DORA, strategia di cyber resilience dell'Eurosistema e armonizzazione delle prassi

Claudio Impenna, Banca d'Italia
Capo del Servizio Supervisione Mercati e sistemi di pagamento

Regolamento DORA

- Obiettivo: armonizzare e rafforzare la **resilienza operativa digitale** delle entità finanziarie e del settore finanziario a livello europeo - **Requisiti armonizzati su 5 *building blocks:***

ICT RISK MANAGEMENT	ICT MAJOR INCIDENT REPORTING	THIRD-PARTY RISK	TESTING	INFO SHARING

- **Destinatari**

OPERATORI FINANZIARI	FORNITORI CRITICI DI SERVIZI ICT (cTTP)
• Requisiti in continuità con quanto previsto dalla regolamentazione vigente per alcuni soggetti (ad es. banche) • Requisiti nuovi e armonizzati per alcune tipologie di entità (ad es. SGR)	• Nuovo regime di sorveglianza diretta su fornitori critici identificati a livello europeo • In linea con recenti previsioni e prassi di vigilanza e sorveglianza adottate in Italia per alcuni fornitori di servizi tecnologici e strumentali rilevanti per il sistema finanziario

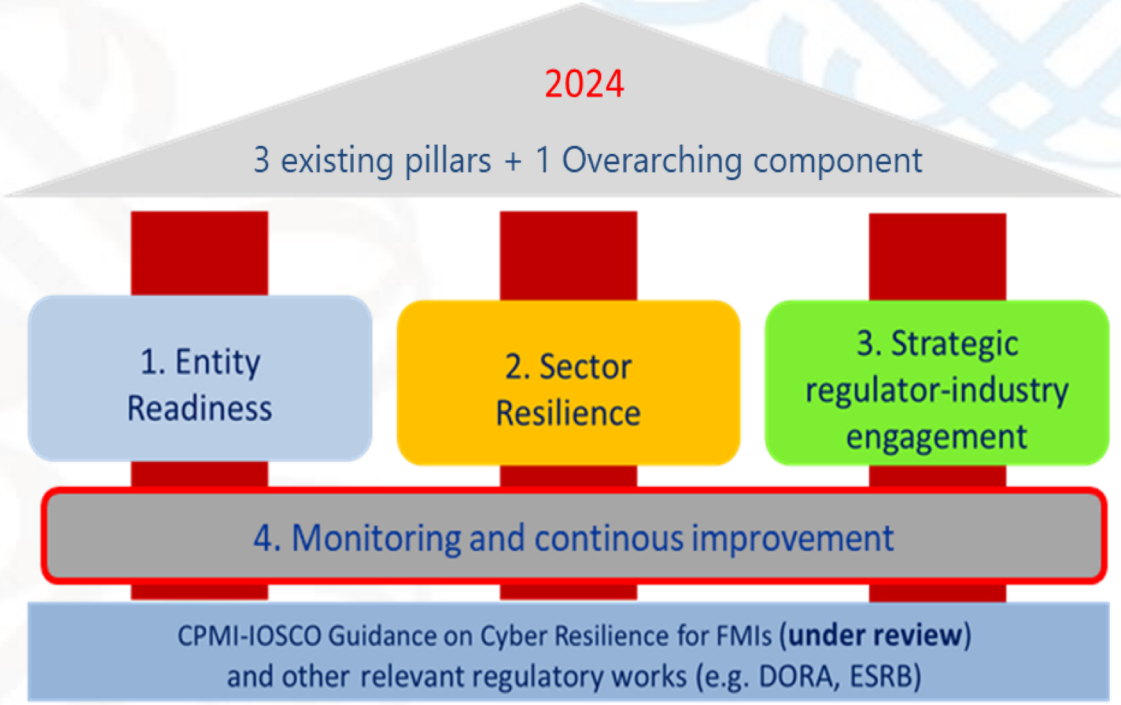
- **Sistemi e schemi di pagamento** fuori DORA perché già nei framework di sorveglianza dell'Eurosistema

Aggiornamento della Strategia di Cyber Resilience dell'Eurosistema

Strategia di Cyber Resilience dell'Eurosistema

- **Aggiornata** la Strategia di resilienza cibernetica per i soggetti sorvegliati (ottobre 2024)

- **Obiettivi**
  - rafforzare la sicurezza dell'ecosistema finanziario europeo
  - armonizzare le regole sulla resilienza operativa digitale del settore, anche in vista di DORA



- **Principali aggiornamenti**
  - Estensione dell'ambito soggettivo: infrastrutture di mercato e sistemi di pagamento + strumenti, servizi e schemi di pagamento elettronici
  - Aggiornamento metodologie e strumenti per maggiore allineamento a DORA (ad es. CROE, TIBER-EU 2.0)
  - Nuovi strumenti di assessment (ad es. *Cyber stress test)*

Spunti di riflessione (1)

- **DORA: passaggio** (sfidante) dalla regolamentazione all'implementazione nazionale
  - **Autorità**: aggiornamento normativa nazionale; adeguamento metodologie e prassi di supervisione, nazionali e internazionali
  - **Operatori**: adeguamento ai requisiti DORA per tutti i 5 building block (ad es. registro fornitori, adeguamento contratti, presidi tecnico-organizzativi, …)
- Importanza del ruolo dei **fornitori ICT critici (cTTP)** e dei **rischi di interconnessione e concentrazione**
  - **Complessità del framework**
  - **cTTP:** adeguamento dei framework di governance e gestione dei rischi IT, confronto con le autorità ed evidenze per i criteri di sorveglianza previsti da DORA (art. 33)
- **Disponibilità di risorse qualificate** (sfida comune per Autorità e industria)
- **Tempistiche e modalità di adeguamento** della normativa vigente (ad es. Circ. 285/Linee Guida EBA)

Spunti di riflessione (2)

- **Comunicazione e coordinamento** tra Autorità a livello nazionale ed europeo
  - Istituzione di un quadro di coordinamento per gli incidenti cyber su larga scala (*EU Systemic Cyber Incident Coordination Framework*, EU-SCICF)
  - Duplice modalità di funzionamento: *non-crisis mode e crisis mode*

- Esigenze di **raccordo con altre norme europee** (NIS2 e CER) e **nazionali** (decreti legislativi di recepimento e Perimetro di Cybersicurezza) e coordinamento con le altre autorità nazionali o di altri settori (ad es. ACN, PdCM)

- **Rilevanza dei test avanzati di sicurezza (TLPT) e coordinamento con i test TIBER-IT (volontari)**
  - Pubblicazione da parte della BCE del TIBER-EU 2.0 per allinearlo a RTS DORA
  - Aggiornamento dei framework nazionali (ad es. TIBER-IT)