



CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

Dalla compliance alla strategia

CRA, AI Act, NIS2 e Regolamento Macchine letti insieme per passare dall'obbligo normativo alla visione di crescita.

Ing. Georgia Cesarone
CTO

Centro di Competenza START4.0



CHI SIAMO

START 4.0 è uno degli otto Centri di Competenza nazionali ad alta specializzazione costituiti nell'ambito del Piano Industria 4.0. È un'Associazione pubblico-privata che riunisce imprese, università, enti di ricerca e istituzioni con una specializzazione nella sicurezza e nell'ottimizzazione delle infrastrutture strategiche e nella cybersecurity.

La missione di START 4.0 è accompagnare la trasformazione digitale sicura e sostenibile delle imprese italiane con particolare attenzione alle PMI, facilitando l'accesso a competenze, tecnologie, servizi specialistici ed opportunità di finanziamento.

START 4.0 opera all'interno di una rete europea e internazionale creando connessioni tra competenze, tecnologie e opportunità. Dall'assessment alla formazione, dalla sperimentazione "test before invest" ai progetti di innovazione, START 4.0 accompagna le organizzazioni nel trasformare le nuove tecnologie in soluzioni concrete, sicure e sostenibili.

Dalla necessità di compliance ai vantaggi della strategia

Il quadro normativo europeo sta modificando profondamente il modo in cui le organizzazioni devono governare cybersecurity, prodotti digitali, intelligenza artificiale, macchine, dati e supply chain.

Normative differenti intervengono sempre più spesso sugli stessi prodotti, sugli stessi processi e sulle stesse tecnologie.

La sfida non è quindi semplicemente essere conformi alle normative, ma costruire una governance capace di comprendere l'intero framework normativo e recepirlo in modo integrato.



L'approccio tradizionale alla compliance tende a partire dalla singola norma: si individuano gli obblighi, si assegnano alle funzioni competenti e si costruisce un piano di adeguamento.

Questo modello diventa insufficiente quando normative diverse insistono sugli stessi asset, prodotti, sistemi, dati, fornitori e processi aziendali.

Una macchina può essere contemporaneamente un prodotto con elementi digitali, utilizzare AI, essere collegata alla rete di un soggetto NIS2 e presentare rischi cyber capaci di produrre conseguenze sulla safety.

Non possiamo governare una realtà integrata attraverso compliance separate.

Il passaggio dalla compliance alla strategia consiste proprio nel costruire un modello di governo unitario, capace di mantenere distinte le specificità normative, ma di integrare ciò che può essere gestito attraverso processi comuni.

NIS2: il rischio cyber diventa un tema di Governance

La Direttiva NIS2 sposta definitivamente la cybersecurity dalla dimensione esclusivamente tecnica alla gestione del rischio aziendale.

I soggetti essenziali e importanti devono adottare misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza delle reti e dei sistemi informativi e per prevenire o minimizzare l'impatto degli incidenti.

Ma l'elemento forse più significativo è la governance: l'art. 20 richiede agli organi di gestione di approvare le misure di gestione del rischio cyber e sovrintendere alla loro attuazione.

La cybersecurity entra quindi nelle responsabilità del management e coinvolge organizzazione, processi, persone, fornitori e continuità operativa.

NIS2 sposta il rischio cyber dall'IT al sistema di governo dell'organizzazione.



DECRETO LEGISLATIVO 138/2024 (NIS2)

La nuova disciplina italiana per la cybersicurezza Cosa cambia per le PMI

Il Decreto Legislativo 138/2024 recepisce la Direttiva UE 2022/2555 (NIS2) e **rafforza** il livello comune di cybersicurezza nell'Unione Europea.

L'obiettivo: aumentare la **resilienza** delle organizzazioni e la capacità di prevenire, rilevare e rispondere agli incidenti informatici.



I PILASTRI DELLA NIS2



GESTIONE DEL RISCHIO

Adozione di misure tecniche, operative e organizzative adeguate e proporzionate al rischio.



OBBLIGO DI NOTIFICA

Notifica degli incidenti significativi alle autorità competenti entro tempi definiti.



RESPONSABILITÀ DEGLI ORGANI DI VERTICE

Il management è responsabile per l'approvazione e la vigilanza sulle misure di cybersicurezza.



SUPERVISIONE E CONTROLLI

Le autorità competenti possono effettuare verifiche, ispezioni e richiedere informazioni.



