ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

I PRINCIPALI CONTENUTI DEL REGOLAMENTO DORA E GLI IMPATTI SULLA GOVERNANCE DI BANCHE E INTERMEDIARI FINANZIARI

Alcuni temi di lavoro per gli esponenti aziendali.

ALBERTO BALESTRERI

16 settembre 2024

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

Agenda

1. **Le priorità di vigilanza del SSM 2024-2026**
2. **La «digital security» nei *Principles of Corporate Governance* del G20/OCSE**
3. **La governance nel regolamento DORA**

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

1. Le priorità di vigilanza del SSM 2024-2026

Priorità n. 3: «ulteriori progressi nella trasformazione digitale e nella realizzazione di solidi assetti di resilienza operativa»

«Sebbene gran parte degli enti vigilati stia compiendo progressi nella digitalizzazione di operazioni e servizi per fronteggiare le crescenti sfide della concorrenza, essi devono anche **rafforzare e adeguare**, **ove necessario, i propri assetti di resilienza operativa per attenuare i rischi potenziali.**

Il conseguimento della resilienza operativa dovrebbe:

- contribuire alla **sostenibilità dei modelli imprenditoriali** delle banche nel medio periodo;
- consentire loro, tra l'altro, di **cogliere i benefici delle tecnologie innovative**.

Tuttavia, alcune banche sono lontane dal raggiungimento dei loro obiettivi in questo ambito. Inoltre, gli enti vigilati devono affrontare le vulnerabilità derivanti dalla crescente dipendenza operativa da fornitori terzi e migliorare la gestione del rischio di sicurezza informatica/cibernetica. Questo aspetto riveste particolare importanza alla luce delle sempre più numerose minacce cibernetiche riconducibili all'attuale contesto geopolitico.»

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

1) Vulnerabilità individuata come priorità:
Carenze nelle strategie di trasformazione digitale.

Obiettivo strategico: le banche dovrebbero elaborare e attuare solidi **piani di trasformazione digitale** mediante meccanismi adeguati (ad esempio strategia aziendale e gestione dei rischi) al fine di rafforzare la sostenibilità dei propri modelli imprenditoriali e attenuare i rischi connessi all'uso di tecnologie innovative.

(…) gli enti vigilati dovrebbero essere in grado di gestire l'aumento previsto dei costi operativi **senza mettere a repentaglio gli imprescindibili investimenti nella trasformazione digitale**.

Secondo le attese, la digitalizzazione dovrebbe **consolidare la posizione concorrenziale e la capacità di tenuta delle banche alla concorrenza esterna al settore bancario**.

Nel 2023 la Vigilanza bancaria della BCE ha condotto una valutazione orizzontale (…)

Le ispezioni mirate, che hanno integrato la valutazione orizzontale, hanno sollevato **preoccupazioni circa l'efficacia dell'indirizzo strategico e dell'esecuzione**, ponendo in risalto anche l'importanza della riqualificazione professionale del personale e degli organi di amministrazione.

Sono emerse, tra l'altro, carenze nella pianificazione finanziaria e del bilancio, date le difficoltà delle banche a monitorare l'impatto finanziario delle loro iniziative di trasformazione digitale.

In prospettiva, la Vigilanza bancaria della BCE continuerà a concentrarsi sulla trasformazione digitale, coniugando indagini mirate a ispezioni dedicate.

Inoltre, pubblicherà le proprie aspettative di vigilanza sulla trasformazione digitale delle banche. Le aspettative riviste contribuiranno a rafforzare la metodologia di valutazione prudenziale.

Principali attività nell'ambito del programma di lavoro sulle priorità di vigilanza

Indagini mirate **sull'impatto della trasformazione digitale delle banche:**

- sul modello imprenditoriale;
- sulla strategia aziendale;
- sulla governance;
- sulla individuazione/gestione dei rischi;

integrate dall'attività di follow-up dei GVC laddove emergano carenze rilevanti.

Ispezioni mirate **sulla trasformazione digitale**, che combinano la dimensione del modello imprenditoriale all'aspetto informatico delle strategie di trasformazione digitale delle banche.

2) Vulnerabilità individuata come priorità:

Carenze negli assetti di resilienza operativa, ossia rischi di esternalizzazione dei servizi informatici e di sicurezza informatica/cibernetica

Obiettivo strategico: le banche dovrebbero disporre di:

i) solidi meccanismi di gestione del rischio di esternalizzazione;
ii) sistemi di sicurezza informatica e di resilienza cibernetica

per far fronte in maniera proattiva a qualsiasi rischio non attenuato che possa determinare **interruzioni rilevanti di attività o servizi critici**, assicurando al tempo stesso il rispetto dei requisiti regolamentari e delle aspettative di vigilanza pertinenti.

