CONFINDUSTRIA
VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

INNOVATION ROADMAP

Webinar tematici: INTELLIGENZA ARTIFICIALE

CYBERSECURITY PER L' AI E LA FABBRICA CONNESSA

ForGetInCompliance

Risposte razionali a contesti complessi

Fabio Trevisanato – Consulente Henko

16 Giugno 2026

FABIO TREVISANATO

Valutatore Privacy e Auditor ISDP 10003

Membro Osservatorio679 Data specialist

Auditor at Inveo Certification

CONFINDUSTRIA
VENETO EST

“Trust” Framework

insieme strutturato di **principi, regole, ruoli e tecnologie** che consente a più attori di operare in un ecosistema condiviso con **fiducia reciproca**

è un elemento trasversale e fondamentale in tutti i sistemi che trattano dati, sicurezza e responsabilità condivise.

Protezione dei dati personali: si costruisce attraverso trasparenza, accountability e sicurezza. Gli utenti devono poter confidare che i loro dati siano trattati **in modo lecito, corretto e sicuro.**

Cybersecurity: nasce dalla consapevolezza che le minacce possono provenire anche dall’interno e che la sicurezza deve essere continua, adattiva e contestuale . **La fiducia, quindi, è dinamica e basata su prove, non su presunzioni**.

Supply Chain (catena di fornitura): ogni fornitore può rappresentare un punto di vulnerabilità. La fiducia si costruisce **su trasparenza, tracciabilità e responsabilità condivisa lungo tutta la catena**.

In ambienti complessi (es. cloud, outsourcing, joint venture), la fiducia tra i diversi data owner, controller e processor si basa su:

- Contratti chiari (es. DPA – Data Processing Agreement)
- Ruoli e responsabilità ben definiti
- Meccanismi di audit e monitoraggio
- Condivisione delle metriche di rischio e sicurezza

Accountability

Il principio di responsabilizzazione

un individuo o un'organizzazione si assuma la responsabilità delle proprie azioni e decisioni, e sia disposto a rispondere delle proprie prestazioni e risultati.

Governance: Un'amministrazione pubblica è "accountable" se è in grado di spiegare le proprie decisioni e di rispondere alle domande dei cittadini.

Aziende: Un'azienda è "accountable" se è in grado di dimostrare di aver gestito in modo responsabile le risorse dei propri azionisti e di aver rispettato le leggi ambientali.

Privacy: Il GDPR (Regolamento Generale sulla Protezione dei Dati) richiede ai titolari del trattamento dei dati di essere "accountable", ovvero di adottare misure per garantire la protezione dei dati personali e di poter dimostrare di averlo fatto.

Il principio di rendicontazione

la capacità di fornire informazioni chiare e dettagliate sulle attività svolte, sui risultati ottenuti e sulle risorse utilizzate.

Rendicontazione: Questo aspetto dell'accountability riguarda la capacità di fornire informazioni chiare e dettagliate sulle attività svolte, sui risultati ottenuti e sulle risorse utilizzate.

Trasparenza: L'accountability richiede che le azioni e le decisioni siano prese in modo trasparente, in modo che possano essere verificate e comprese da altri.

Conformità: L'accountability implica anche il rispetto delle leggi, dei regolamenti e degli standard applicabili.

By Design:

si riferisce a qualcosa che è stato pianificato e realizzato intenzionalmente, non per caso o per errore, inclusa nel progetto o nel processo fin dall'inizio.
sottolinea l'intenzionalità e la pianificazione dietro una specifica caratteristica o risultato.

dei dati personali

la tutela della privacy fin dalla fase di progettazione di sistemi e processi, come richiesto dall'art. 25 del GDPR, garantendo minimizzazione, trasparenza e sicurezza dei dati

Dei perimetri di sicurezza digitale

implica costruire sistemi con misure di protezione intrinseche, prevenendo vulnerabilità già in fase di sviluppo, anziché correggerle a posteriori.

dei Processi organizzativi

strutturare workflow e procedure tenendo conto fin dall'inizio di requisiti normativi, di qualità e di rischio, per garantire conformità e resilienza operativa.

