Regolamento DORA: Digital Operational Resilience Act (DORA)

proofpoint®



Indice

¿Qué es DORA?

¿Cuál es la finalidad de DORA?

¿Cuáles son los 5 requisitos de DORA?

¿A qué entidades afecta DORA?

Alcance internacional de DORA

Situación actual y perspectivas de DORA

Aplicación de DORA

¿Qué desafíos afrontan las organizaciones con DORA?

DORA y los Servicios Financieros

DORA y los proveedores de TIC

Cómo prepararse para cumplir con DORA

En qué puede ayudarle Proofpoint

Cos’è il Digital Operational Resilience Act?

Il Digital Operational Resilience Act è un regolamento adottato dall’UE nel 2022 ed entrerà in vigore nel gennaio 2025. È stato concepito per armonizzare le norme e i requisiti relativi alla resilienza operativa per il settore finanziario in tutta l’UE, coprendo oltre 20 tipi diversi di entità finanziarie e fornitori di servizi ICT (Information and Communications Technology) di terze parti.

Più che una semplice salvaguardia raccomandata, il DORA è un regolamento fondamentale che mira a rafforzare la posizione di cybersecurity e la resilienza operativa del sistema finanziario europeo nel suo complesso. A tal fine, il DORA prevede che gli istituti finanziari comprendano l’intera infrastruttura IT, compresi i fornitori terzi, e identifichino le vulnerabilità e i rischi potenziali. Queste entità dovranno implementare strategie solide per proteggere i loro sistemi, i loro dati e i loro clienti eventuali disfunzioni.

Qual è lo scopo del regolamento DORA?

La normativa Digital Operational Resilience Act cerca di consentire al settore finanziario di: identificare, proteggere, rilevare, reagire e recuperare meglio gli incidenti legati ai servizi ICT che potrebbero minacciare l'erogazione di servizi finanziari critici. I suoi obiettivi principali includono:

- Rafforzare la sicurezza informatica e la resilienza operativa delle entità finanziarie dell'Unione Europea, come banche, compagnie assicurative e società di investimento.
- L'istituzione di un quadro completo garantisce che il settore finanziario possa resistere e riprendersi da gravi interruzioni operative, compresi gli attacchi informatici.
- Standardizzare i requisiti relativi alla resilienza operativa per il settore finanziario dell'UE, compresi i vari tipi di entità finanziarie e i fornitori di servizi ICT di terze parti.
- Garantire che gli istituti finanziari comprendano l'intera infrastruttura IT, compresi i fornitori di terze parti, consente di identificare potenziali vulnerabilità e rischi e di implementare strategie solide per proteggere i sistemi, i dati e i clienti da eventuali interruzioni.

Lo scopo principale di DORA è quello di elevare gli standard di cybersecurity e la resilienza operativa digitale nel settore finanziario europeo. L'obiettivo è andare oltre le semplici misure difensive, sostenendo un solido quadro di resilienza che garantisca la continuità e la qualità dei servizi finanziari, anche a fronte di significative interruzioni operative.

Quali sono i 5 requisiti della normativa DORA?

Il quadro completo della DORA per il rafforzamento della cybersicurezza e della resilienza operativa del settore finanziario dell'UE è strutturato su cinque requisiti chiave:

1.Gestione del rischio ICT

Il regolamento DORA richiede che le entità finanziarie dispongano di un solido quadro di gestione del rischio ICT con strategie, politiche e procedure per la protezione delle informazioni, del software e delle risorse fisiche. Inoltre, le entità devono condurre analisi dell'impatto sul business, creare piani di risposta e ripristino e testarli regolarmente. Devono anche implementare programmi di security awareness per tutto il personale e il management.

2. Gestione, classificazione e segnalazione degli incidenti legati alle ICT

Le entità devono essere in grado di classificare, affrontare e segnalare rapidamente gli incidenti e le minacce informatiche alle autorità di regolamentazione e alle parti interessate. Gli incidenti devono essere segnalati entro quattro ore dal momento in cui se ne viene a conoscenza, e un rapporto più dettagliato deve essere fornito entro una settimana. Ciò richiede che le entità dispongano di solidi piani di risposta agli incidenti e di processi per l'analisi delle cause principali.

3. Test di resilienza operativa digitale

La DORA richiede alle entità di condurre test regolari sui propri sistemi e infrastrutture ICT per valutare le vulnerabilità e l'efficacia delle misure di protezione. Ciò include test di base annuali e test di penetrazione più completi guidati dalle minacce ogni tre anni per identificare lacune e punti deboli nelle capacità di resilienza dell'ente.