SANZIONI

Sanzioni amministrative significative in caso di inadempimento degli obblighi.



COOPERAZIONE

Maggiore collaborazione tra Stati, CSIRT, autorità e condivisione delle informazioni.

PERCHÉ NIS2?



Minacce in aumento

Gli attacchi informatici sono più frequenti, sofisticati e impattano su servizi essenziali e supply chain.



Impatto sistemico

Un incidente presso una singola organizzazione può avere effetti a catena su clienti, fornitori e sull'intero sistema economico.



Armonizzazione europea

NIS2 introduce requisiti e responsabilità comuni in tutti gli Stati membri per un livello di sicurezza più elevato e omogeneo.



Maggiore accountability

Più obblighi, più controlli e responsabilità dirette per gli organi di vertice.

GLI OBBLIGHI PRINCIPALI

- Analisi e gestione dei rischi informatici.
- Adozione di misure di sicurezza appropriate e proporzionate (tecniche, operative e organizzative).
- Politiche di sicurezza e procedure interne.
- Formazione e sensibilizzazione del personale.
- Gestione degli incidenti: rilevazione, risposta, ripristino.
- Business continuity e disaster recovery.
- Gestione della sicurezza nella supply chain (fornitori e terze parti).
- Valutazione dell'efficacia delle misure adottate.
- Conservazione dei log e registrazioni.

A CHI SI APPLICA?

NIS2 amplia la platea dei soggetti interessati.

SOGGETTI ESSENZIALI

Enti e imprese che erogano servizi essenziali per il mantenimento di attività sociali o economiche vitali.

Esempi di settori:

- Energia
- Trasporti
- Banche
- Infrastrutture dei mercati finanziari
- Sanità
- Acqua potabile
- Infrastrutture digitali
- Pubblica Amministrazione
- Spazio

SOGGETTI IMPORTANTI

Altri settori ad alto impatto economico e sociale.

Esempi di settori:

- Servizi postali e di corriere
- Gestione dei rifiuti
- Produzione, trasformazione e distribuzione alimentare
- Chimica
- Manifatturiero
- Fornitori di servizi digitali (es. cloud, data center, DNS)
- Ricerca

 Le PMI possono rientrare nella disciplina in base al settore di appartenenza e al ruolo nella catena del valore.

NOTIFICA DEGLI INCIDENTI

In caso di incidente significativo:



 Le autorità possono richiedere aggiornamenti e informazioni aggiuntive durante tutto il ciclo di gestione dell'incidente.



SANZIONI

Sanzioni amministrative pecuniarie fino a:

SOGGETTI ESSENZIALI
10 MILIONI €
o fino al 2% del fatturato mondiale totale annuo.

SOGGETTI IMPORTANTI
7 MILIONI €
o fino all'1,4% del fatturato mondiale totale annuo.

 Le sanzioni si applicano anche in caso di mancata o tardiva notifica degli incidenti.

RESPONSABILITÀ DEGLI ORGANI DI VERTICE

Gli organi di amministrazione e direzione devono:

- approvare le misure di gestione dei rischi di cybersicurezza;
- vigilare sulla loro attuazione;
- essere informati regolarmente sul livello di rischio;
- possono essere ritenuti responsabili in caso di inadempimento.

COME PUÒ UNA PMI ADEGUARSI?



Valuta i rischi informatici per la tua organizzazione.



Definisci misure di sicurezza proporzionate al contesto.



Forma e sensibilizza il personale in modo continuo.



Definisci procedure di incident response e business continuity.



Coinvolgi i fornitori e la supply chain.



Monitora, verifica e migliora costantemente.

Cyber Resilience Act: la cybersecurity diventa una caratteristica del prodotto

Il Cyber Resilience Act introduce requisiti orizzontali di cybersecurity per i prodotti con elementi digitali, intervenendo sull'intero ciclo di vita del prodotto.

Il fabbricante deve effettuare una valutazione dei rischi di cybersecurity associati al prodotto e tenerne conto durante pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione.

La cybersecurity non viene quindi verificata soltanto prima dell'immissione sul mercato, ma entra nel modo in cui il prodotto viene progettato, sviluppato, aggiornato e mantenuto.

Il CRA introduce inoltre requisiti relativi a gestione delle vulnerabilità, aggiornamenti di sicurezza, componenti di terze parti, documentazione, conformity assessment e reporting.

