

# DORA

## Caso aziendale e valutazione dei contratti di servizi ICT (FEI e Critici)

A cura di Simone Filippini



# Digital Operation Resilience Act

1

La rivoluzione della resilienza digitale nel settore finanziario

2

Il Caso Aziendale

3

Valutare i rischi, i contratti FEI e Critici

4

Valutare I contratti

5

I quesiti chiave

6

Evoluzione dei contratti FEI



# La rivoluzione della resilienza digitale nel settore finanziario

DORA (Digital Operational Resilience Act) è un nuovo regolamento europeo che impone alle istituzioni finanziarie di adottare misure concrete per garantire la resilienza operativa dei loro sistemi e processi informatici.

## Obiettivi Principali

- Proteggere i consumatori
- Rafforzare la stabilità del sistema finanziario
- Armonizzare il quadro normativo

### **Governance dei rischi informatici**

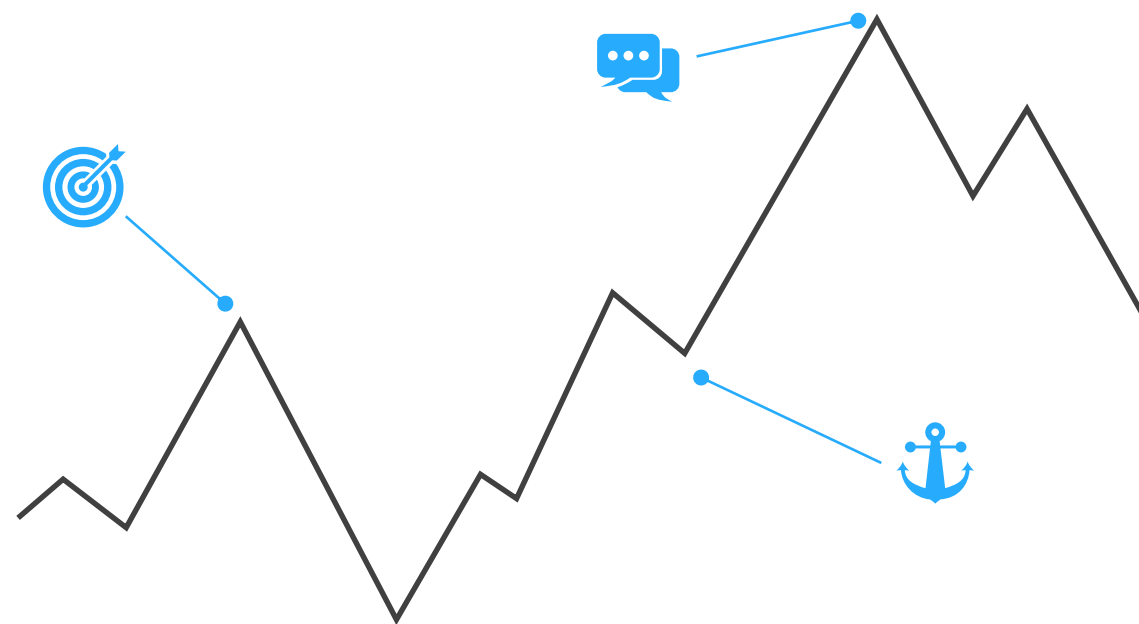
Definizione di un quadro di governance robusto per identificare, valutare e mitigare i rischi informatici.

### **Resilienza operativa**

Capacità di prevenire, rilevare e rispondere rapidamente a incidenti informatici, garantendo la continuità operativa.

### **Gestione degli incidenti**

Procedure chiare e tempestive per la gestione degli incidenti informatici, dalla notifica alle autorità competenti alla comunicazione ai clienti.



# Il Caso Aziendale

## Le difficoltà incontrate nell'approccio a DORA

Prima dell'implementazione di DORA, Credit Agricole Factoring ha dovuto affrontare sfide legate a:



### Gestione complessa dei dati

Un numero elevato di dati sensibili richiedeva sistemi e processi più efficienti.



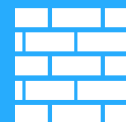
### Cybersecurity

Proteggere i dati dei clienti e garantire la continuità operativa era una priorità assoluta.



