

Digital Operational Resiliency Act (DORA)

Come prepararsi al prossimo intervento da parte del Regolatore Europeo attraverso un programma di “DORA Compliance in a Box”

Digital Operational Resiliency Act (DORA)

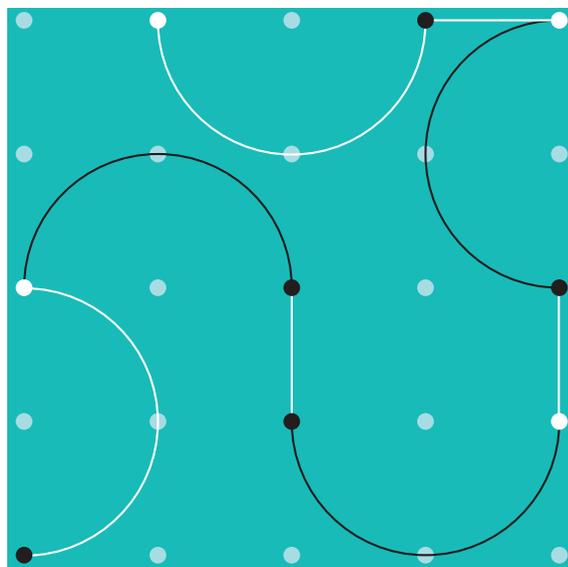
Il presente documento illustra la prospettiva di IBM Consulting in merito alla bozza di Regolamento Digital Resilience Operational Act (DORA), della Commissione Europea destinato agli “enti finanziari”¹.

Il Regolamento fa parte del “Pacchetto Finanza Digitale” e rientra all’interno delle misure atte ad abilitare e sostenere il potenziale della finanza digitale, in termini di innovazione e concorrenza, mitigando i rischi operativi che derivano dal costante aumento dell’utilizzo di tecnologie digitali nel settore dei servizi finanziari e delle minacce cyber.

Il 24 settembre 2020 la Commissione Europea, andando a modificare la normativa esistente in tema di Network and Information Security (Direttiva NIS), ha pubblicato la proposta di regolamento in materia di resilienza operativa digitale per il settore finanziario, per garantire standard di sicurezza alle infrastrutture ICT, nonché monitorare i fornitori ICT operanti nel settore.

L’obiettivo del Regolatore Europeo è quello di definire un quadro di regole per l’identificazione e la gestione dei rischi e dei disservizi ICT, stabilendo obblighi in carico agli enti finanziari in ambito di testing delle infrastrutture e dei servizi, di controllo sui fornitori terzi critici, nonché sull’adozione di strategie, politiche e procedure per garantire la resilienza operativa digitale. Rischi che, a causa della pandemia da Covid-19, sono aumentati, essendo aumentata la diffusione di servizi finanziari digitali e degli strumenti di lavoro in modalità remota.

La Commissione Europea ha deciso di introdurre un atto unico al fine di uniformare le norme a livello comunitario e nazionale e limitare gli impatti di natura economica derivanti dagli incidenti ICT che influiscono sulla continuità operativa.



DORA: la Resilienza Digitale Operativa come modello di garanzia della Business Continuity e Customer Experience, gestendo in modo end-to-end la Cyber Security, Rischi, Incidenti e Test ICT nei Financial Services e i rapporti con Fornitori Terzi critici

Benefici attesi dal Regolamento

Il Regolamento comporterà effetti positivi, in termini di impatto regolamentare, economico-sociale, innovazione tecnologica su tutti gli operatori del settore finanziario. Grazie alla proposta, per gli stakeholder coinvolti sarà più facile comprendere quali siano le norme da applicare e i costi di conformità potrebbero anche diminuire.

Il principale beneficio da un punto di vista sociale del Regolamento, infatti, riguarda sia i consumatori che gli investitori: una maggiore resilienza operativa digitale del sistema finanziario da un lato diminuisce il numero e i costi medi degli incidenti ICT e dall'altro garantisce che la società, nel suo complesso, tragga vantaggio dall'accresciuta fiducia nel settore dei servizi finanziari. La decrescita del numero degli incidenti ICT, specie di quelli che impattano la user experience, garantisce inevitabilmente una maggiore resilienza di tutte le istituzioni che, tenendo conto anche del proprio core business e/o degli stakeholder coinvolti nei loro processi, potrebbero essere considerate piattaforme sistemiche. Non da ultimo, importanti impatti positivi sono da annoverare anche in ambito di innovazione tecnologica, poiché il Regolatore incoraggia un uso maggiore delle infrastrutture e dei servizi ICT di ultima generazione.