La cybersecurity non protegge soltanto l'impresa e deve essere incorporata nel prodotto.

CHE COS'È

Il Cyber Resilience Act (CRA) introduce requisiti di cybersecurity obbligatori per i prodotti con elementi digitali, lungo tutto il loro ciclo di vita, dalla progettazione alla dismissione.

OBIETTIVI

- Prodotti con un livello di sicurezza adeguato e verificabile
- Riduzione delle vulnerabilità diffuse nel mercato
- Maggiore trasparenza e gestione efficace degli aggiornamenti

PERCHÉ È IMPORTANTE

- Riduce i rischi per utenti, imprese e infrastrutture
- Aumenta la fiducia nei prodotti digitali
- Rafforza la competitività delle imprese europee in un mercato globale



QUALI PRODOTTI SONO COINVOLTI?

Prodotti con elementi digitali, ad esempio:

- IoT e dispositivi connessi
- Software e app
- Dispositivi embedded
- Prodotti industriali e macchine con componenti digitali
- Soluzioni cloud e servizi digitali

CHI È COINVOLTO?

- FABBRICANTI**
Responsabili della conformità del prodotto e della gestione della cybersecurity lungo tutto il ciclo di vita
- IMPORTATORI**
Devono immettere sul mercato solo prodotti conformi
- DISTRIBUTORI**
Devono verificare la presenza dei requisiti e collaborare in caso di azioni correttive

PRINCIPALI ESCLUSIONI

- Aerospazio
- Difesa
- Automotive (già regolato)
- Dispositivi medici (già regolato)
- Apparecchiature elettroniche di comunicazione (già regolato)

PRINCIPALI OBBLIGHI

1 VALUTAZIONE DEL RISCHIO  Effettuare e documentare la valutazione dei rischi di cybersecurity del prodotto.	2 REQUISITI DI CYBERSECURITY  Progettare e sviluppare prodotti che soddisfino i requisiti essenziali di cybersecurity.	3 GESTIONE DELLE VULNERABILITÀ  Processi per identificazione, correzione e divulgazione delle vulnerabilità.	4 AGGIORNAMENTI DI SICUREZZA  Fornire aggiornamenti per il periodo di supporto dichiarato.	5 DOCUMENTAZIONE E CONFORMITÀ  Redigere documentazione tecnica, garantire la valutazione della conformità e la marcatura CE.	6 REPORTING  Notificare vulnerabilità attivamente sfruttate e incidenti gravi secondo tempi e modalità previste.
--	--	---	--	--	--

BENEFICI PER LE IMPRESE

- Prodotti più sicuri e affidabili
- Maggiore fiducia da parte di clienti e partner
- Accesso facilitato ai mercati e vantaggio competitivo

AI Act: governare l'AI lungo tutto il suo ciclo di vita

L'AI Act è il primo quadro normativo europeo organico dedicato all'intelligenza artificiale e introduce un **modello di regolamentazione basato sul rischio**. L'obiettivo è garantire che i sistemi di AI sviluppati e utilizzati nell'Unione europea siano sicuri, trasparenti e affidabili e rispettino salute, sicurezza e diritti fondamentali.

Il Regolamento distingue obblighi e responsabilità in funzione del livello di rischio del sistema, del suo utilizzo e del ruolo assunto dall'organizzazione nella catena del valore dell'AI. Alcune pratiche sono vietate, mentre per i sistemi classificati ad alto rischio sono previsti requisiti più stringenti lungo l'intero ciclo di vita.

Per questi sistemi diventano centrali la gestione continua del rischio, la qualità e la governance dei dati, la documentazione e la tracciabilità, la trasparenza, la supervisione umana, l'accuratezza, la robustezza e la cybersecurity, insieme al monitoraggio successivo all'immissione sul mercato.

L'AI Act introduce inoltre il principio dell'AI literacy, richiedendo alle organizzazioni di sviluppare competenze adeguate nelle persone che utilizzano o gestiscono sistemi di intelligenza artificiale.

L'AI Act porta quindi l'intelligenza artificiale da semplice tecnologia da adottare a sistema da governare lungo tutto il suo ciclo di vita.



OBIETTIVO

Garantire che i sistemi di intelligenza artificiale sviluppati e utilizzati nell'Unione europea siano sicuri, trasparenti e affidabili, nel rispetto di salute, sicurezza e diritti fondamentali.