By Default:

una condizione o un'impostazione che viene applicata automaticamente, senza che l'utente debba intervenire o specificarla in modo esplicito. .

dei dati personali
per impostazione predefinita, siano trattati solo i dati strettamente necessari, limitando accessi, visibilità e durata del trattamento

Dei perimetri di sicurezza digitale
i sistemi devono essere configurati con **impostazioni di sicurezza massime già attive**, riducendo la superficie di attacco senza richiedere modifiche manuali da parte dell'utente

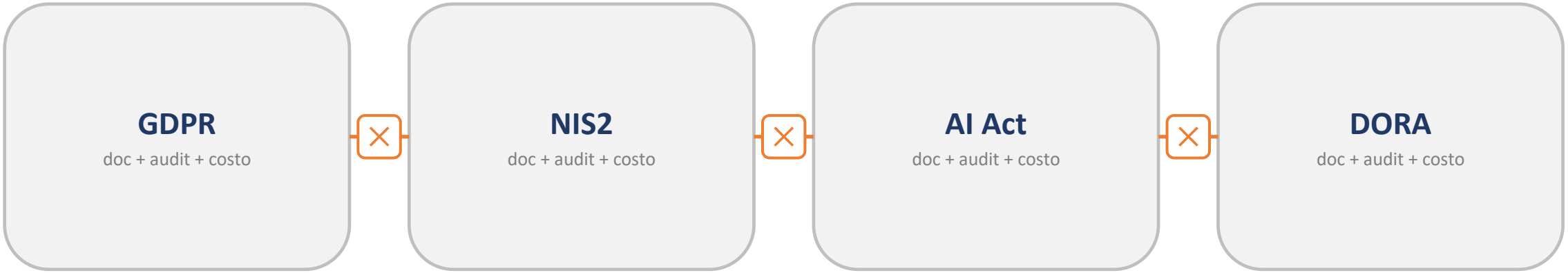
dei Processi organizzativi
strutturare workflow e procedure tenendo conto fin dall'inizio di requisiti normativi, di qualità e di rischio, per garantire conformità e resilienza operativa. le **procedure operative standard** siano progettate per garantire conformità, sicurezza e qualità,

La fabbrica connessa: ogni nodo è opportunità — e obbligo

Ogni nodo aggiunge efficienza — e, insieme, una superficie di rischio e un obbligo normativo.

CONFINDUSTRIA VENETO EST

Il problema: la compliance a compartimenti stagni



Costi ×3
spesa duplicata

Sforzi ripetuti
stesso lavoro più volte

Nessuna visione unica
governo assente

Conformi sulla carta, esposti nella realtà.