Roadmap di applicazione DORA

La pubblicazione del Regolamento da parte della Commissione Europea in versione definitiva si ipotizza possa avvenire entro il 2022.

Per fornire maggiore rilevanza alla normativa DORA, la Banca Centrale Europea, il 4 giugno 2021, ha pubblicato un dossier² sulla proposta di normativa, sottolineando l'importanza di alcuni aspetti specifici: in particolare il rafforzamento delle funzioni di risk e incident management nonché la reporting strategy.

Un ulteriore avallo all'iniziativa della Commissione è arrivato da parte delle tre Supervisory Authority (EBA, EIOPA, ESMA)³ che hanno emesso in data 27 gennaio 2022 un comunicato congiunto⁴. Il Joint Committee europeo, in risposta alla raccomandazione formulata dallo European Systemic Risk Board (ESRB)⁵ rispetto al tema Systemic Cyber Risk, ha confermato la necessità di avviare le attività per l'identificazione di un framework comune a livello europeo (Pan-European systemic cyber incident coordination framework - EU-SCICF) per la gestione delle casistiche di gravi incidenti ICT che potrebbero avere impatti sistemici sul settore finanziario dell'Unione.

Oltre alla versione definitiva del Regolamento stesso, ci sono importanti aspetti di dettaglio che saranno successivamente definiti e attesi indicativamente nel 2023, attraverso la definizione delle cosiddette norme tecniche di regolamentazione (Regulatory Technical Standards). Si tratterà di strumenti, metodi, processi e politiche di gestione del rischio ICT, classificazione degli incidenti, processi di controllo da parte della Autorità di Vigilanza Europee, che forniranno ulteriori linee guida specifiche a favore di tutte le istituzioni che operano nel settore dei servizi finanziari.

Principali obiettivi di DORA

La proposta di regolamento DORA si articola in sei settori d'intervento, prevedendo che gli enti finanziari debbano:

- garantire una governance interna più efficiente (articolo 4)
- rafforzare le practice di ICT Risk Management (articoli da 5 a 14)
- rafforzare il framework di ICT Incident Management (articoli da 15 a 20)
- dotarsi di un programma onnicomprensivo di test di resilienza operativa digitale che comprenda anche la Cybersecurity (articoli da 21 a 24)
- garantire un monitoraggio più efficiente e sicuro dei fornitori ICT critici (articoli da 25 a 39)
- garantire una condivisione (su base volontaria da parte degli enti finanziari) delle informazioni relative alle minacce informatiche (articolo 40)

Key Pillar DORA



Governance e strutture interne rafforzate



Gestione integrata Rischi e reporting Incident ICT



Gestione del rischio derivante da Terze Parti



Test di resilienza operativa digitale



Condivisione informativa su minacce informatiche

Ecosystem of Partners

IBM Consulting services

IBM Research

IBM Technology

Best practice and capabilities

IBM Resilience Assessment (Risk & Incident)

IBM Zero Trust (Security)

IBM Performance Engineering Management Methodology (Test Mgmt)

Celonis

AWS

Thought Machine

Adobe

Salesforce

Ui Path

Oracle

Microsoft

SAP

Promontory

Kyndryl

Workday

Palantir

← Co-created, co-operated, and co-executed through the IBM Garage →



IBM Consulting: un Partner strategico per la definizione di un Programma di "DORA Compliance in a Box"

IBM Consulting come partner strategico per indirizzare un programma end-to-end a garanzia della Resilienza Operativa

La resilienza operativa delle applicazioni e delle infrastrutture rientra nel più generale quadro di gestione dei rischi, quindi è necessario affrontare l'emergere di questioni critiche di natura tecnica con un approccio e una metodologia più ampia di sana gestione del rischio, in quanto non si tratta solo di un problema tecnologico.

Difatti, gli impatti per le istituzioni finanziarie sono relativi anche ad aspetti organizzativi: l'obiettivo del Regolatore Europeo è quello di identificare e/o rafforzare i framework e processi di Risk & Incident Management, affinché le istituzioni dispongano di un quadro di gestione dei rischi ICT solido, completo e ben documentato, che consenta loro di affrontare il rischio in modo rapido, efficiente e completo e di garantire un elevato livello di resilienza operativa e di strategia digitale, corrispondente alle loro esigenze aziendali, dimensioni e complessità.

IBM Consulting si qualifica come partner strategico per la definizione di un Programma di "DORA Compliance in a Box".