A. Il **rischio cibernetico e la sicurezza dei dati** continuano a rappresentare importanti fattori di rischio operativo per le banche.

Il numero di incidenti cibernetici segnalati dagli enti vigilati alla Vigilanza bancaria della BCE è aumentato nella prima metà del 2023, di riflesso alla significativa esposizione del settore bancario alle minacce cibernetiche in evoluzione, riconducibile tra l'altro alla guerra della Russia in Ucraina e all'acuirsi delle **tensioni geopolitiche.**

Gli **attacchi distruttivi** sono diventati una delle componenti principali delle operazioni delle entità statali, di cui anche le istituzioni finanziarie sono un probabile obiettivo, dato il loro ruolo per le infrastrutture critiche.

Gli **attacchi ransomware** in particolare continuano ad aumentare, diventando più sofisticati, e le banche sono sempre più colpite dalle *tecniche di estorsione in evoluzione.*

B. Le **debolezze negli accordi di esternalizzazione dei servizi informatici** rappresentano un'altra vulnerabilità principale, data la crescente dipendenza delle banche da fornitori terzi.

L'allungamento e la maggiore complessità delle catene di approvvigionamento impongono alle banche di **comprendere e controllare meglio i rapporti con i fornitori nonché le dipendenze da (e interdipendenze con) questi ultimi** per affrontare in modo proattivo i potenziali rischi di concentrazione.

Una sana gestione delle attività e dei fornitori è quindi essenziale affinché le banche riescano a soddisfare le esigenze della clientela e a migliorare la propria efficienza in un contesto sempre più competitivo, assicurando nel contempo un'adeguata gestione dei rischi derivanti dagli accordi di esternalizzazione e dall'adozione di soluzioni cloud.

L'esito dello SREP 2023 ha ulteriormente confermato la rilevanza delle carenze delle banche nella gestione dell'esternalizzazione dei servizi informatici e dei rischi di sicurezza informatica/cibernetica; di fatto il rischio operativo continua a essere l'elemento che ha ottenuto i peggiori punteggi SREP.

Principali attività nell'ambito del programma di lavoro sulle priorità di vigilanza

1. **Raccolta di dati e analisi orizzontale dei registri delle attività di esternalizzazione** al fine di individuare le interconnessioni tra enti vigilati e fornitori terzi e le potenziali concentrazioni dei rischi in relazione a determinati fornitori.
2. **Indagini mirate** sugli accordi di esternalizzazione e della resilienza cibernetica.
3. **Ispezioni mirate** sulla gestione dell'esternalizzazione e della sicurezza cibernetica.
4. **Prova di stress sulla resilienza cibernetica sistemica nel 2024** incentrata sulla capacità di risposta e ripresa delle banche in seguito a un incidente di sicurezza cibernetica e sulla loro capacità di limitarne l'impatto e ripristinare tempestivamente i servizi.

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

2. La «digital security» nei Principles of Corporate Governance del G20/OCSE

1. Corporate governance practices of individual companies are also often influenced by human rights and environmental laws, and **increasingly laws related to digital security, data privacy and personal data protection** (p. 11);
2. Adopting digital solutions in regulatory and supervisory processes also comes with challenges and risks. Important considerations include ensuring the quality of data; ensuring that staff have proper technical competence; considering interoperability between systems in the development of reporting formats; and **managing third-party dependencies and digital security risks** (p. 12).

3. Many companies rely on technology vendors to manage remote participation. When choosing service providers, it is important to consider that they have the appropriate professionalism **as well as data handling and digital security capacity** to support the conduct of fair and transparent shareholder meetings, with technical and organizational security measures in place for each of the processing operations carried out by virtue of their service, especially concerning personal data, which require stricter security measures (p. 16).

4. Users of financial information and market participants **need information on *reasonably foreseeable material risks* *that* may include:**

- risks that are specific to the industry or the geographical areas in which the company operates;
- dependence on commodities and supply chains;
- financial market risks including interest rate or currency risk;
- risks related to derivatives and off-balance sheet transactions;
- business conduct risks;
- **digital security risks;**
- compliance risks;
- sustainability risks, notably climate-related risks (p. 30).

5. Another important board responsibility is to oversee **the risk management system** and **mechanisms designed to ensure that <u>the corporation obeys applicable laws</u>**, including relating to tax, competition, labour, human rights, environmental, equal opportunity, **digital security**, data privacy and personal data protection, and health and safety (p. 34).

6. Of notable importance is **the management of digital security risks,** which are dynamic and can change rapidly. Risks may relate, among other matters:

- to data security and privacy;
- the handling of cloud solutions;
- authentication methods;
- security safeguards for remote personnel working on external networks.

As with other risks, these risks should be integrated more broadly within the overall cyclical company risk management framework (p. 36).

