HADRIAN

Lista di controllo per la conformità al DORA

Nell'affrontare il dinamico panorama del settore finanziario, il Digital Operational Resilience Act (DORA) rappresenta un punto di riferimento cruciale per le organizzazioni che intendono intraprendere un percorso volto al miglioramento della propria resilienza operativa. Per consentire alla tua organizzazione di ottenere e mantenere la conformità al DORA, è stata creata questa esaustiva lista di controllo che funge da tabella di marcia strategica.

Ogni elemento è stato meticolosamente studiato per guidare la tua organizzazione nello sfaccettato territorio del DORA, incoraggiando non solo la conformità, ma anche la creazione di un quadro di resilienza operativa solido e adattivo.

Comprensione e conformità ai regolamenti DORA

- [ ] **Definizione della giurisdizione del DORA:** stabilisci se l'organizzazione rientra nell'ambito della giurisdizione del DORA e individuane i requisiti specifici.
- [ ] **Sviluppo di una strategia di resilienza:** formula una strategia di resilienza operativa digitale allineata ai regolamenti DORA.
- [ ] **Analisi regolare dei requisiti:** resta aggiornato sui requisiti DORA, assicurandone la continua comprensione e conformità.

Valutazione e gestione del rischio

- [ ] **Potenziamento della sicurezza delle informazioni:** potenzia le misure di sicurezza delle informazioni, tra cui controlli degli accessi, crittografia, codifica sicura e protezione dei dati.
- [ ] **Esecuzione della valutazione dei rischi:** valuta i rischi potenziali e le vulnerabilità dei sistemi TIC, affrontando le minacce interne ed esterne.
- [ ] **Gestione del rischio di terze parti:** valuta la resilienza e la sicurezza dei fornitori di terze parti assicurandoti che siano in linea con i requisiti DORA.
- [ ] **Identificazione e protezione degli asset TIC:** implementa misure di identificazione e protezione degli asset TIC in conformità alle normative DORA.
- [ ] **Utilizzo di soluzioni automatizzate:** implementa soluzioni automatizzate e il rilevamento delle minacce per un'efficiente identificazione dei rischi.
- [ ] **Priorità alle procedure correttive:** concentrati sulle procedure correttive e predisponi le prove di conformità.
- [ ] **Monitoraggio dei rischi esterni:** monitora le fonti esterne per i rischi potenziali e condivide le informazioni per rafforzare la resilienza.
- [ ] **Creazione di un quadro di gestione del rischio TIC:** stabilisci un quadro di gestione del rischio TIC ed esegui test di resilienza operativa digitale.

Cultura e leadership

- [ ] **Promozione di una cultura aziendale positiva:** crea una cultura aziendale positiva che incoraggi la collaborazione e la resilienza.
- [ ] **Priorità alla cultura della sicurezza:** coltiva una cultura aziendale incentrata sulla sicurezza attraverso la formazione e il coinvolgimento dei dipendenti.
- [ ] **Responsabilizzazione della leadership:** responsabilizza la leadership aziendale con una formazione adeguata a un'efficace conformità.
- [ ] **Approccio olistico alla conformità:** coinvolgi più team in modo collaborativo per un approccio olistico alla conformità.
- [ ] **Formazione e sensibilizzazione dei dipendenti:** offri programmi di formazione esaustivi per istruire i dipendenti sulle migliori pratiche di sicurezza informatica e sulla segnalazione degli incidenti.

Processo e automazione

- [ ] **Implementazione dell'integrazione continua/distribuzione continua e test automatizzati:** esegui l'integrazione continua, la distribuzione continua (CD) e i test automatizzati per ottimizzare i processi.
- [ ] **Piano di risposta agli incidenti:** sviluppa un piano dettagliato di risposta agli incidenti per rilevare, rispondere e risolvere gli incidenti di sicurezza.
- [ ] **Documentazione e registri:** tieni una documentazione dettagliata delle valutazioni del rischio, dei piani di risposta agli incidenti e delle misure di conformità.
- [ ] **Test di penetrazione:** esegui regolarmente test di penetrazione, utilizzando framework come TIBER-EU.
- [ ] **Automatizzazione del rilevamento delle minacce:** automatizza il rilevamento delle minacce utilizzando strumenti come EDR, XDR, scanner e SIEM.