La capacità di IBM Consulting di coniugare pensiero strategico con profonde competenze funzionali, tecnologiche e regolamentari (grazie al know-how specialistico della società Promontory del Gruppo IBM), permettono di supportare le istituzioni finanziarie in un processo di adeguamento ai dettami del Regolatore.

L'esperienza e le competenze in ambito tecnologico di IBM Consulting, strettamente raccordate con priorità di business e con requisiti emergenti di modello operativo, possono garantire il raggiungimento degli obiettivi di adeguamento alla normativa, facendo sinergia e valorizzando capability organizzative e processi già esistenti.

L'utilizzo delle "new IT" a supporto

All'interno dei contesti aziendali ormai sempre più data driven, i processi di gestione del rischio giocano un ruolo di primo ordine per tutte le funzioni. Security e Compliance, per esempio, sono chiamati a partecipare sempre di più agli aspetti di gestione del dato, senza tralasciare l'importanza della prevenzione di rischi e incidenti ICT e una più generale gestione end-to-end degli eventi di sicurezza.

Gli enti finanziari stanno portando avanti progetti di trasformazione digitale, usando piattaforme open, scalabili, integrabili e multicloud, per permettere agli utenti e clienti di accedere ad applicazioni diverse in qualsiasi momento.

Per questo motivo, è fondamentale dotarsi di soluzioni di Security Information and Event Management (SIEM), anche integrate con soluzioni di Managed Detection and Response (MDR) che garantiscano alti livelli di sicurezza delle applicazioni, come richiesto dal Regolamento DORA.

L'utilizzo di best practice SIEM nel corso del tempo si è evoluto fino ad includere anche soluzioni di advanced analytics (ad esempio la User Behavior Analytics) e di Artificial Intelligence (AI) per accelerare il rilevamento e la gestione di possibili rischi e incidenti.

L'utilizzo di strumenti di AI per le attività di raccolta, organizzazione e analisi dei dati (creando specifici database pronti per il Business), abilita quindi le funzioni competenti ad individuare in modo proattivo e tempestivo le attività anomale e i degni di performance dei sistemi o delle reti, nonché possibili malware. Specifiche capability possono essere usate per definire indicatori di early warning e criteri per l'avvio automatico dei processi di individuazione e indirizzamento degli incidenti ICT.

L'individuazione tempestiva delle attività anomale e il successivo indirizzamento è, tra l'altro, uno degli obblighi che il Regolatore prevede di imporre agli enti finanziari: l'utilizzo di soluzioni basate sull'Intelligent Workflow – es. Business Process Management – permette agli utenti di attivare processi automatici che indirizzano tempestivamente gli incidenti, attivano eventuali processi di escalation e di comunicazione verso utenti, clienti e autorità competenti ed eseguono attività di reportistica. L'utilizzo di soluzioni integrate con specifici strumenti di robotica, garantisce inoltre, di ridurre la root cause analysis, accorciando di conseguenza la gestione complessiva dell'incidente.

Considerando la centralità dei dati per gli enti finanziari, strumenti basati su Machine Learning possono essere utilizzati ed "istruiti" per le attività di lettura dei log dei sistemi con l'obiettivo di identificare possibili vulnerabilità, possibili incidenti e di attuare successive attività di analisi degli storici e di confronto degli stessi anche con database di malware nazionali e internazionali.

Al fine di essere costantemente allineati al rapido contesto delle nuove minacce informatiche, gli enti finanziari possono utilizzare strumenti e sistemi IT con l'obiettivo di introdurre misure di prevenzione. L'analisi di dati e processi, mediante pratiche di data/process mining, permette alle funzioni - oltre che di identificare possibili efficientamenti sui processi e sulla gestione del dato - anche di adottare tecniche molto efficaci per le attività di fraud detection, intrusion detection, previsioni di incidenti e possibili degradamenti delle performance dei sistemi e delle reti.

Il fenomeno della Digital Transformation offre da anni alle funzioni di controllo l'opportunità di migliorare le proprie modalità operative e far leva su strumenti e processi a supporto anche delle fondamentali attività di test dei sistemi IT.

Come prescritto dalla bozza di normativa, le capacità e le funzioni incluse nel quadro di gestione dei rischi ICT dovranno essere sottoposte periodicamente a test, al fine di accertarne il grado di preparazione, identificarne punti deboli, carenze o lacune e verificarne la capacità di attuare tempestivamente misure correttive.

L'adozione di specifiche strategie di test delle nuove funzionalità e di quelle ritenute rilevanti per il proprio core business diventa cruciale per rafforzare la resilienza operativa.