4. Gestione del rischio ICT proveniente da terze parti

Il DORA impone alle entità di gestire attivamente i rischi ICT posti dai fornitori di servizi terzi, anche effettuando due diligence e audit. I contratti con le terze parti devono includere disposizioni per la sicurezza, la segnalazione degli incidenti e le strategie di uscita. Le entità sono inoltre responsabili di garantire che le terze parti rispettino i requisiti del DORA.

5. Condivisione di informazioni e intelligence

Per contribuire a creare una consapevolezza collettiva e a sviluppare le migliori pratiche per prevenire e rispondere alle minacce informatiche, le entità sono incoraggiate a partecipare alla condivisione volontaria di cyber threat intelligence con altri istituti finanziari. La condivisione delle informazioni deve essere conforme alle normative sulla protezione dei dati ed evitare di divulgare informazioni sensibili sui clienti.

Implementando questi cinque requisiti, le entità finanziarie dell'UE possono rafforzare la loro resilienza operativa digitale complessiva e resistere e riprendersi meglio da gravi interruzioni legate alle TIC.

Quali sono le entità interessate dalla DORA?

Il campo di applicazione del regolamento DORA è ampio e copre una vasta gamma di entità e servizi finanziari dell'UE. Le principali entità interessate dalla DORA sono:

Istituzioni finanziarie tradizionali

- Istituti di credito (banche)
- Istituti di pagamento
- Istituti di moneta elettronica
- Imprese di investimento
- Società di assicurazione e riassicurazione
- Agenzie di rating del credito

Questi operatori tradizionali del settore finanziario sono i principali obiettivi di DORA, in quanto responsabili di servizi finanziari critici e detentori di grandi quantità di dati sensibili dei clienti.

Entità finanziarie emergenti

- Fornitori di servizi di cripto-asset (CASP)
- Fornitori di servizi di crowdfunding
- Gestori di fondi di investimento alternativi (GEFIA)
- Società di gestione di OICVM

Il DORA copre anche i nuovi operatori dei mercati finanziari, riconoscendo il loro ruolo crescente nella fornitura di servizi e la necessità di garantire la resilienza operativa.

Fornitori di servizi critici di terze parti

- Fornitori di cloud computing
- Operatori di data center
- Fornitori di software
- Aziende di analisi dei dati

La DORA include fornitori di servizi ICT critici di terze parti che supportano le operazioni delle entità finanziarie. Questi fornitori sono considerati di importanza sistemica e devono anch'essi rispettare i requisiti della DORA.

Ambito internazionale del regolamento DORA

La DORA è una rete ampia, che copre una vasta gamma di istituzioni finanziarie e fornitori di servizi dell'UE. Tuttavia, il suo campo di applicazione va oltre le istituzioni con sede nell'UE: il DORA copre anche le entità finanziarie non UE che operano nei mercati europei. Ciò significa che anche se un'organizzazione ha sede al di fuori dell'UE ma è presente o fornisce servizi all'interno dell'UE, è comunque soggetta alle normative DORA.

L'ampia portata di DORA è intenzionale, in quanto mira a migliorare la resilienza operativa complessiva dell'intero settore finanziario europeo. Coinvolgendo banche tradizionali, operatori fintech emergenti e fornitori di servizi critici di terze parti, DORA cerca di mitigare i rischi sistemici derivanti da interruzioni o incidenti informatici che colpiscono qualsiasi parte dell'ecosistema finanziario.

Stato attuale e prospettive per DORA

A partire dalla primavera del 2024, il Digital Operational Resilience Act si trova nel periodo di attuazione, che dura due anni dal momento della sua entrata in vigore. Ciò significa che tutte le entità finanziarie interessate nei mercati dell'UE e i loro fornitori di ICT critici devono essere pronti a conformarsi completamente ai requisiti della DORA entro gennaio 2025.

Sebbene i regolatori europei stiano ancora ultimando i dettagli tecnici specifici, l'ambito e i requisiti generali della normativa DORA sono ormai chiari. Nel gennaio 2024, le autorità di vigilanza europee (ESA) hanno pubblicato la prima serie di requisiti previsti dalla DORA per la gestione del rischio ICT e di terzi e la classificazione degli incidenti. Queste regole sono disponibili sul sito web del European Insurance and Occupational Pensions Authority.

Applicazione del regolamento DORA

Dopo un periodo di attuazione di due anni, la legge sulla resilienza operativa digitale sarà pienamente applicabile a partire da gennaio 2025. Le autorità di regolamentazione competenti in ogni Stato membro dell'UE applicheranno i requisiti della DORA. Tali autorità avranno il potere di monitorare la conformità e di imporre sanzioni alle entità finanziarie che non rispettano gli standard del regolamento.

