

CORA DORA è il modulo di GRC CORA pensato per supportare le aziende nei processi di adeguamento al **Regolamento DORA - Digital Operation Resilience Act**: analisi e valutazione del rischio, definizione e implementazione del piano per la gestione dei rischi informatici, monitoraggio e valutazione dei rischi legati alle “terze parti”.

Il contesto normativo

Il DORA è un **regolamento dell' UE relativo al settore dei servizi finanziari**.

Il DORA si riferisce esplicitamente ai servizi finanziari nell'UE, con una particolare attenzione al mantenimento della resilienza nella cybersicurezza.

Come il GDPR, il DORA **consolida e aggiorna la gestione dei rischi nel settore ICT** e la gestione dei rischi informatici nei servizi finanziari.

Nello specifico, il documento ha l'obiettivo di:

- **rafforzare e armonizzare a livello europeo i principali requisiti di cybersecurity** per i soggetti operanti nell'ambito finanziario e assicurativo;
- **armonizzare i requisiti di rischio delle tecnologie dell'informazione e della comunicazione** (di seguito, “tecnologie ICT”) in tutta l'Unione Europea, creando un approccio comune in tutto il settore dei servizi finanziari;
- **garantire che tutti i soggetti interessati dispongano di idonee garanzie per mitigare eventuali attacchi informatici e altri rischi cyber**, attraverso l'implementazione di misure di governance, gestione del rischio del tecnologie ICT e segnalazione degli incidenti.

La soluzione

Il Regolamento propone sei diversi “pillar” che le Organizzazioni dovranno implementare:

- ICT Governance;
- ICT Risk Management;
- Gestione degli incidenti;
- Test di Resilienza;
- Rischi Terze Parti;
- Condivisione delle informazioni.

CORA DORA supporta le aziende e gli enti nell'intero percorso di gestione delle attività necessarie per la valutazione del rischio di cybersicurezza:

- Identificazione dei **rischi** e **simulazione scenari**;
- Applicazione delle **misure di sicurezza**;
- Valutazione dell'**efficacia delle misure** applicate;
- Valutazione del **livello di compliance e garanzie offerte delle “terze parti”**;
- Gestione centralizzata del **piano per la gestione dei rischi informatici**;
- Gestione completa degli **incidenti**; (identificazione, valutazione, comunicazione, azioni correttive);
- **Analytics e reportistica**.

CORA DORA è integrabile con i sistemi già presenti in azienda (quali soluzioni HR, identity management, log collectors, ...).

A chi si applica

Il Regolamento DORA si rivolge a un **ampio novero di operatori finanziari**, quali enti creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti, istituti di moneta elettronica, imprese di investimento, fornitori di servizi per le cripto-attività, depositari centrali di titoli, controparti centrali, sedi di negoziazione, repertori di dati sulle negoziazioni, gestori di fondi di investimento alternativi, società di gestione, fornitori di servizi di comunicazione dati, imprese di assicurazione e di riassicurazione, intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio, enti pensionistici aziendali o professionali, agenzie di rating del credito, amministratori di indici di riferimento critici, fornitori di servizi di crowdfunding, repertori di dati sulle cartolarizzazioni.

Le istituzioni finanziarie non riescono a soddisfare I requisiti DORA **possono essere soggetti a multe fino a 10 milioni di euro o al 5% del loro fatturato** annuo totale.

In breve



INFRASTRUTTURA DI SUPPORTO

Disegna l'infrastruttura informatica per avere un'immagine dettagliata della tua organizzazione e di dove vengono conservati i dati.



PIANO PER LA GESTIONE DEI RISCHI INFORMATICI

Organizza il piano di gestione dei rischio informatici in un repository centrale sempre aggiornato.



GESTIONE DEGLI INCIDENTI

Mantieni il registro degli incidenti, identifica gli owner e le azioni da intraprendere per il contrasto.



ANALISI DEL RISCHIO

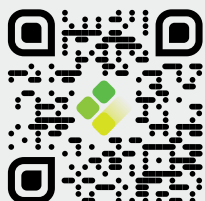
Effettua valutazioni sul rischio in ambito di cybersicurezza, identifica e valuta l'efficacia delle misure di sicurezza. Permette la simulazione di scenari di rischio.



VALUTAZIONE DELLE TERZE PARTI

Effettua valutazioni sulle «terze parti» attraverso survey e connessioni con banche dati di rating per identificare potenziali rischi derivanti.

La suite per la compliance
semplice, completa, scalabile.



CORA DORA è parte della soluzione GRC CORA.

GRC CORA è una soluzione personalizzabile e modulabile in base alle specifiche esigenze di ogni realtà.



Cloud
Marketplace

Ci trovi sul Marketplace ACN
Catalogo dei servizi Cloud
per la PA qualificati