CONFINDUSTRIA VENETO EST

LA TRAPPOLA DEI COMPARTIMENTI STAGNI

Il Problema

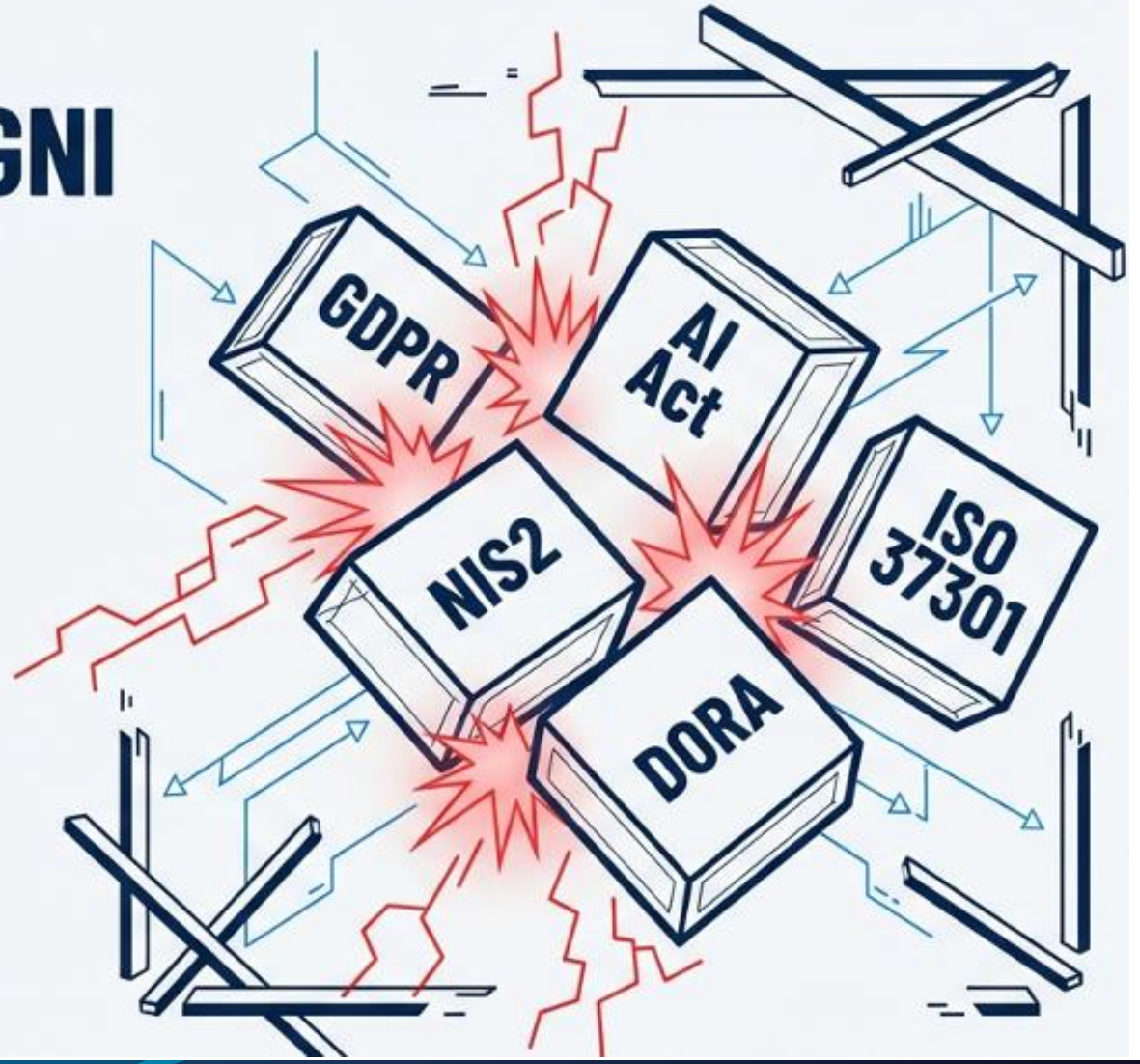
Le aziende sono prigioniere di una gestione normativa frammentata.

La Conseguenza

Inefficienza operativa, duplicazione dei costi e paralisi decisionale.

Il Rischio

Una gestione separata delle catene valoriali non è solo costosa, è un rischio operativo strutturale.