Gli aspetti critici degli standard di applicazione della DORA includono:

- **Sorveglianza normativa:** le autorità di vigilanza controlleranno attentamente la conformità delle entità finanziarie ai requisiti del DORA, tra cui: la gestione del rischio ICT, la segnalazione degli incidenti, i test di resilienza e le pratiche di gestione del rischio di terzi.
- **Sanzioni in caso di non conformità:** le autorità possono imporre sanzioni significative agli istituti finanziari che non rispettano gli standard della DORA. Queste sanzioni possono includere multe amministrative fino all'1% del fatturato annuo totale dell'ente, nonché altre azioni correttive come rimproveri pubblici o addirittura la revoca dell'autorizzazione a operare.
- **Orientamento e coordinamento:** le autorità di regolamentazione forniranno inoltre linee guida e indicazioni sulle migliori pratiche per aiutare le entità finanziarie a conformarsi al DORA. Inoltre, promuoveranno il coordinamento e l'uniformità delle pratiche di vigilanza in tutta l'UE per garantire condizioni di parità.
- **Supervisione delle terze parti critiche:** DORA introduce un nuovo quadro per la supervisione dei fornitori terzi di servizi ICT critici che supportano il settore finanziario. Questi fornitori saranno soggetti a una supervisione diretta da parte delle autorità di vigilanza europee per gestire i rischi che comportano per le entità finanziarie.

Dando alle autorità di regolamentazione la possibilità di monitorare da vicino la conformità e di imporre sanzioni significative, il DORA mira a garantire che le istituzioni finanziarie dell'UE adottino le misure necessarie per rispettare gli standard normativi del DORA.

Quali sono le sfide che le organizzazioni devono affrontare con il DORA?

Nel momento in cui le entità finanziarie procedono verso la conformità con il Digital Operational Resilience Act, si trovano ad affrontare diverse sfide e ostacoli fondamentali per soddisfare gli standard del DORA.

Complessità dei requisiti normativi

Data la loro natura complessa, l'interpretazione e la comprensione delle numerose normative DORA può essere impegnativa. Le organizzazioni devono investire tempo e risorse significative per comprendere a fondo i requisiti della normativa e sviluppare strategie di conformità su misura.

Vincoli delle risorse

Molte organizzazioni devono fare i conti con le limitazioni di budget, manodopera e competenze tecniche necessarie per implementare le robuste misure di conformità richieste dal DORA. Ciò include la conduzione di valutazioni approfondite del rischio, l'investimento in soluzioni avanzate di cybersecurity e l'aggiornamento dei sistemi IT esistenti.

Legacy IT Systems

Le infrastrutture obsolete e i sistemi legacy all'interno delle entità finanziarie possono non avere le capacità e le misure di sicurezza necessarie per soddisfare i requisiti della DORA. L'aggiornamento o la sostituzione di questi sistemi può essere un'impresa costosa e complessa.

Minacce informatiche in continua evoluzione

La natura dinamica e sofisticata delle minacce informatiche rappresenta una sfida costante per le organizzazioni che cercano di mantenere la conformità alle normative. Il monitoraggio, la valutazione e il miglioramento continui delle misure di sicurezza sono necessari per tenere il passo con l'evoluzione del panorama delle minacce.

Gestione del rischio proveniente dalle parti terze

La DORA pone un'enfasi significativa sulla gestione dei rischi ICT posti dai fornitori di servizi terzi. Le entità finanziarie devono stabilire solidi processi di supervisione e due diligence per la loro vasta rete di fornitori, il che può essere un'impresa complessa e dispendiosa in termini di risorse.

Test di resilienza

Verificare regolarmente la resilienza operativa digitale delle entità finanziarie, come richiesto dalla DORA, può essere una sfida. Le organizzazioni devono sviluppare un approccio strategico e coordinato alle valutazioni di vulnerabilità, ai test di penetrazione e ad altri esercizi di resilienza per garantire una copertura completa delle loro funzioni critiche.

Promuovere la cultura della conformità

Per un'efficace conformità al DORA è fondamentale creare una cultura di consapevolezza del rischio, responsabilità e miglioramento continuo in tutta l'organizzazione. Il superamento delle mentalità isolate e l'allineamento di vari team, come quelli dell'IT, della compliance, dell'ufficio legale e della gestione del rischio, possono rappresentare una sfida significativa.

Per affrontare queste sfide è necessario che le entità finanziarie adottino un approccio proattivo e collaborativo, sfruttando, se necessario, competenze e soluzioni esterne. Un'attenta pianificazione, un'allocazione strategica delle risorse e l'impegno a migliorare la resilienza operativa digitale saranno essenziali per soddisfare con successo i requisiti del DORA.