### Outsourcing

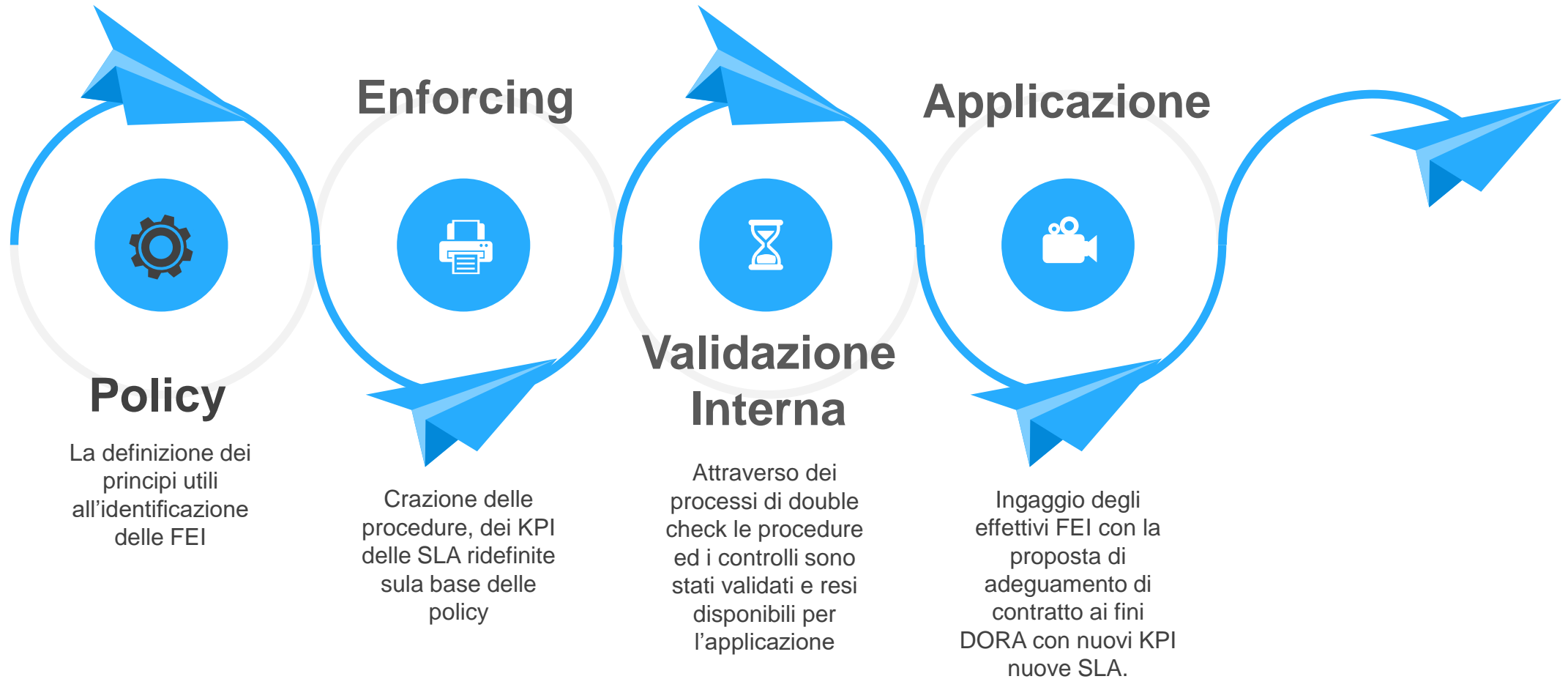
La gestione di terze parti comportava rischi che dovevano essere mitigati.



### Policy e Procedure

L'implementazione della legge richiedeva l'acquisizione e la dotazione di nuove procedure

# Il Caso Aziendale



# Valutare i rischi I contratti FEI e Critici

## Definizione di contratti FEI e Critici

**FEI (Fonte Esternalizzata Importante):** Provider che fornisce servizi all'istituzione, senza i quali quest'ultima non potrebbe operare in modo efficiente o sicuro.

**Critico:** Fornitore che, in caso di interruzione del servizio, potrebbe causare un impatto significativo sull'operatività dell'istituzione finanziaria.

