi di un framework di gestione del rischio ICT che includa anche il **monitoraggio e la gestione dei rischi ICT derivanti da rapporto con fornitori di servizi ICT terzi**, estendendo il perimetro di verifica precedentemente regolato dalle ESAs anche ai contratti diversi da accordi di esternalizzazione

Adozione di una **strategia per i rischi informatici derivanti da terzi** (incl. una politica per l'uso di servizi ICT a supporto di funzioni essenziali o importanti prestati da terzi)

Istituzione di un **registro di informazioni su tutti gli accordi contrattuali per l'utilizzo di servizi ICT prestati da fornitori terzi,** documentando i contratti e distinguendo quelli a supporto di funzioni essenziali o importanti dagli altri

**Definizione di un framework di gestione del rischio ICT** derivanti da terzi, che copra **tutte le fasi del rapporto** di fornitura:



# ICT Third Party Risk Management


**Quali sono gli aspetti da considerare <u>prima di stipulare un accordo contrattuale</u> per l'utilizzo di servizi ICT?**

- **Valutazione impatto su funzioni essenziali o importanti:** verificare se l'accordo contrattuale riguardi l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti e, in tal caso, che i fornitori ICT possiedano gli standard di qualità più aggiornati ed elevati in materia di sicurezza delle informazioni
- **Risk assessment:** identificare e valutare i rischi relativi all'accordo contrattuale (incl. valutazione del rischio di concentrazione)
- **Due diligence:** effettuare i controlli di due diligence sui potenziali fornitori di servizi ICT, anche garantendo l'idoneità del fornitore nel corso del processo di selezione e valutazione
- **Analisi conflitti di interesse:** individuare e valutare potenziali conflitti di interesse che possano derivare dalla stipula dell'accordo

*«All'atto dell'identificazione e della valutazione dei rischi […] le entità finanziarie tengono conto altresì dell'eventualità che la prevista conclusione di un accordo contrattuale relativo a servizi TIC a supporto di funzioni essenziali o importanti possa avere una delle seguenti conseguenze:*

*a) la **conclusione di un contratto con un fornitore terzo** di servizi TIC **non facilmente sostituibile**; o*

*b) la **presenza di molteplici accordi contrattuali relativi alla prestazione di servizi TIC** a supporto di funzioni essenziali o importanti **con lo stesso fornitore** terzo oppure con fornitori terzi strettamente connessi […]»*

*Reg. DORA art. 29*

# ICT Third Party Risk Management


**Quali sono gli aspetti da considerare <u>in sede di stipula di un accordo contrattuale</u> per l'utilizzo di servizi ICT?**

- **Format contrattuale:** prevedere clausole e allegati contrattuali in linea con i requisiti minimi previsti dal Regolamento DORA
- **Clausole di risoluzione:** stabilire clausole per la risoluzione degli accordi contrattuali in caso di:
  - rilevanti **violazioni del quadro normativo vigente**,
  - **elementi rilevati in sede di monitoraggio** dei rischi ICT derivanti da terzi, che possano alterare i requisiti concordati nell'accordo contrattuale
  - **punti deboli del fornitore** emersi riguardo alla sua gestione complessiva dei rischi informatici
- **Strategie di uscita:** definire per i servizi ICT a supporto di funzioni essenziali o importanti, **piani di uscita esaustivi e regolarmente testati**, idonei a garantire la continuità operativa aziendale (es. prevedendo un periodo di transizione)

***Principali disposizioni contrattuali***

a) *«la **descrizione chiara e completa** di tutte le funzioni che il fornitore terzo di servizi ICT deve svolgere e tutti i servizi ICT che deve prestare […]*

b) *le **località** […] in cui si devono **svolgere le funzioni** […] compreso il **luogo di conservazione** […]*

c) *le **disposizioni** in materia di **disponibilità, autenticità, integrità e riservatezza** in relazione alla protezione dei dati, compresi i dati personali*

d) *le **disposizioni relative alle garanzie di accesso, ripristino e restituzione**,[…]*

e) *le descrizioni dei **livelli di servizio**, compresi relativi aggiornamenti e revisioni*

f) *l'**obbligo** per il fornitore terzo di servizi TIC **di prestare assistenza all'entità finanziaria** senza costi aggiuntivi o a un costo stabilito ex ante, qualora si verifichi un incidente connesso alle ICT relativo al servizio ICT fornito […]*

g) *l'**obbligo** per il fornitore terzo di servizi di TIC **di operare senza riserve con le autorità competenti** e con le autorità di risoluzione dell'entità finanziaria […]*

h) *i **diritti di risoluzione e il relativo termine minimo di preavviso** per la risoluzione degli accordi contrattuali […]*

i) *le condizioni riguardanti **la partecipazione dei fornitori terzi di servizi ICT ai programmi di sensibilizzazione** sulla sicurezza delle TIC […]»*