Il regolamento DORA ed i servizi finanziari

Il settore dei servizi finanziari è stato identificato come un obiettivo primario per le minacce informatiche, sottolineando la necessità critica di solide misure di resilienza operativa. Secondo il Fondo Monetario Internazionale (FMI), la loro indagine ha rilevato che il settore finanziario è a rischio a causa della debolezza delle difese di sicurezza informatica.

A questo parere fa eco la Banca d'Inghilterra, il cui ultimo sondaggio sul rischio sistemico ha rivelato che il 74% degli intervistati considera gli attacchi informatici come il rischio più elevato per il settore finanziario.

Strutture normative come DORA sono diventate fondamentali per aiutare le istituzioni finanziarie e i loro fornitori associati, come i fornitori di ICT, a capire come gestire efficacemente questi rischi informatici in continua evoluzione. Recenti ricerche di settore evidenziano le significative minacce informatiche che il settore finanziario deve affrontare:

- Il Verizon 2022 Data Breach Investigations Report (DBIR) ha registrato le minacce più diffuse, tra cui violazioni di dati, attacchi DDoS e ransomware. Il rapporto sottolinea che il furto di credenziali è un fattore chiave per il successo di molti di questi attacchi.
- Un'indagine della Commodity Futures Trading Commission del 2022 ha rilevato che il 74% delle 130 istituzioni finanziarie globali intervistate ha subito almeno un attacco ransomware nell'anno precedente.

Queste statistiche allarmanti sottolineano l'urgente necessità per le entità finanziarie di rafforzare la propria posizione di cybersecurity e la propria resilienza operativa in linea con regolamenti come il DORA.

DORA e fornitori di ICT

La legge sulla resilienza operativa digitale enfatizza fortemente la gestione del rischio di terzi, riconoscendo il ruolo significativo che i fornitori di ICT svolgono a supporto del settore dei servizi finanziari.

Una ricerca di settore evidenzia la crescente minaccia di attacchi alla catena di fornitura rivolti al settore finanziario. Secondo il Verizon 2022 Data Breach Investigations Report, il settore finanziario è stato il secondo obiettivo più popolare per questo tipo di attacchi. Il DORA mira ad affrontare questa vulnerabilità stabilendo requisiti completi per le entità finanziarie per gestire i rischi ICT posti dai loro fornitori di servizi terzi.

L'Agenzia dell'Unione Europea per la Cybersecurity (ENISA) ha segnalato un aumento della complessità e del volume degli attacchi alla catena di fornitura, con gli attori delle minacce che prendono di mira la catena di fornitura tecnologica per rubare dati e risorse finanziarie. Le disposizioni del DORA per la gestione del rischio di terzi coordineranno i requisiti utilizzando i quadri esistenti, come le linee guida sull'outsourcing dell'Autorità bancaria europea (EBA).

Qualsiasi fornitore di TIC designato come "critico" da un'autorità di vigilanza europea sarà soggetto a un rigoroso quadro di supervisione. Questo controllo rafforzato garantisce che questi fornitori di tecnologia di importanza critica per il sistema implementino solide misure di sicurezza e rispettino i requisiti della DORA.

Le istituzioni finanziarie si rivolgono sempre più spesso a soluzioni Zero Trust per gestire efficacemente i rischi di terzi. Queste tecnologie forniscono una maggiore visibilità sulla rete estesa di fornitori, compresi i fornitori di ICT. Applicando misure di sicurezza come l'accesso con privilegi minimi e il controllo proattivo delle aree e dei dati sensibili, Zero Trust aiuta a prevenire le violazioni dei dati e a mitigare l'impatto del ransomware e di altre minacce informatiche.

Come prepararsi alla conformità DORA

Con l'avvicinarsi del termine di applicazione del Digital Operational Resilience Act, previsto per gennaio 2025, gli istituti finanziari devono adottare misure proattive per assicurarsi di essere pronti a soddisfare i requisiti della normativa. Ecco alcuni consigli utili per prepararsi in modo proattivo alla conformità al DORA:

Comprendere a fondo la DORA regulation

- Studia a fondo la regolamentazione DORA, i suoi requisiti specifici e il modo in cui si applica alla tua organizzazione.
- Prendi in considerazione l'idea di seguire una formazione specializzata, come ad esempio diventare uno Specialista di conformità certificato DORA, per approfondire la tua conoscenza della normativa.

Valutare i rischi informatici

- Esegui una valutazione completa dei rischi informatici nella tua organizzazione e nella catena di fornitura estesa.
- Utilizza soluzioni di valutazione del rischio per identificare e valutare le potenziali vulnerabilità.