CHI È COINVOLTO?

Obblighi e responsabilità in funzione del ruolo nella catena del valore:



Provider

sviluppa il sistema AI



Deployer

utilizza il sistema AI



Importatori

immettono sul mercato



Distributori

mettono a disposizione

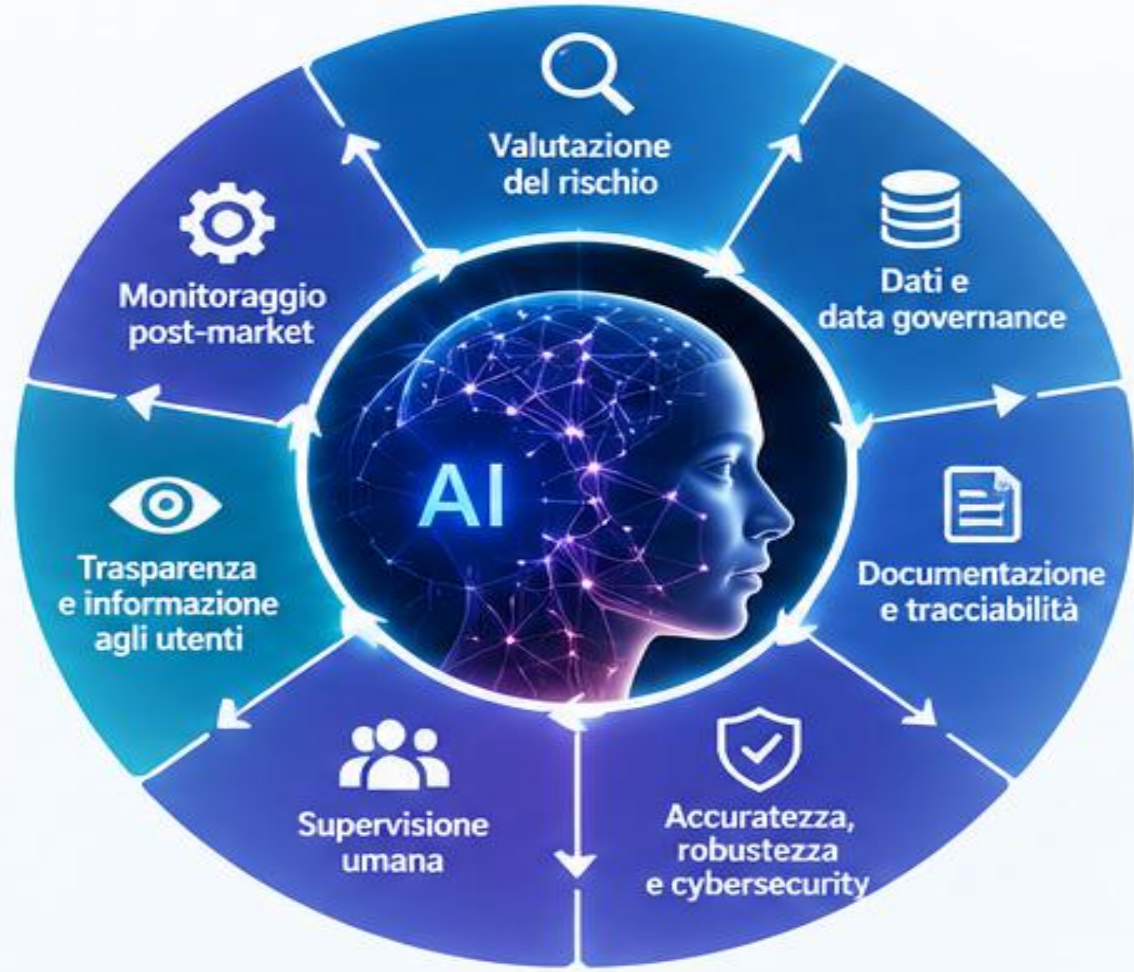
UN APPROCCIO BASATO SUL RISCHIO

Obblighi e regole proporzionati al livello di rischio del sistema AI.



REQUISITI LUNGO TUTTO IL CICLO DI VITA

Per i sistemi ad alto rischio e, dove applicabile, per altre categorie.