Particolare rilevanza nel quadro normativo potrà avere anche la possibile dicotomia tra le consolidate pratiche di DevOps, che prevedono la sinergia continua tra sviluppatori e le funzioni di Operations, e la richiesta di DORA circa la garanzia di indipendenza delle funzioni addette all'esecuzione dei test.

Ad ogni modo, le strategie devono prevedere l'esecuzione di una serie completa di test adeguati, tra cui individuazione e valutazione delle vulnerabilità, analisi open source, valutazioni della sicurezza delle reti, analisi delle carenze, esami della sicurezza fisica, assessment su codice sorgente (ove fattibile), test di compatibilità, test basati su specifici scenari, stress test, test end-to-end o test di penetrazione.

Esempi concreti di best practice in questo ambito possono essere afferenti all'approccio del Chaos Engineering (introdotta da Netflix con il tool "Chaos Monkey" nel 2010): una pratica orientata all'individuazione di possibili incidenti IT e/o degradamento dei sistemi IT, prima che si trasformino in effettive interruzioni dei servizi. Testando in modo proattivo e randomico il modo in cui un sistema IT risponde sotto stress, è possibile infatti, identificare e correggere eventuali problemi prima che questi ultimi abbiano impatti sull'operatività utente e/o sui clienti finali.

La strategia si basa sull'individuazione di ipotesi su come un sistema IT dovrebbe comportarsi in caso di un problema (es. riavvio improvviso dei server o di singole istanze/servizi/applicazioni). Successivamente, si progetta un possibile scenario di test della casistica identificata e infine, viene misurato l'impatto del problema, nonché le attività da eseguire per evitare che il problema si presenti o, quantomeno, per ridurre al minimo gli impatti sulla Business Continuity.

Naturalmente, la tecnologia diventa sempre più efficace all'aumentare della consapevolezza del rischio operativo da parte degli utenti: campagne di sensibilizzazione, training ad hoc o campagne di phishing possono aiutare a migliorare la propria "security posture" e ad aumentare la consapevolezza verso la possibilità di incorrere in rischi operativi.

Pronti per la "DORA Compliance in a Box"?

La futura emanazione del Regolamento DORA evidenzia come la Commissione Europea si ponga l'obiettivo di preparare l'Europa per l'era digitale, promuovendo la regolamentazione della resilienza operativa digitale.

Come noto, IBM ha un ruolo fondamentale nel settore finanziario nazionale e globale, ed accoglie con favore l'obiettivo della normativa. DORA rappresenta solo un primo ma fondamentale passo verso la resilienza operativa dei servizi finanziari e, ancorché le tempistiche di approvazione non siano definite, i principali key driver identificati non dovrebbero essere oggetto di modifiche rilevanti.

L'evoluzione a cui sono chiamati gli enti finanziari potrebbe presentare problemi e rischi da affrontare durante la transizione: IBM Consulting propone, a tal fine, di avviare sin da subito attività in ambito «organizational awareness/education» con partecipazione ad appositi webinar/workshop con focus sulla normativa e sulla sua possibile evoluzione, nonché sui suoi possibili impatti dal punto di vista applicativo.

Al fine di poter individuare eventuali adeguamenti da un punto di vista strettamente tecnico, si consiglia di effettuare un primo assessment: un «DORA Compliance HealthCheck», per identificare l'aderenza del landscape applicativo/infrastrutturale ai primi pillar individuati dalla bozza di regolamento e quelli che possono essere, di contro, i possibili macro-gap da colmare.

IBM Consulting vuole mettere a disposizione un approccio end-to-end che ha come obiettivi quelli di analizzare, pianificare e prioritizzare le attività di adeguamento al Regolamento DORA e mette a disposizione team multi-funzionali con specifiche competenze con l'obiettivo di supportare le attività di:

- monitoraggio proattivo della normativa
- analisi dei framework di Risk & Incident Mgmt al fine di verificarne l'aderenza alle prime linee guida regolamentari di DORA, con particolare attenzione alla Cyber Security
- verifica di aderenza della propria test strategy al programma di test di Resilienza Operativa
- verifica del rispetto delle prime linee guida della normativa del framework per la gestione delle Terze Parti

Digital Operating Resilience Act

Sostenere il potenziale della finanza digitale, garantendo la resilienza operativa delle applicazioni e mitigando i rischi operativi ITC