Adottare un principio di proporzionalità

- Assicurati che il tuo approccio alla conformità DORA tenga conto della portata, della complessità e dell'importanza delle dipendenze e dei rischi legati all'ICT.
- Prendi decisioni informate sulla gestione del rischio che siano in linea con i requisiti della normativa.

Coinvolgere team interfunzionali

- Coinvolgi più team nel processo di conformità DORA, tra cui: sicurezza IT, legale, conformità, gestione del rischio e senior leadership.
- Garantisci un approccio olistico e globale all'organizzazione per affrontare i requisiti DORA.

Responsabilizzare la dirigenza

- Assicurati che l'alta dirigenza guidi l'implementazione del DORA e riceva una formazione adeguata, ad esempio diventando un Certified Cyber Risk Officer.
- Assicurati il consenso e il supporto del consiglio di amministrazione per le modifiche necessarie relative al DORA.

Revisione e aggiornamento regolari dei piani

- Esamina e aggiorna continuamente la tua strategia di resilienza operativa digitale e le politiche di gestione del rischio ICT di terze parti per rimanere in linea con il DORA.
- Mantieni un approccio agile per apportare le modifiche necessarie in base all'evoluzione delle normative e delle minacce.

Dare priorità alle azioni di rimedio

- Sviluppa un processo semplice per stabilire le priorità e affrontare le vulnerabilità operative identificate attraverso le valutazioni DORA.
- Concentrati prima sulle aree più critiche per mitigare i rischi più importanti.

Produrre prove dimostrabili

- Sii in grado di fornire ai funzionari di vigilanza le prove che la tua organizzazione è in grado di resistere sia alle minacce specifiche dell'azienda che a quelle più ampie del settore.
- Mantieni una documentazione completa per dimostrare i tuoi sforzi di conformità al DORA.

Tenere conto dell'ambiente esterno

- Monitora regolarmente il panorama delle minacce esterne e incorpora queste informazioni nella tua strategia generale di resilienza operativa.
- Rimani informato sui rischi potenziali e adotta misure proattive per mitigarli.

Identificare le funzioni critiche

- Identifica chiaramente le funzioni critiche o importanti (CIF) all'interno della tua organizzazione in base ai requisiti DORA.
- Assicuratevi che queste funzioni siano il punto focale per costruire una solida resilienza operativa.

Seguendo questi suggerimenti completi, gli istituti finanziari possono prepararsi meglio ai prossimi requisiti di conformità DORA e rafforzare la loro resilienza operativa digitale complessiva.

In che modo Proofpoint può aiutare

Proofpoint offre una gamma di soluzioni e competenze che possono aiutare le organizzazioni del settore finanziario a conformarsi efficacemente ai requisiti del Digital Operational Resilience Act. Le capacità di Proofpoint possono migliorare la resilienza complessiva della cybersecurity e le capacità di risposta agli incidenti di un'organizzazione. Fornendo strumenti di **advanced threat detection**, prevention e response, Proofpoint consente alle aziende di proteggersi meglio da: le minacce informatiche esterne, i rischi insider e le vulnerabilità della supply chain, tutti componenti critici della conformità alla DORA e alla direttiva Network and Information Systems (NIS 2).

Come incoraggiato da queste normative, Proofpoint facilita anche la condivisione delle informazioni e lo scambio di informazioni sulle minacce. I **servizi di threat intelligence** e le piattaforme di collaborazione sicure dell'azienda aiutano le organizzazioni a rimanere informate sulle ultime minacce informatiche e a coordinare i loro sforzi di risposta con gli stakeholder e le autorità competenti. Dall'esecuzione di valutazioni del rischio e analisi delle lacune allo sviluppo di strategie di conformità su misura, Proofpoint può aiutare le organizzazioni a comprendere le loro capacità attuali, a identificare le aree di miglioramento e a implementare i controlli e i processi necessari.

Inoltre, le soluzioni di Proofpoint consentono anche il monitoraggio continuo della conformità e il reporting. Le organizzazioni possono sfruttare gli strumenti di Proofpoint per valutare regolarmente la loro posizione di sicurezza, identificare le vulnerabilità e generare la documentazione necessaria per dimostrare la loro aderenza ai requisiti DORA e NIS 2 agli enti normativi.

Collaborando con Proofpoint, le istituzioni finanziarie e altri fornitori di infrastrutture critiche possono rafforzare la loro resilienza operativa digitale complessiva e soddisfare i rigorosi standard di cybersecurity stabiliti da queste importanti normative europee. Per saperne di più, **contatta Proofpoint**.