CONFINDUSTRIA VENETO EST

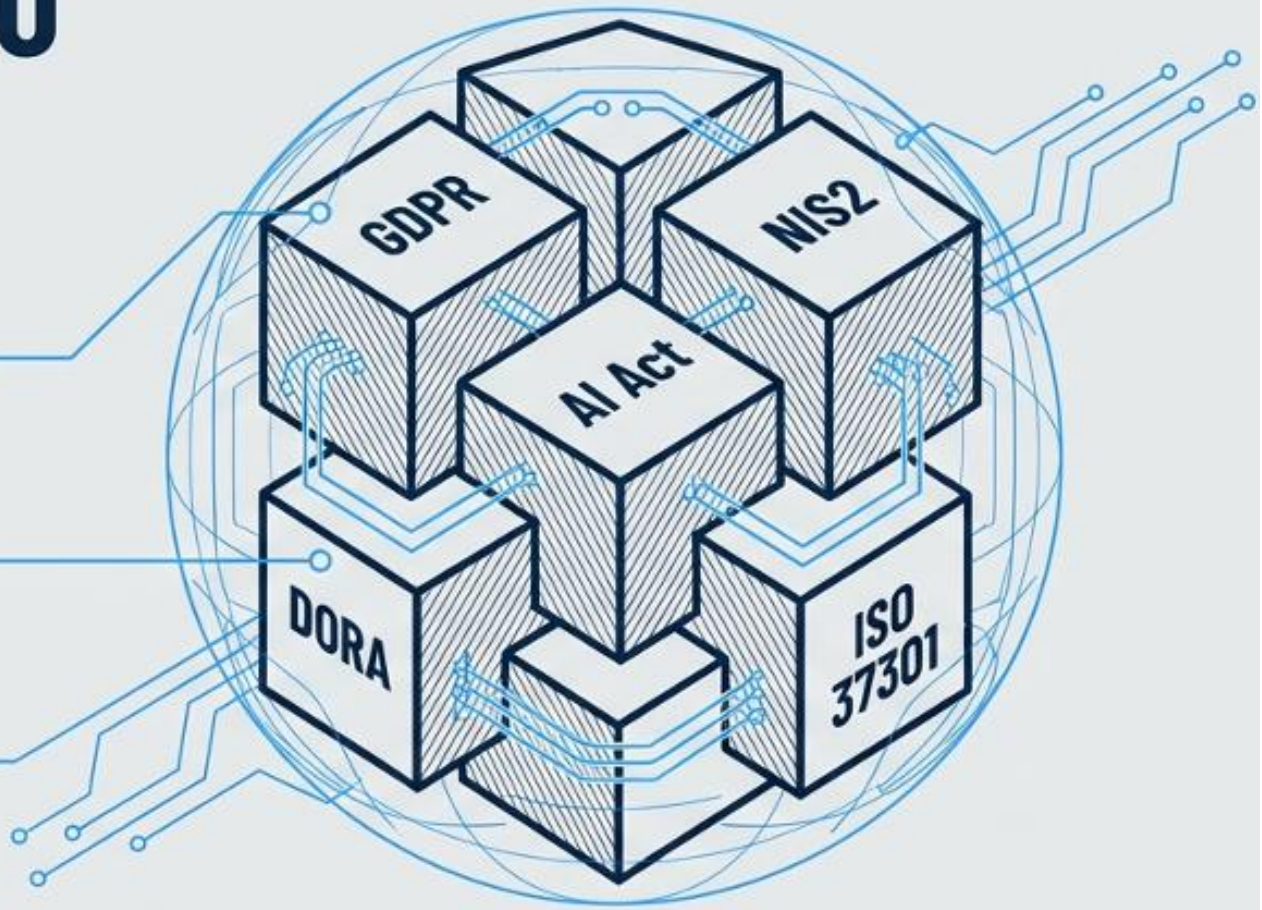
COMPLIANCE COME SISTEMA INTEGRATO

Non semplice consulenza, ma architettura tecnica e procedurale.

Integrazione Nativa: Unico framework operativo per requisiti giuridici e tecnici.

Efficienza: Un controllo di sicurezza alimenta privacy e resilienza.

Risultato: Riduzione drastica dell'effort e zero duplicazioni.



CONFINDUSTRIA VENETO EST

Non serve più compliance.
Serve gestirla meglio.

Dall'obbligo → alla sua governance.

CONFINDUSTRIA
VENETO EST

PONTI TRA DIRITTO E TECNOLOGIA

(Data-Driven Compliance)

3ª LINEA (AUDIT)

2ª LINEA (GOVERNANCE)

1ª LINEA (BUSINESS & OPERATION)

- **Unicità**: Far dialogare il mondo legale con i sistemi digitali.
- **Metodo**: Sistemi vivi alimentati dai tool aziendali, non faldoni di carta.
- **Output:** Indicatori di rischio ponderati e uniformi.