PRINCIPALI OBBLIGHI (sistemi ad alto rischio e, dove applicabile)



AI LITERACY

Provider e deployer devono adottare misure per garantire un livello sufficiente di competenza nelle persone che operano con sistemi AI per loro conto, tenendo conto di ruolo, contesto d'uso e livello di rischio del sistema.

PERCHÉ È IMPORTANTE



Maggiore sicurezza
per persone e società



Tutela dei diritti
fondamentali



Maggiore fiducia
da parte di cittadini, clienti e partner



Innovazione responsabile
e sostenibile



Accesso a nuovi mercati
e maggiore competitività



Ecosistema AI europeo
più affidabile e resiliente

Regolamento Macchine: safety, software e cybersecurity convergono

Il Regolamento (UE) 2023/1230 aggiorna il quadro europeo della sicurezza delle macchine in un contesto in cui le macchine sono sempre più connesse e capaci di incorporare sistemi digitali e AI.

La valutazione del rischio rimane centrale per determinare i requisiti essenziali di sicurezza e tutela della salute applicabili, ma il regolamento considera ormai anche le interferenze tra mondo fisico e digitale.

I sistemi di comando devono poter resistere, quando pertinente rispetto alle circostanze e ai rischi, anche a tentativi malevoli ragionevolmente prevedibili di terzi che possano generare situazioni pericolose.

Tra le categorie previste figurano inoltre componenti di sicurezza con comportamento integralmente o parzialmente autoevolutivo basato su machine learning.

Quando il digitale può modificare il comportamento fisico della macchina, cybersecurity e safety devono dialogare.



Regolamento Macchine

Macchine più sicure per un'industria più competitiva

Regolamento (UE) 2023/1230

Nuovi requisiti per la sicurezza delle macchine nella nuova era digitale.



OBIETTIVO

Garantire che le macchine e i prodotti correlati siano sicuri per le persone, proteggano la salute e riducano i rischi, tenendo conto delle nuove tecnologie e dei rischi cyber.



CHI È COINVOLTO?



Fabbricanti

progettano e immettono sul mercato



Importatori

verificano la conformità



Distributori

controllano i requisiti e la documentazione



Utilizzatori

garantiscono uso sicuro e manutenzione adeguata



A CHI SI APPLICA?

Macchine, prodotti correlati e componenti di sicurezza, nuovi e parti di modifiche sostanziali, immessi sul mercato o messi in servizio nell'UE.



PRINCIPALI NOVITÀ



Maggiore attenzione a rischi digitali e cybersecurity

Requisiti specifici per macchine con componenti software, connessioni e funzionalità digitali.



Inclusione di tecnologie emergenti

Considera AI, machine learning e sistemi adattivi.



Maggiore integrazione con altre normative

Coerenza con il nuovo quadro legislativo europeo (es. AI Act, CRA, NIS2).



Approccio al ciclo di vita

Dalla progettazione alla dismissione, con attenzione a manutenzione, aggiornamenti e modifica sostanziale.



Requisiti più chiari su documentazione e tracciabilità

Istruzioni, valutazione dei rischi, fascicolo tecnico e dichiarazione di conformità.



Maggiore focus su usabilità e fattori umani

Interfacce, segnalazioni, prevenzione di errori e interazione sicura.



IL CICLO DI VITA E GLI OBBLIGHI PRINCIPALI

1. PROGETTAZIONE



Valutazione dei rischi e requisiti di sicurezza (inclusi rischi digitali).

2. SVILUPPO



Integrazione delle misure tecniche e di protezione.

3. VERIFICA DI CONFORMITÀ



Test, validazione e fascicolo tecnico.

4. IMMISSIONE SUL MERCATO



Dichiarazione di conformità e marcatura CE.

5. USO E MANUTENZIONE



Utilizzo sicuro, aggiornamenti e manutenzione.

6. MODIFICHE SOSTANZIALI



Nuova valutazione dei rischi e, se necessario, nuova conformità.

7. DISMISSIONE



Gestione sicura a fine vita.



I BENEFICI



Ambienti di lavoro più sicuri



Maggiore affidabilità e continuità operativa



Innovazione responsabile e competitività



Maggiore accesso ai mercati europei



Macchine più sostenibili lungo il ciclo di vita



E' fondamentale non iniziare il percorso di compliance costruendo quattro liste di requisiti, quattro gap analysis, quattro gruppi di lavoro e quattro roadmap, ma è necessario partire dalla domanda:

Chi e come governa tutto questo?