*Reg. DORA art. 30*

# ICT Third Party Risk Management


**Quali sono gli aspetti da considerare <u>nel continuo del rapporto con il fornitore</u>?**

- **Piano di audit:** predeterminare, sulla base di un approccio risk-based, la **frequenza delle verifiche di audit e delle ispezioni** nonché i settori da sottoporre ad audit, aderendo a standard di audit comunemente accettate
- **Servizi ICT a supporto di funzioni essenziali o importanti:** prevedere il monitoraggio costante delle prestazioni del fornitore con:
  - **Diritti incondizionati di accesso, ispezione ed audit,** anche ottenendo copia della documentazione pertinente
  - Obbligo per il fornitore di **cooperare senza riserva** nel corso delle ispezioni in loco
  - Obbligo di fornire **dettagli sull'ambito di applicazione, le procedure adottate e la frequenza** delle ispezioni e degli audit

*«I contratti per la fornitura di servizi TIC a supporto di funzioni essenziali o importanti dovrebbero altresì contenere disposizioni che consentano i **diritti di accesso, ispezione e audit da parte dell'entità finanziaria o di un soggetto terzo designato**, nonché il diritto di ottenere copia, quali strumenti fondamentali per il monitoraggio costante, da parte delle entità finanziarie, delle prestazioni del fornitore terzo di servizi TIC, insieme alla piena collaborazione di quest'ultimo nel corso delle ispezioni.»*

*Reg. DORA considerando 73*

*«[…] il fornitore terzo di servizi TIC e l'entità finanziaria che è una microimpresa **possono convenire che i diritti di accesso, ispezione e audit dell'entità finanziaria possano essere delegati a un terzo indipendente**, nominato dal fornitore terzo di servizi TIC, e che l'entità finanziaria possa richiedere in qualsiasi momento al terzo informazioni e garanzie sulle prestazioni del fornitore terzo di servizi TIC.»*

*Reg. DORA art.30*

# Quadro di sorveglianza per i fornitori ICT «critici»

### *La sorveglianza regolamentare*

Il Regolamento DORA introduce nuovi poteri per le Autorità di Vigilanza finanziaria nei confronti delle terze parti critiche, individuando un'Autorità di sorveglianza capofila, a cui compete la responsabilità di garantire la gestione dei rischi derivanti dalla dipendenza delle entità finanziarie da fornitori di servizi ICT

### *Quali sono gli ambiti di verifica dell'Autorità di sorveglianza?*

L'Autorità ha il compito di verificare la presenza di **norme, procedure, meccanismi** e **accordi** esaustivi, solidi ed efficaci **per gestire i rischi informatici** a cui possono essere esposte le entità finanziari clienti. In particolare con riferimento a:

- la **sicurezza, la disponibilità, la continuità, la scalabilità** e la qualità dei servizi
- la **capacità di mantenere standard di disponibilità, autenticità, integrità o riservatezza** dei dati costantemente elevati
- l'adeguatezza delle **misure di sicurezza fisica**
- la presenza di **processi di gestione del rischio**
- l'adeguatezza delle **strutture organizzative e dei presidi di governance**
- la presenza di **processi di identificazione, monitoraggio e tempestiva segnalazione di incidenti significativi connessi alle ICT**
- l'adozione di meccanismi per garantire **l'effettivo esercizio dei diritti di risoluzione/recesso**
- l'attuazione di **test su sistemi, infrastrutture ICT** e la presenza di modelli di controllo e monitoraggio

### *Cosa si intende con fornitore di servizi «critico»?*

I fornitori di servizi ICT possono essere definiti «critici», e quindi sottoposti alla sorveglianza dell'Autorità capofila, sulla base dei seguenti criteri (cfr. Art.31 Reg. DORA):

- Impatto sistemico in caso di disfunzione operativa del fornitore su vasta scala
- Carattere sistemico o importanza delle entità finanziarie che dipendono da quel fornitore terzo di servizi ICT
- Dipendenza delle entità finanziarie dai servizi prestati dal fornitore in rapporto alle funzioni essenziali o importanti
- Grado di sostituibilità del fornitore

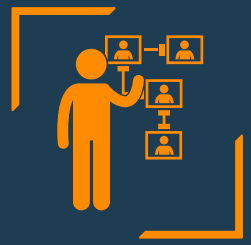
- In caso di **rilevata inadempienza** da parte del fornitore terzo di servizi ICT, l'Autorità ha inoltre il **potere di imporre penalità di mora,** di importo fino all'1 % del fatturato medio quotidiano realizzato a livello mondiale dal fornitore terzo critico di servizi ICT nel precedente esercizio (cfr. Art. 35 Reg. DORA)

# In conclusione

***....quali i principali impatti?***


Evoluzione della **cultura di rischio** aziendale & sviluppo di un **framework di gestione del rischio ICT**

Evoluzione del **rapporto tra Compagnia & Fornitore di servizi ICT**



Ridisegno di **processi aziendali** e definizione di **nuovi ruoli e responsabilità**

Sviluppo di **sistemi IT a supporto** delle verifiche

make your future happen

SCS CONSULTING
make your future happen

Via Toscana 19/A
40069 - Zola Predosa (Bo)
Tel. +39 051.3160311
info@scsconsulting.it

**Serena Bedendo**
Senior Manager Mercato Finance
Mobile +39 334 6892320
mail: s.bedendo@scsconsulting.it

**Federica Toso**
Manager Mercato Finance
Mobile +39 370 3340971
mail: f.toso@scsconsulting.it