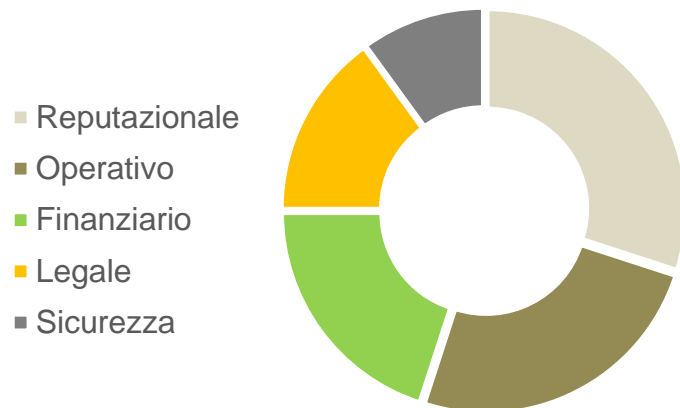
Le FEI sono considerate importanti perché:

**Sono essenziali per il funzionamento dell'azienda:** Senza questi servizi, l'azienda non potrebbe operare in modo efficiente.

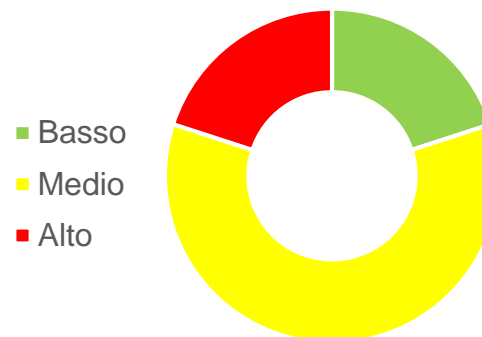
**Dati Sensibili:** Spesso le FEI comportano l'accesso a informazioni riservate dell'azienda o dei suoi clienti.

**Possono avere un impatto significativo sulla reputazione dell'azienda:** Eventuali problemi con i fornitori esterni possono danneggiare l'immagine dell'azienda.

