CYBERSECURITY GOVERNANCE

CISO esterno. Cybersecurity governata come rischio d impresa.

Leadership senior per strategia, cyber risk, controlli, incident readiness, supply chain, NIS2, DORA e ISO/IEC 27001, con reporting al management.

La sicurezza non e solo tecnologia. E una decisione continua su rischio, priorita e resilienza.

UESE garantisce la funzione CISO esterna accanto a direzione e IT, trasformando requisiti e minacce in una roadmap governabile.

Scheda online

Cyber risk

Priorita basate sul rischio reale

NIS2 / DORA

Allineamento agli obblighi applicabili

ISO 27001

Integrazione con SGSI e framework di controllo

Board report

KPI e KRI per decisioni executive

Una funzione senior, con una rete che si adatta all'organizzazione.

Il referente UESE può essere affiancato da consulenti junior e senior in Italia e all'estero, selezionati in base a settore, sedi, lingua, rischio e complessita. Il coordinamento, il metodo e il reporting restano UESE.

RICHIEDI UN CONFRONTO

VEDI LA SCHEDA ONLINE

Il ruolo, il perimetro e le responsabilita

Il CISO esterno e una funzione di governance della sicurezza delle informazioni. Definisce strategia, framework di controllo, gestione del rischio, incident readiness, terze parti, metriche e reporting, coordinandosi con direzione, IT, SOC/MDR e fornitori.

FUNZIONE

Cosa presidia

Cybersecurity strategy, cyber risk, policy e controlli, incident response, business continuity, terze parti, awareness, NIS2/DORA/ISO 27001 e reporting al management.

RESPONSABILITA

Cosa non sostituisce

Il CISO abilita controllo e competenza ma non sostituisce le responsabilita che leggi e regolamenti attribuiscono agli organi di amministrazione e all organizzazione.

Attivita chiave

01

Strategia e rischio

Roadmap, asset critici, scenari, trattamento e rischio residuo.

02

Controlli e resilienza

IAM, vulnerabilita, backup, incident, BCP/DR, cloud e terze parti.

03

Governance e reporting

KPI/KRI, NIS2, DORA, ISO 27001 e board reporting.

Riferimenti principali

D.Lgs. 138/2024 (NIS2); Regolamento (UE) 2022/2554 (DORA) per i soggetti applicabili; ISO/IEC 27001 quale riferimento volontario per i sistemi di gestione della sicurezza delle informazioni.

Servizi e attivita erogate

Il perimetro viene dimensionato sul rischio reale e trasformato in un piano di attivita verificabile.

01

Cyber strategy

Target, priorita, investimenti e roadmap pluriennale.

02

Cyber risk

Asset, scenari, valutazione, trattamento e rischio residuo.

03

Control framework

Policy e controlli su accessi, patch, backup, cloud e dati.

04

Incident readiness

Response, crisis, BCP/DR, escalation ed esercitazioni.

05

Third-party risk

Due diligence, requisiti, classificazione e monitoraggio.

06

Compliance & board

NIS2, DORA, ISO 27001, KPI/KRI e reporting executive.

Deliverable tipici

- Cybersecurity roadmap con owner e milestone
- Cyber risk register e piano di trattamento
- Control framework con evidenze attese
- Incident & crisis response plan
- Dashboard KPI/KRI e terze parti
- Board cyber report su rischio residuo e priorita

Il modello UESE

Un incarico esterno deve creare continuita, controllo e accesso a competenze che l'organizzazione possa utilizzare davvero.

01

Baseline

Asset, rischi, architettura, controlli e obblighi.

02

Roadmap

Target, priorita, quick win e programma.

03

Governance

Policy, comitati, SOC/MDR, fornitori e incident.

04

Board report

KPI/KRI, rischio residuo e decisioni richieste.

Vantaggi per l'organizzazione

Leadership senior

Guida autorevole senza creare subito un CISO full-time.

Visione indipendente

Priorita basate sul rischio, non sul prodotto tecnologico.

Allineamento

Un coordinamento per NIS2, DORA e ISO 27001.

Misurabilita

KPI, KRI e roadmap per rendere la cyber governabile.

Rete UESE: staff + consulenti junior e senior, Italia e estero

Professionisti e società specialistiche possono candidarsi attraverso il Supplier Portal UESE.

PARLA CON UESE

DIVENTA FORNITORE