CONFINDUSTRIA VENETO EST

Il metodo — Legal Engineering: un controllo, più norme

Non faldoni di carta: l'architettura della compliance integrata ai sistemi di sicurezza.

1 CONTROLLO → Integrato

- **Conformità privacy** (GDPR)
- **Sicurezza** (NIS2)
- **Resilienza operativa** (DORA)
- **Governance dell'AI** (AI Act)

CONFINDUSTRIA VENETO EST

Misure di sicurezza obbligatorie

Per il dettaglio sulle misure da adottare si veda l'Annex del Regolamento di Esecuzione della NIS2 (2690 del 17/10/24)

Art. 24

Gestione dei Rishi

politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete

Gestione Incidenti

gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26;

Continuità Operativa

continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi

Supply Chain

sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi

Security by Design

sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità

Valutazione efficacia

politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica

Cyber Hygiene

pratiche di igiene di base e di formazione in materia di sicurezza informatica;

Crittografia

politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura

Sicurezza Risorse Umane

sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti

Controllo Accessi

autenticazione a più fattori o di autenticazione continua, comunicazioni protette, sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno

Un sistema vivo, alimentato dai dati — e dall'AI

Dalla fotografia annuale dell'audit al presidio continuo del rischio.

i vostri strumenti alimentano il sistema in tempo reale

AI

presidio continuo
+ misurabile

governata su tutto il ciclo (AI Act)