7. The establishment of committees to advise on additional issues should remain at the discretion of the company and should be flexible and proportional according to the needs of the board. Some boards have created a sustainability committee to advise the board on social and environmental risks, opportunities, goals and strategies, including related to climate. **Some boards have also established a committee to advise on the management of digital security risks as well as on the company's digital transformation** (p. 41).

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

3. La governance nel Regolamento DORA

I principali obiettivi del Regolamento DORA

Il Regolamento Dora statuisce tre obiettivi:

1) resilienza operativa;

2) prestazioni;

3) stabilità del sistema finanziario

Il Regolamento rappresenta uno strumento di **notevole rafforzamento per l'azione della Vigilanza europea** in quanto:

A. sarà uno strumento di armonizzazione a livello continentale;

B. potrà diventare strumento di riduzione dei costi per le entità finanziarie transfrontaliere;

C. dovrebbe incentivare il mercato unico europeo dei servizi finanziari;

D. estende i processi di controllo all'intero ecosistema tecnologico che si interfaccia con il settore finanziario (e che sarà quindi sottoposto a controllo diretto anche da parte delle Autorità di Vigilanza).

Struttura del Regolamento

CAPO I- Disposizioni Generali (artt. 1-4)

CAPO II – Gestione dei rischi informatici (artt. 5-16)

Sezione I (art. 5)

Sezione II (artt. 6-16)

CAPO III – Gestione, classificazione e segnalazione degli incidenti informatici (artt. 17-23)

CAPO IV – Test di resilienza operativa digitale (artt. 24-27)

CAPO V – Gestione dei rischi informatici derivanti da terzi (artt. 28-39)

Sezione I – Principi fondamentali di una solida gestione dei rischi informativi derivanti da terzi (artt. 28-30)

Sezione II – Quadro di sorveglianza dei fornitori terzi di servizi critici di servizi TIC (artt. 31-44)

CAPO VI – Meccanismi di condivisione delle informazioni (art. 45)

CAPO VII – Autorità competenti (artt. 46-56)

CAPO VIII – Atti Delegati (art. 57)

CAPO IX – Disposizioni transitorie e finali (artt. 58-63).

Ruolo dell'organo con funzione di gestione (Considerando 45-46)

«Per garantire il pieno allineamento e la coerenza complessiva tra le strategie aziendali delle entità finanziarie, da un lato, e la gestione dei rischi informatici, dall'altro, è opportuno richiedere agli organi di gestione delle entità finanziarie di **mantenere un ruolo attivo e fondamentale nella guida e nell'adeguamento del quadro per la gestione dei rischi informatici e della strategia globale di resilienza operativa digitale.**

Gli organi di gestione dovrebbero adottare un **approccio che non consideri solamente i mezzi per assicurare la resilienza dei sistemi di TIC, ma si estenda anche alle persone e ai processi** mediante un ventaglio di strategie che promuovano, a ciascun livello dell'azienda e per tutto il personale, un **forte senso di consapevolezza dei rischi informatici** nonché **l'impegno a osservare a tutti i livelli una rigorosa igiene informatica (cyber hygiene).**

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

Ruolo dell'organo con funzione di gestione (Considerando 45-46)

La responsabilità principale dell'organo di gestione nell'affrontare i rischi informatici di un'entità finanziaria **dovrebbe concretizzarsi nel principio guida di tale approccio complessivo**, tradotto ulteriormente nel **costante coinvolgimento dell'organo di gestione a controllare il monitoraggio della gestione dei rischi informatici.**

Inoltre, il principio della piena e principale responsabilità dell'organo di gestione per la gestione dei rischi informatici dell'entità finanziaria si accompagna alla **necessità di assicurare un livello di investimenti connessi alle TIC e un bilancio complessivo dell'entità finanziaria** che consentirebbero all'entità finanziaria di conseguire un elevato livello di resilienza operativa digitale.»

Governance e organizzazione (art. 5)

Le entità finanziarie predispongono un **quadro di gestione e di controllo interno (framework)** che garantisce una gestione efficace e prudente di tutti i rischi informatici al fine di acquisire un elevato livello di resilienza operativa digitale.

L'organo di gestione dell'entità finanziaria:

- definisce e approva l'attuazione di tutte le disposizioni concernenti il quadro per la gestione dei rischi informatici;
- vigila su tale attuazione;
- ne è responsabile.

