REGOLAMENTO D.O.R.A.

Digital Operational Resilience Act

il Digital Operational Resilience Act nasce con l'obiettivo di rafforzare e armonizzare i requisiti operativi in ambito cybersecurity nel Settore Bancario, Finanziario e Assicurativo, ivi comprese le Società di Servizi di Criptovalute.

www.motoreunicoamministrativo.it

Cos'è D.O.R.A.

Si tratta di un Regolamento, ovvero di una Norma Europea immediatamente applicabile in tutti gli Stati membri dell'Unione, senza bisogno di alcuna legge di recepimento, nato per garantire che le Imprese del Settore Finanziario e Assicurativo siano in grado di affrontare attacchi informatici anche di grave portata, aventi impatto pesante sull'operatività aziendale, attraverso l'implementazione di Misure di Sicurezza, Gestione del Rischio, Governance, Cybersecurity e Incident Reporting.

D.O.R.A. si inserisce nel solco dell'attività legislativa europea volta a contrastare la crescita e la gravità dei cyberattacchi e delle loro conseguenze, per incrementare la resilienza, ovvero la continuità operativa del Settore Finanziario di tutti gli Stati appartenenti all'Unione.

Lo scopo principale di D.O.R.A. è quello di adottare requisiti di sicurezza standard per prevenire e reagire a minacce informatiche che non solo si fanno sempre più sofisticate ma che, qualora colpiscano il bersaglio, possono avere conseguenze di portata dirompente al di là di ogni immaginazione per tutti i cittadini dell'Unione e dell'intero pianeta.

Punti Cardine

01 Necessità di Governance e Organizzazione Interna

I soggetti interessati dovranno costituire al proprio interno un Dipartimento di Governance del Rischio in grado di garantire un monitoraggio costante dei rischi IT, la predisposizione delle misure di sicurezza e la gestione di eventuali incidenti in tempo rapido, al fine di garantire un elevato livello di Resilienza Operativa Digitale.

02 Obbligo di gestire il Risk Management

Sarà obbligatorio formulare un Quadro di Gestione del Rischio solido, completo e ben documentato, con evidenza di quali sono state le scelte compiute in termini di strumenti IT, identificazione degli Entry Point di rischio, e adozione di Procedure di Prevenzione e Protezione.

03 Creazione delle procedure per Incident Management e Reporting

Il Regolamento prevede l'obbligo di scrivere e applicare Procedure per garantire la Business Continuity e il Disaster Recovery, dotarsi di Personale idoneamente ed accuratamente formato pronto a rilevare vulnerabilità, minacce, incidenti e attacchi informatici e valutarne le conseguenze, nonché prevedere Piani di Comunicazione nei confronti degli Stakeholder.

04 Gestione dei Fornitori di Servizi Critici ICT

Le Autorità di Vigilanza in ambito finanziario avranno specifici poteri di sorveglianza non solo nei confronti dei diretti interessati all'applicabilità del Regolamento ma anche verso i Fornitori di Servizi Critici, quali ad esempio i servizi erogati in Cloud.

Road Map

DORA sarà sottoposto ad un periodo di “vacatio” o grace period: gli operatori interessati avranno 24 mesi per conformarsi e uniformarsi agli standard richiesti, a decorrere dall’entrata in vigore del Regolamento, che dunque diventerà pienamente operativo a fine 2024.

Anche per questo Regolamento vale il principio dell’approccio basato sul rischio e il concetto di **Accountability:** saranno le Aziende destinatarie della Normativa, con l’adozione di un approccio proattivo e consapevole, a stabilire quali saranno le azioni da porre in essere all’interno del framework stabilito da DORA che dovrebbe articolarsi come di seguito:

01 Gap Analysis dell’ICT Risk Management Framework

02 Revisione della Struttura di Governance interna e delle Misure di Gestione dei Rischi e Incidenti ICT già adottate

03 Verifica del grado di Preparazione e Consapevolezza Aziendale rispetto al nuovo Impianto Normativo

04 Valutazione Status Quo rispetto al Regolamento in termini di Risorse, Strategie e Procedure di risposta agli incidenti.

05 Valutazione Piani di Aggiornamento e Adeguamento secondo l'Assessment e il Profilo di Rischio Aziendale

La Soluzione?

Adottare uno strumento in grado di garantire tutte le esigenze che emergono dalla compliance a DORA; uno strumento che, ad esempio, **garantisca in automatico** l'effettuazione di tutti gli adempimenti previsti da DORA.

Lo strumento, il **MUA** (Motore Unico Amministrativo) di **L&T Group**, esiste ed è già presente sul mercato, **adottato con successo da anni da centinaia di enti e aziende** e **già aggiornato per supportare tutte le prescrizioni di DORA.**

L&T Group ha anni di esperienza nel supportare i propri clienti nell'adozione di MUA, attraverso progetti condotti dalla propria area di **Consulenza**, che hanno attivato MUA in grosse realtà nazionali.

L&T Group dispone inoltre della propria **L&T Academy** per indirizzare con successo la necessaria **formazione del personale** del cliente.

Infine, L&T ha una comprovata presenza pluriennale anche nell'ambito dei servizi operativi mirati alla CyberSecurity, con il proprio **SOC** e il servizio **MDR** (Managed Detectionand Response).

L'insieme di questi prodotti e servizi costituisce quindi **la migliore soluzione al problema dell'adeguamento al framework DORA presente sul mercato, stabile, affidabile e già pronta all'uso.**

Modulo MUA - D.O.R.A.

Il Modulo MUA-D.O.R.A prevede lo sviluppo, l'automazione e l'aggiornamento degli adempimenti richiesti dal Regolamento, attraverso le seguenti attività:

01 **Predisposizione Quadro per la Gestione Rischi Informatici, anche attraverso Asset Tracker e Sistemi di Vulnerability Management**

02 **Monitoraggio delle Misure di Sicurezza e Remediation**

03 **Predisposizione, Aggiornamento e Monitoraggio della Business Impact Analisys, Piano di Continuità Operativa e Disaster Recovery**

04 **Gestione Formalizzazione dei Ruoli Obbligatori previsti dalla Norma**

05 **Attività di Audit**

06 **Gestione Incident e Procedura di Comunicazione alle Autorità Competenti**

07 **Predisposizione e Aggiornamento Piano di Comunicazione della Crisi**

08 **Procedura di Gestione Fornitori TIC**

09 **Realizzazione del Programma Test di Resilienza**

MUA Framework - Integrated Compliance

Mappatura

- Organigramma
- Processi
- Strumenti
- Normative

Adeguamento

- D.O.R.A.
- Privacy
- Prevenzione della Corruzione
- D.Lgs. 231/2001
- D.Lgs. 81/2008
- Gestione integrata del rischio
- Manuale di gestione
- Piano di fascicolazione
- Manuale di conservazione
- Mappatura dei Processi
- Sicurezza informatica
- NIS
- Sistema Digitale di Approvazione