Architettura, progettazione e gestione di terze parti

- [ ] **Progettazione per la scalabilità e la resilienza:** progetta sistemi per la scalabilità, la resilienza e la manutenibilità.
- [ ] **Architettura a microservizi:** implementa l'architettura a microservizi e la containerizzazione per operazioni efficienti.
- [ ] **Considerazioni sui fornitori di terze parti:** esamina le politiche sulle terze parti TIC e prendi in considerazione le normative quando ricorri a fornitori di servizi di terze parti.
- [ ] **Impiego di programmi di formazione:** utilizza strumenti come il programma di formazione di CybeReady per consentire agli sviluppatori di sviluppare applicazioni sicure.

Monitoraggio, misurazione e miglioramento continuo

- [ ] **Definizione di KPI e monitoraggio in tempo reale:** definisci indicatori di prestazione chiave (KPI) e implementa il monitoraggio in tempo reale.
- [ ] **Analisi regolare delle strategie di resilienza:** rivedi e aggiorna regolarmente le strategie e le politiche di resilienza.

- [ ] **Analisi degli incidenti passati:** analizza gli incidenti passati, implementa quanto appreso e apporta i dovuti miglioramenti.
- [ ] **Monitoraggio e valutazione continui:** implementa processi di monitoraggio continuo per rilevare e rispondere tempestivamente ai rischi e alle vulnerabilità emergenti.
- [ ] **Audit e valutazioni interne:** conduci regolarmente audit e valutazioni interne per identificare le aree di miglioramento e affrontare le criticità relative alla conformità.

Sicurezza e conformità giuridica

- [ ] **Integrazione dele pratiche di sicurezza:** integra le pratiche di sicurezza nel ciclo di vita dello sviluppo con un approccio DevSecOps.
- [ ] **Esecuzione di audit di sicurezza:** esegui regolarmente audit di sicurezza e valutazioni di vulnerabilità, garantendo la privacy dei dati.
- [ ] **Implementazione dell'ISMS:** definisci un sistema di gestione per la sicurezza delle informazioni (ISMS) allineato agli standard internazionali come l'ISO 27001.
- [ ] **Conformità agli standard giuridici:** garantisci la conformità agli standard giuridici, normativi e di settore, compreso il GDPR.
- [ ] **Cooperazione con le autorità di regolamentazione:** tieniti informato sugli aggiornamenti normativi e avvia un dialogo aperto con le autorità competenti per comprendere la conformità.

Come Hadrian può aiutare

Continuamente

Il Continuous Automated Red Teaming (CART) di Hadrian simula attacchi costanti e automatizzati sul tuo sistema per identificare vulnerabilità e debolezze. Essendo un processo continuo, possiamo rilevare nuove minacce e vulnerabilità man mano che emergono.

Autonomi

La piattaforma di sicurezza di Hadrian, alimentata da un'intelligenza avanzata, valuta l'intera superficie d'attacco, scoprendo le vulnerabilità dei terzi. Analizza la probabilità e l'impatto dello sfruttamento in tutta l'organizzazione, offrendo raccomandazioni di rimedio e garantendo una sicurezza continua dopo la correzione.

Completo

I rapporti di conformità tradizionali mancano di aggiornamenti in tempo reale, lasciando le aziende all'oscuro dei problemi finché non è troppo tardi. Hadrian offre rapporti chiari e precisi per le parti esterne, conformi alla legge DORA. Facili da condividere, tengono tutti informati sulla conformità alla legge DORA.

Leggi la guida per prepararti alla regolamentazione sulla resilienza operativa digitale

Scarica la guida Oppure scansiona il codice QR