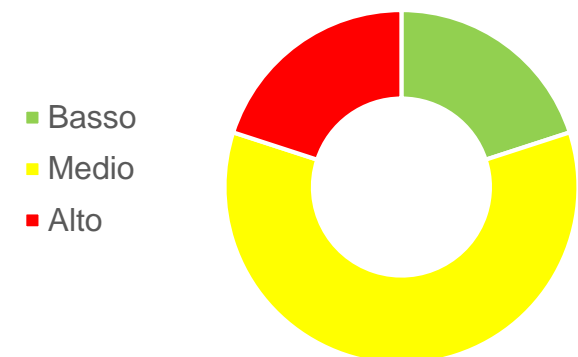
Tipologia di rischio



Impatto dei Rischi  
sui Contratti



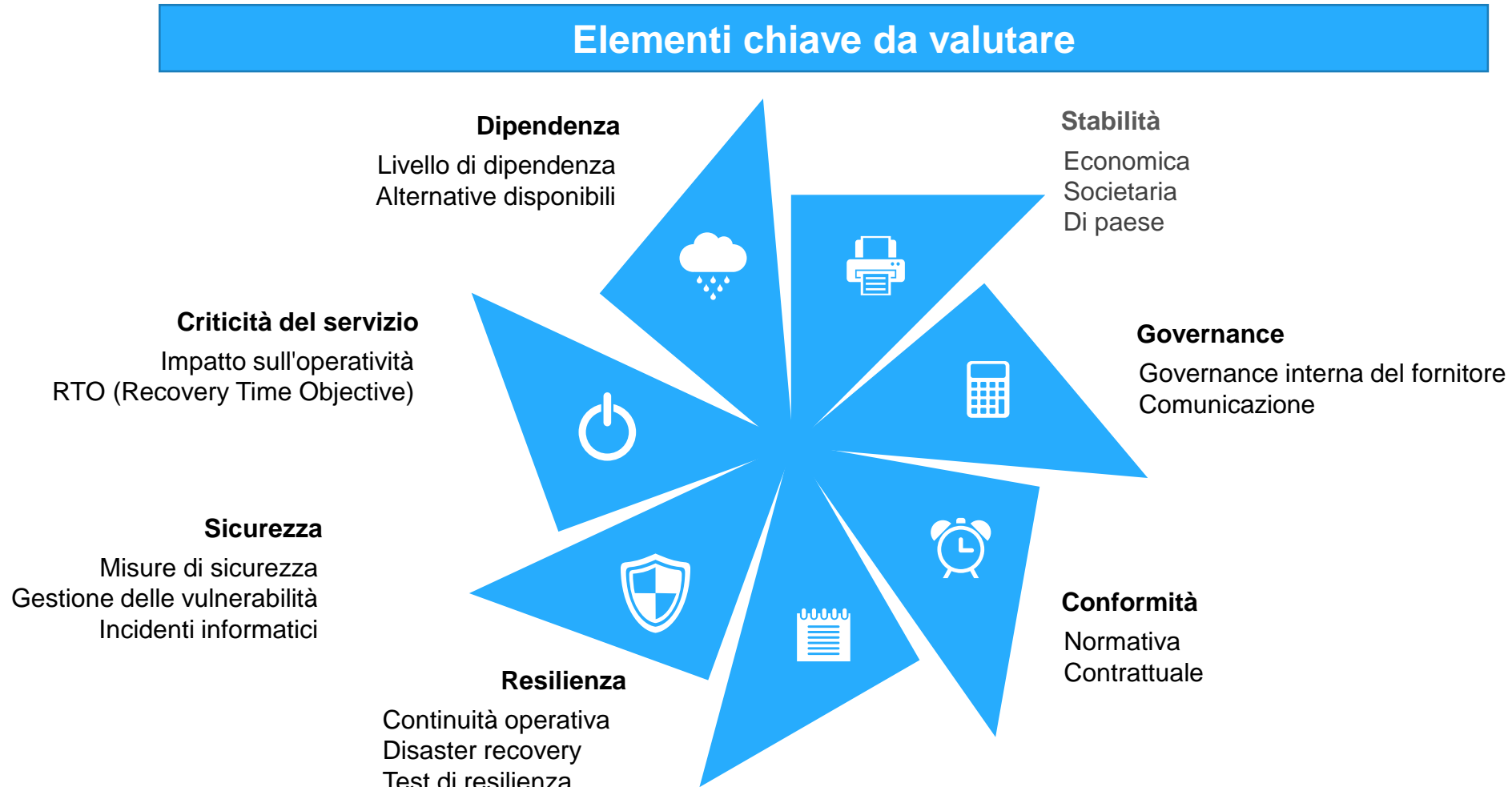
Rischi per probabilità



# Valutare i contratti

**Dipendenza critica:** Le istituzioni finanziarie spesso dipendono da questi fornitori per servizi essenziali come il cloud computing, la sicurezza informatica e la gestione dei pagamenti.

**Rischi elevati:** Un'interruzione o una violazione della sicurezza da parte di questi fornitori può comportare gravi conseguenze per l'istituzione.



# Valutare i contratti

Le domande  
Chiave  
Della Security





# Evoluzione dei contratti

## L'Impatto del DORA

**Prima dell'era DORA:** Contratti generici, focalizzati su servizi e responsabilità limitate.

**Dopo l'era DORA:** Contratti più dettagliati e rigorosi, con focus sulla resilienza operativa e sulla gestione dei rischi.

## Elementi Chiave dei Nuovi Contratti

**Requisiti minimi di servizio:** livelli di servizio garantiti e penali per mancato rispetto

**Obblighi di sicurezza informatica:** misure di protezione dei dati e dei sistemi

**Trasparenza e comunicazione:** obblighi informativi e canali di comunicazione efficaci

01

02

03

04

## Benefici dei Nuovi Contratti

**Maggiore resilienza operativa:** riduzione del rischio di interruzioni dei servizi

**Migliore gestione dei rischi:** identificazione e mitigazione proattiva delle minacce

**Maggiore efficienza:** ottimizzazione dei processi e riduzione dei costi

## Sfide

**Complexit :** contratti pi  lunghi e dettagliati

**Costi:** implementazione di nuove misure di sicurezza

**Rischi legali:** responsabilit  in caso di incidenti

# Open Questions

## Misure di mitigazione

**Contratti rigorosi:** Clausole dettagliate su sicurezza, resilienza, responsabilità.

**Due diligence:** Valutazione approfondita dei fornitori prima e durante la collaborazione.

**Monitoraggio continuo:** Verifiche periodiche delle performance e della conformità.

**Incidents response plan:** Piani di emergenza per gestire gli incidenti.

**Business continuity planning:** Pianificazione per garantire la continuità operativa in caso di disastro.

**Cybersecurity:** Misure di protezione informatica robuste.

**Governance:** Definizione di ruoli e responsabilità chiare.

## Indicatori Chiave di Performance (KPI)

Monitorare l'efficacia delle misure di mitigazione. Esempi: tempo medio di risoluzione degli incidenti, numero di vulnerabilità identificate e corrette, percentuale di fornitori valutati annualmente.

# Grazie!