Responsabilità dell'organo di gestione (art. 5)

a) assume la responsabilità finale per la gestione dei rischi informatici dell'entità finanziaria;

b) predispone politiche miranti a garantire il mantenimento di standard elevati di disponibilità, autenticità, integrità e riservatezza dei dati;

c) definisce chiaramente ruoli e responsabilità per tutte le funzioni connesse alle TIC e stabilisce adeguati meccanismi di governance al fine di garantire una comunicazione, una cooperazione e un coordinamento efficaci e tempestivi tra tali funzioni;

d) ha la responsabilità generale di definire e approvare la strategia di resilienza operativa digitale, compresa la determinazione del livello appropriato di tolleranza per i rischi informatici dell'entità finanziaria;

e) approva, supervisiona e riesamina periodicamente l'attuazione della politica di continuità operativa delle TIC e dei piani di risposta e ripristino relativi alle TIC dell'entità finanziaria;

f) approva e riesamina periodicamente i piani interni di audit in materia di TIC dell'entità finanziaria, gli audit in materia di TIC e le più importanti modifiche a essi apportate;

g) assegna e riesamina periodicamente le risorse finanziarie adeguate per soddisfare le esigenze di resilienza operativa digitale dell'entità finanziaria rispetto a tutti i tipi di risorse, compresi:

- i pertinenti programmi di sensibilizzazione sulla sicurezza delle TIC;
- le attività di formazione sulla resilienza operativa digitale;
- le competenze in materia di TIC per tutto il personale;

h) approva e riesamina periodicamente la politica dell'entità finanziaria relativa alle modalità per l'uso dei servizi TIC prestati dal fornitore terzo di servizi TIC;

i) istituisce a livello aziendale canali di comunicazione che gli consentono di essere debitamente informato in merito a quanto segue:

- gli accordi conclusi con i fornitori terzi di servizi TIC sull'uso di tali servizi,
- le relative eventuali modifiche importanti e pertinenti previste riguardo ai fornitori terzi di servizi TIC,
- il potenziale impatto di tali modiche sulle funzioni essenziali o importanti soggette agli accordi in questione, compresa una sintesi dell'analisi del rischio per valutare l'impatto di tali modifiche, nonché almeno gli gravi incidenti TIC e il loro impatto, le misure di risposta e ripristino e le misure correttive.

A. Framework

1. Identificazione (art. 8)
2. Protezione (art. 9)
3. Prevenzione (art. 9)
4. Individuazione (art. 10)
5. Risposta (art. 11)
6. Ripristino (art. 11)
   - Politiche di backup (art. 12)
   - Politiche di ripristino (art. 12)
7. Apprendimento (art. 13)
8. Evoluzione (art. 13)
9. Comunicazione (art. 14)
10. Programma di test di resilienza operativa (art. 24)

B. Strategia di resilienza digitale (art. 6)

Il quadro per la gestione dei rischi informatici comprende una **strategia di resilienza operativa digitale** che definisce le modalità di attuazione del quadro.

A tal fine la strategia di resilienza operativa digitale include **metodi** per affrontare i rischi informatici e conseguire specifici obiettivi in materia di TIC:

a) spiegando in che modo il quadro per la gestione dei rischi informatici **sostiene gli obiettivi e la strategia commerciale dell'entità finanziaria;**

b) fissando il **livello di tolleranza per i rischi informatici**, conformemente alla propensione al rischio dell'entità finanziaria e analizzando la tolleranza d'impatto per le perturbazioni a livello di TIC;

c) indicando **chiari obiettivi in materia di sicurezza delle informazioni**, compresi indicatori chiave di prestazione e parametri chiave di rischio;

d) spiegando **l'architettura di riferimento a livello di TIC** e le eventuali modifiche necessarie per conseguire specifici obiettivi commerciali;

e) delineando i differenti **meccanismi introdotti per individuare incidenti connessi alle TIC**, prevenire il loro impatto e proteggersi dallo stesso;

f) documentando **l'attuale situazione di resilienza operativa digitale** sulla base del numero di gravi incidenti TIC segnalati, nonché l'efficacia delle misure preventive;

g) attuando **test di resilienza operativa digitale**;

h) delineando una **strategia di comunicazione** in caso di incidenti connessi alle TIC di cui è richiesta la divulgazione.

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

Che fare?

1. Definire i Principi guida;
2. Sviluppare cultura digitale più che cultura della computer security;
3. Implementare il Regolamento DORA per prepararsi al futuro;
4. Andare oltre alle aspettative della Vigilanza;
5. Mappare e governare la *value constellation* delle centinaia di temi toccati dal Regolamento DORA e dai RTS/ITS;
6. La «strategia di digitalizzazione» e la «strategia di resilienza digitale» sono due binari paralleli;
7. Resilienza digitale quale tema di lavoro quotidiano;
8. Diffondere a tutti i livelli della banca «igiene cyber»;
9. Investire nelle risorse interne (e meno nella consulenza esterna);
10. DORA non è il GDPR: compliance condizione necessaria ma non sufficiente.

Riferimenti

Alberto Balestreri

Presidente Commissione banche,
intermediari finanziari e assicurazioni.
ODCEC Milano

ab@studiobalestreri.it