2cents on Security
Pillole di Cyber Sicurezza

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

#9 DORA PARTE 2
IL DIGITAL OPERATIONAL RESILIENCE ACT

Il regolamento DORA stabilisce requisiti tecnici per entità finanziarie e provider ICT in 4 aree principali:

GESTIONE DEL RISCHIO ICT E GOVERNANCE:

le entità devono sviluppare strategie di gestione del rischio ICT e mantenere un framework completo per la gestione dei rischi.

Ciò include:

- **La mappatura dei sistemi ICT.**
- **L'identificazione di funzioni e asset critici.**
- **La valutazione continua dei rischi.**

RISPOSTA AGLI INCIDENTI E REPORTISTICA:

le entità devono stabilire sistemi per monitorare e segnalare incidenti ICT. Per incidenti critici, sono richiesti rapporti iniziali, intermedi e finali.

TEST DI RESILIENZA OPERATIVA DIGITALE:

le entità devono testare regolarmente i propri sistemi ICT per valutarne la robustezza e identificare le vulnerabilità. Ogni anno, è richiesta l'esecuzione di test di base e le entità finanziarie ritenute critiche per il sistema dovranno sottoporsi ogni tre anni a penetration test basati su minacce (TLPT).

GESTIONE DEL RISCHIO DI TERZE PARTI:

le entità finanziarie devono gestire attivamente il rischio associato ai fornitori ICT. Devono negoziare accordi specifici con i fornitori e assicurarsi che questi soddisfino i requisiti DORA. I fornitori critici saranno sottoposti alla supervisione diretta delle autorità europee.