Gestori di fondi e compagnie assicurative



Istituti di pagamento



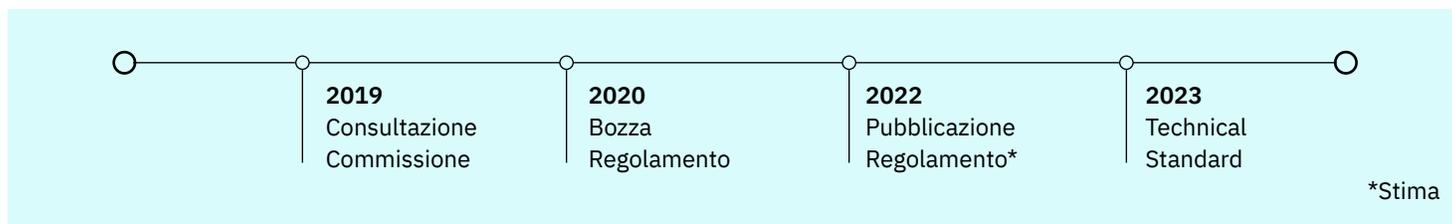
Banche



Istituti di moneta elettronica e fornitori di servizi di cripto-valuta

Principali impatti e perimetro di applicabilità

- Governance e struttura interna per adozione, gestione e monitoraggio di un framework per la corretta e tempestiva valutazione dei rischi ICT
- Valutazione e gestione integrata del rischio ICT, monitoraggio e reporting degli incidenti ICT
- Test di resilienza operativa digital per monitorare l'efficacia della strategia a garanzia della continuità operativa
- Revisione delle dipendenze da fornitori terzi e delle procedure di monitoraggio dei rischi associati a attività esternalizzate
- Condivisione informativa su minacce informatiche nella community di entità soggette al DORA



Perché IBM Consulting?

Advisor and Global Service ICT

Cognitive and Tech Asset Capabilities

Approccio end-to-end di cooperazione

Specializzazione sull'Industry Banking

Ecosistema di partner

Let's keep in touch per specifici workshop informativi sulle principali disposizioni della normativa DORA e sugli impatti per gli Enti Finanziari e relativi fornitori

Annex

Articolo 2 Ambito di applicazione soggettivo

1. Il presente regolamento si applica alle seguenti entità:
 - a. enti creditizi;
 - b. istituti di pagamento;
 - c. istituti di moneta elettronica;
 - d. imprese di investimento;
 - e. fornitori di servizi per le cripto-attività, emittenti di cripto-attività, emittenti di token collegati ad attività ed emittenti di token collegati ad attività significativi;
 - f. depositari centrali di titoli;
 - g. controparti centrali;
 - h. sedi di negoziazione;
 - i. repertori di dati sulle negoziazioni;
 - j. gestori di fondi di investimento alternativi;
 - k. società di gestione;
 - l. fornitori di servizi di comunicazione dati;
 - m. imprese di assicurazione e di riassicurazione;
 - n. intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio;
 - o. enti pensionistici aziendali o professionali;
 - p. agenzie di rating del credito;
 - q. revisori legali e imprese di revisione;
 - r. amministratori degli indici di referimen and critici;
 - s. fornitori di servizi di crowdfunding;
 - t. repertori di dati sulle cartolarizzazioni;
 - u. fornitori terzi di servizi di TIC

2. Ai fini del presente regolamento le entità di cui alle lettere da a) a t) sono definite collettivamente “entità finanziarie”

Autori



Alberto Fietta

Partner | Banking & Financial Markets
IBM Consulting

alberto.fietta@ibm.com



Marta Spinetoli

Senior Manager | Digital Strategy - Tech & Data Strategy
IBM Consulting

marta.spinetoli@ibm.com



Francesco Scarfò

Manager | Banking & Financial Markets
IBM Consulting

francesco.scarfo@ibm.com



Viola Luisa Saredi

Senior Consultant | Enterprise Strategy -
Tech & Data Strategy
IBM Consulting

viola.saredi@ibm.com

Footnotes

1. L'elenco completo degli enti finanziari è descritto dall'Articolo 2 Ambito di applicazione soggettivo del Regolamento DORA e riportato anche nella sezione "Annex"
2. Opinione BCE del 4 giugno 2021 sulla proposta di Regolamento DORA
3. European Banking Authority – EBA, European Insurance and Occupational Pension
4. JC_2022_02_esas_statement_esrb_recommendation_cyberincident
5. European Commission's Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM (2020) 595numbers, Authors

© Copyright IBM Corporation 2022

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
July 2022

IBM, the IBM logo, and IBM Trademarks List, are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