CONFINDUSTRIA VENETO EST

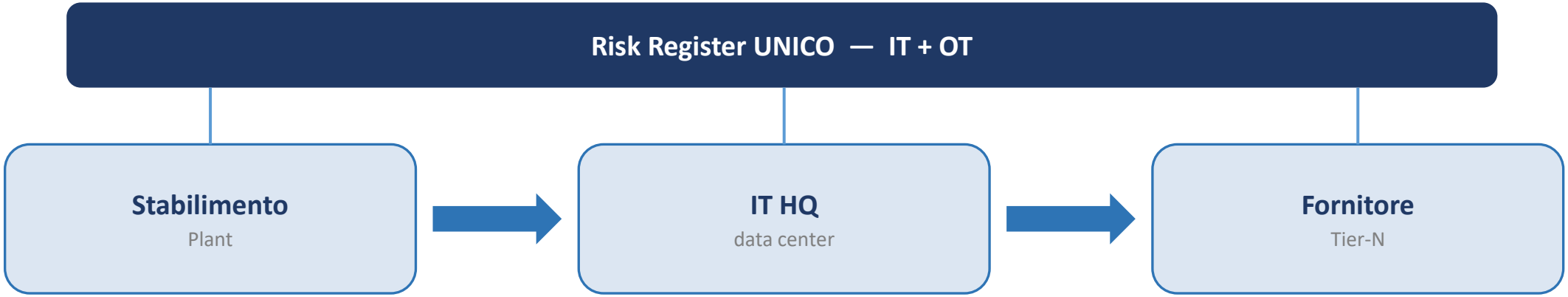
Asset Classification Policy 1/3

tipologia di asset

Tipologia di asset	Descrizione operativa	Rischi principali (esempi)	Controlli minimi richiesti (art. 21 NIS2 + requisiti tecnici Reg. 2024/2690)	Riferimenti normativi
SaaS (Software as a Service)	Applicazioni erogate via cloud (es. CRM, ERP, email, collaboration), gestite dal fornitore su infrastruttura propria o di terzi	Compromissione identità/tenant, perdita disponibilità dati, vulnerabilità app, supply chain del provider	Politiche di sicurezza e analisi del rischio; IAM/MFA e zero trust; patch/vuln management; logging e monitoraggio; BC/DR con RTO/RPO; contratti con clausole di sicurezza e prove di conformità (es. certificazioni)	NIS2 art. 21 (misure di gestione rischio) e art. 23 (notifica); Reg. 2024/2690 allegato (requisiti tecnici); campo soggettivo per fornitori di servizi di cloud computing
PaaS (Platform as a Service)	Piattaforme di sviluppo/esecuzione (runtime, DB gestiti, integrazione)	Compromissione servizi di piattaforma (DB, runtime), escalation privilegi, dipendenze librerie	Segmentazione environ, hardening runtime/DB, gestione segreti, CI/CD sicuro, test statici/dinamici, monitoraggio eventi/quasi incidenti	NIS2 art. 21-23; Reg. 2024/2690 (cloud computing)
IaaS (Infrastructure as a Service)	Compute, storage, hypervisor, virtual networking gestiti dal provider	Hypervisor escape, failure storage, misconfigurazioni rete, DDoS	Politiche di rete sicura (firewall, segmentazione, VPN, accesso fornitori “time-bound”); gestione patch; vulnerability scanning, pen test; monitoraggio traffico anomalo/DDoS	NIS2 art. 21-23; Reg. 2024/2690 (cloud computing, soluzioni di sicurezza di rete, gestione patch, test sicurezza)
Networking (WAN/LAN, SD-WAN, edge)	Trasporto e instradamento, segmentazione, accesso remoto	BGP hijack, misconfig ACL, insider, accessi non autorizzati	Firewall, segmentazione, gestione accessi, VPN; best practice per instradamento e igiene dell’instradamento; monitoraggio traffico	NIS2 art. 21 (politiche/igiene); Reg. 2024/2690 (sicurezza di rete, migliori pratiche instradamento)
DNS (servizi, registri TLD)	Risoluzione nomi, gestione zone TLD e registrar	DNS hijacking, cache poisoning, DoS contro autoritativi	DNSSEC, hardening, monitoraggio e rilevazione pattern anomali, piani BC/DR	Reg. 2024/2690 (DNS, best practice DNS), NIS2 art. 21-23
CDN (Content Delivery Network)	Distribuzione contenuti, caching edge	Poisoning cache, compromissione POP, DDoS	Hardening POP, monitoraggio performance/anomalie, protezioni DDoS, controllo accessi	Reg. 2024/2690 (CDN), NIS2 art. 21-23
Data center (colocation/hosting)	Facility e infrastrutture fisiche/energia/rete	Failure alimentazione, incendi, accessi fisici, guasti rete	Controlli fisici, alimentazione e raffreddamento ridondati; BC/DR, piani di ripristino; monitoraggio allarmi; gestione fornitori	Reg. 2024/2690 (data center), NIS2 art. 21 (continuità operativa)
Servizi gestiti (MSP) & Sicurezza gestita (MSSP)	Gestione IT e sicurezza per conto dei clienti	Supply chain (abuso accessi MSP), compromissione strumenti RMM, incidenti multi-cliente	Separazione funzioni/ruoli, controllo accessi privilegiati, registrazione/monitoraggio, test sicurezza periodici; contratti con clausole di sicurezza	Reg. 2024/2690 (servizi gestiti e di sicurezza gestiti), NIS2 art. 21-23
Mercati online, motori di ricerca, piattaforme social	Servizi digitali di piattaforma	DDoS, abuso account, contenuti malevoli, supply chain	IAM forte, MFA, anti-abuso, monitoraggio eventi/quasi incidenti, piani risposta	Reg. 2024/2690 (piattaforme digitali), NIS2 art. 21-23
PC/client				

CONFINDUSTRIA VENETO EST

In pratica: la filiera produttiva (IT / OT)



Prima

Livelli diversi tra stabilimenti · audit ripetuti · fornitori uno-a-uno · dubbi sull'incident readiness

Con l'integrazione

Registro unico IT/OT · audit combinati · qualifica fornitori multi-norma · risposta già pronta

CONFINDUSTRIA VENETO EST

Asset Classification Policy 2/3

attributi di rilevanza

Gli asset sono identificati in ragione della loro funzione nei processi considerati ereditandone gli attributi di criticità identificati con la seguente tassonomia:

Livello di criticità	Definizione
Non critico	Sistemi e asset che non rientrano nei settori sopra indicati o che, per dimensione e impatto, non sono considerati rilevanti ai fini della NIS2.
Critico	Sistemi che supportano servizi importanti ma non essenziali, il cui malfunzionamento può avere impatti significativi su settori specifici.
Altamente Critico	Sistemi e asset che supportano servizi essenziali per il funzionamento della società e dell'economia, il cui malfunzionamento può causare gravi impatti sistemici.

Gli effetti della compromissione degli asset sono classificati (alto, medio o basso) come dalla seguente tabella:

area d'applicabilità	Altamente critico	critico	Non critico
Economico e reputazionale	ha conseguenze in grado di incidere significativamente sul risultato economico dell'azienda, assorbibili in più esercizi	ha conseguenze rilevanti sul risultato economico dell'azienda, comunque assorbibili nell'esercizio di riferimento;	ha conseguenze non rilevanti sul risultato economico dell'azienda
reputazionale	se il mercato percepisce l'indisponibilità dei prodotti/servizi erogati dal sotto processo con conseguenze sulla fidelizzazione della clientela e sull'avviamento che si manifestano per un periodo maggiore dell'esercizio di riferimento; se risulta compromessa l'immagine societaria e l'affidabilità dell'organizzazione può essere messa in discussione anche dal personale, dai collaboratori, dalla filiera di approvvigionamento e/o dai mercati; se gli effetti dell'interruzione possano generare esposizioni mediatiche;	se il mercato percepisce l'indisponibilità dei prodotti/servizi erogati dal sotto ma, attraverso opportuni presidi (comunicazione, presidi organizzativi, altro) viene mantenuta la fidelizzazione della clientela senza conseguenze sull'avviamento, o comunque contenute nell'esercizio di riferimento;	se l'indisponibilità dei prodotti/servizi erogati dal sotto processo non viene percepita dal mercato (portatori di interessi, terzi, non percepiscono l'indisponibilità dei prodotti/servizi erogati dal processo)
NIS2	interruzioni che generano una riduzione della capacità di produzione o un impatto economico superiore a 500.000,00 € o al 5% del fatturato se più basso.	interruzioni che non hanno effetti significativi ed il periodo di ripristino sia coerente con le misure previste e pianificate	interruzioni che siano trascurabili in termini di impatto economico, di continuità operativa e/o di tenuta della società.
GDPR	interruzioni che comportano per gli interessati conseguenze significative, materiali, immateriali, reputazionali, sulla salute, economici o in termini di limitazione dei propri diritti	interruzioni che comportano per gli interessati conseguenze significative, materiali, immateriali, reputazionali, sulla salute, economici o in termini di limitazione dei propri diritti che tuttavia sono in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, etc.).	interruzioni che comportano per gli interessati conseguenze non significative, materiali, immateriali, reputazionali, sulla salute, economici o in termini di limitazione dei propri diritti che tuttavia non comportano particolari oneri o impatti (tempo trascorso a reinserire informazioni, fastidi, etc.).
compliance	interruzioni che comportano il rischio di una non conformità particolarmente significativa (es. contratti, terze parti, oneri ulteriori) con possibilità di sospensione dell'attività specifica	interruzioni che comportano violazioni non particolarmente significative ma che tuttavia possano prevedere sanzioni amministrative/penali contrattuali;	interruzioni che non comportano nessun tipo di sanzione/non conformità

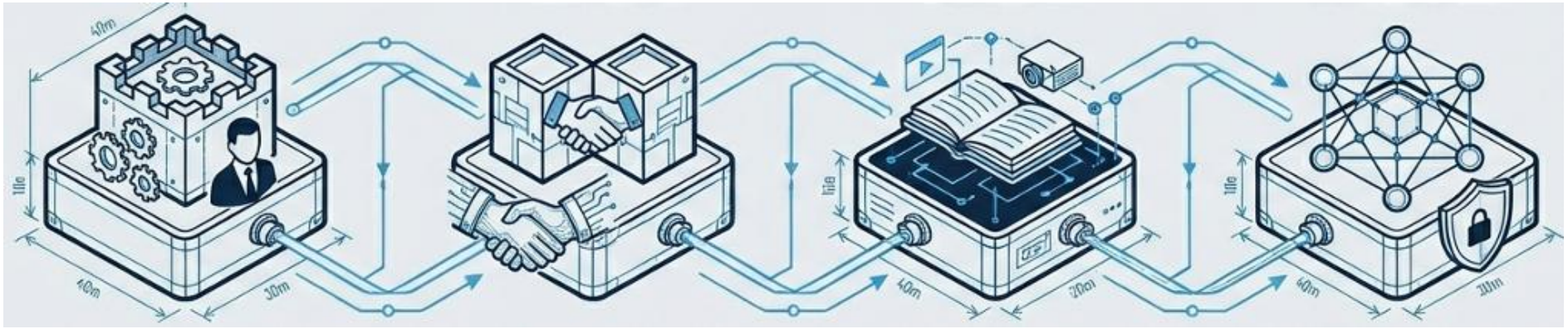
TPRM& Classification Policy 1/4

attributi di rilevanza

gli attributi relativi ai servizi erogati sono preventivamente identificati assegnando un primo “indicatore di criticità” definito in ALTO, MEDIO, BASSO in base ai criteri di cui alla seguente tabella che riporta le prime indicazione circa le attività da predisporre in re della loro criticità:agion

Indicatore di Criticità del Fornitore ICT	Livello di Criticità NIS2/DORA	Descrizione	Criteri principali	Implicazioni operative
Alto	Altamente critico	Servizi che supportano funzioni essenziali o infrastrutture critiche (es. DNS, cloud, data center, MSSP, TLD, CDN)	- Fornitori MSSP, CDN, DNS, Cloud, Data Center - Impatto diretto su disponibilità, integrità, riservatezza - Coinvolti nella gestione incidenti, sicurezza, rete, dati	- Obbligo di registrazione e monitoraggio continuo - Clausole contrattuali specifiche - DPA e audit periodici (GDPR relevant) - Rilevanza per compliance NIS2 e DORA
Medio	Critico	Servizi che supportano operazioni ICT rilevanti per la continuità operativa, ma non direttamente critici	- Fornitori ICT, MSP, PaaS - Supporto a sviluppo, analisi, gestione operativa - Trattamento di dati personali o tecnici	- Valutazione contrattuale e tecnica - Monitoraggio SLA/KPI - Rilevanza per GDPR, ISMS, DORA
Basso	Non critico	Servizi con impatto limitato sulla resilienza complessiva, spesso locali o non essenziali	- Fornitori non ICT - Accesso a dati personali, tecnici, riservati - Funzioni di supporto o indirette	- Valutazione tecnica e contrattuale - Monitoraggio SLA e KPI - Verifica accessi e protezione dati
Variabile	Variabile	Servizi non ICT o indiretti, ma potenzialmente rilevanti se trattano dati personali, tecnici o riservati	- Fornitori non ICT - Accesso a dati personali, tecnici, riservati - Funzioni di supporto o indirette	- Applicare criteri di classificazione dati - Valutare accessi e impatti indiretti

Il risultato: meno costi, più valore, più controllo



Efficienza

Audit combinati e fine delle duplicazioni: oneri di controllo giù.

Controllo

Una sola vista sulla catena del valore, non tre report scollegati.

Reattività

Pronti a un'ispezione o a un incidente: il sistema risponde subito.

Valore

Da centro di costo a sistema di governo che protegge brand e continuità.

La compliance da centro di costo a sistema di governo.

CONFINDUSTRIA VENETO EST

Per informazioni:
ricercainnovazione@confindustriavenest.it

Grazie per l’attenzione.