La governance deve stabilire chi decide, chi assume il rischio, chi implementa le misure, chi controlla, quali informazioni arrivano al management e come vengono gestite le interdipendenze tra i diversi domini normativi.

Il punto di partenza non è quindi il singolo adempimento, ma costruire il sistema attraverso cui gli adempimenti verranno governati.

Cosa significa Governance?

La governance è il sistema attraverso cui un'organizzazione definisce chi decide, con quali responsabilità, regole e informazioni, e come vengono gestiti e monitorati i rischi.

Trasforma requisiti normativi e obiettivi strategici in decisioni, processi, ruoli e azioni coordinate.

- ☐ chi assume le decisioni?
- ☐ sulla base di quali informazioni?
- ☐ con quali responsabilità?
- ☐ secondo quali regole?
- ☐ con quali risorse?
- ☐ attraverso quali meccanismi di controllo?
- ☐ con quali processi di escalation e riesame?

Significa assicurare che Cybersecurity, AI, Product Security, Safety, Data e Supply Chain possano mantenere competenze specialistiche ma operare all'interno di un modello decisionale coerente.

La Governance è un ciclo, non un progetto



IL PRIMO COMPITO DELLA GOVERNANCE: IL RISCHIO

Le quattro normative hanno finalità e perimetri differenti, ma condividono un'impostazione fondamentale:
le misure vengono determinate a partire dal rischio.

Questo significa che l'impresa non dovrebbe mai iniziare chiedendosi: “Quali controlli devo implementare?”

La domanda da porsi è:

“Quali rischi devo governare e quali misure risultano necessarie e proporzionate rispetto a quei rischi?”

Il risk assessment diventa quindi uno strumento decisionale della governance, non un documento prodotto esclusivamente per dimostrare la compliance.



L'articolo 21 della NIS2 richiede misure:

“tecniche, operative e organizzative adeguate e proporzionate” per gestire i rischi alla sicurezza dei sistemi informativi e di rete.

Nel valutare la proporzionalità devono essere considerati, tra gli altri elementi, grado di esposizione al rischio, dimensione del soggetto, probabilità degli incidenti e loro gravità, compreso l'impatto sociale ed economico.

Quindi:



**Non esiste una cybersecurity efficace semplicemente perché esiste una checklist di controlli.
Le misure devono essere coerenti con il rischio che devono governare.**

CRA: il risk assessment entra nel prodotto

Il CRA richiede al fabbricante di effettuare una valutazione dei rischi di cybersecurity associati al prodotto con elementi digitali.

Il risultato deve essere utilizzato durante:



La valutazione considera almeno finalità prevista, uso ragionevolmente prevedibile, condizioni d'uso, ambiente operativo, asset da proteggere e durata prevista di utilizzo.

Deve inoltre indicare se e come determinati requisiti di cybersecurity siano applicabili al prodotto e come implementarli sulla base del rischio.

Il risk assessment CRA contribuisce quindi a guidare la progettazione e l'implementazione della sicurezza.

AI Act: il rischio è un processo continuo

Per i sistemi AI ad alto rischio, il sistema di gestione dei rischi deve essere un processo continuo e iterativo durante l'intero ciclo di vita.

Deve consentire di:

- ✓ identificare e analizzare i rischi noti e ragionevolmente prevedibili per salute, sicurezza e diritti fondamentali;
- ✓ stimare e valutare i rischi derivanti dall'uso previsto e dall'uso improprio ragionevolmente prevedibile;
- ✓ considerare ulteriori rischi emergenti dal post-market monitoring;
- ✓ adottare misure appropriate e mirate di gestione del rischio.

Non basta valutare il sistema AI prima di utilizzarlo: bisogna continuare a governarne il rischio.

Regolamento Macchine: il rischio determina le misure di sicurezza

La valutazione del rischio nel Regolamento Macchine serve a determinare i requisiti essenziali di sicurezza e tutela della salute applicabili.

Il processo porta a:

- ☐ determinare i limiti della macchina;
- ☐ identificare i pericoli;
- ☐ stimare i rischi;
- ☐ valutarne l'accettabilità;
- ☐ eliminare i pericoli o ridurre i rischi attraverso misure di protezione.



La documentazione tecnica deve comprendere un'analisi e una valutazione adeguate dei rischi.
Ancora una volta: il rischio non è un allegato alla progettazione ma contribuisce a determinarla.

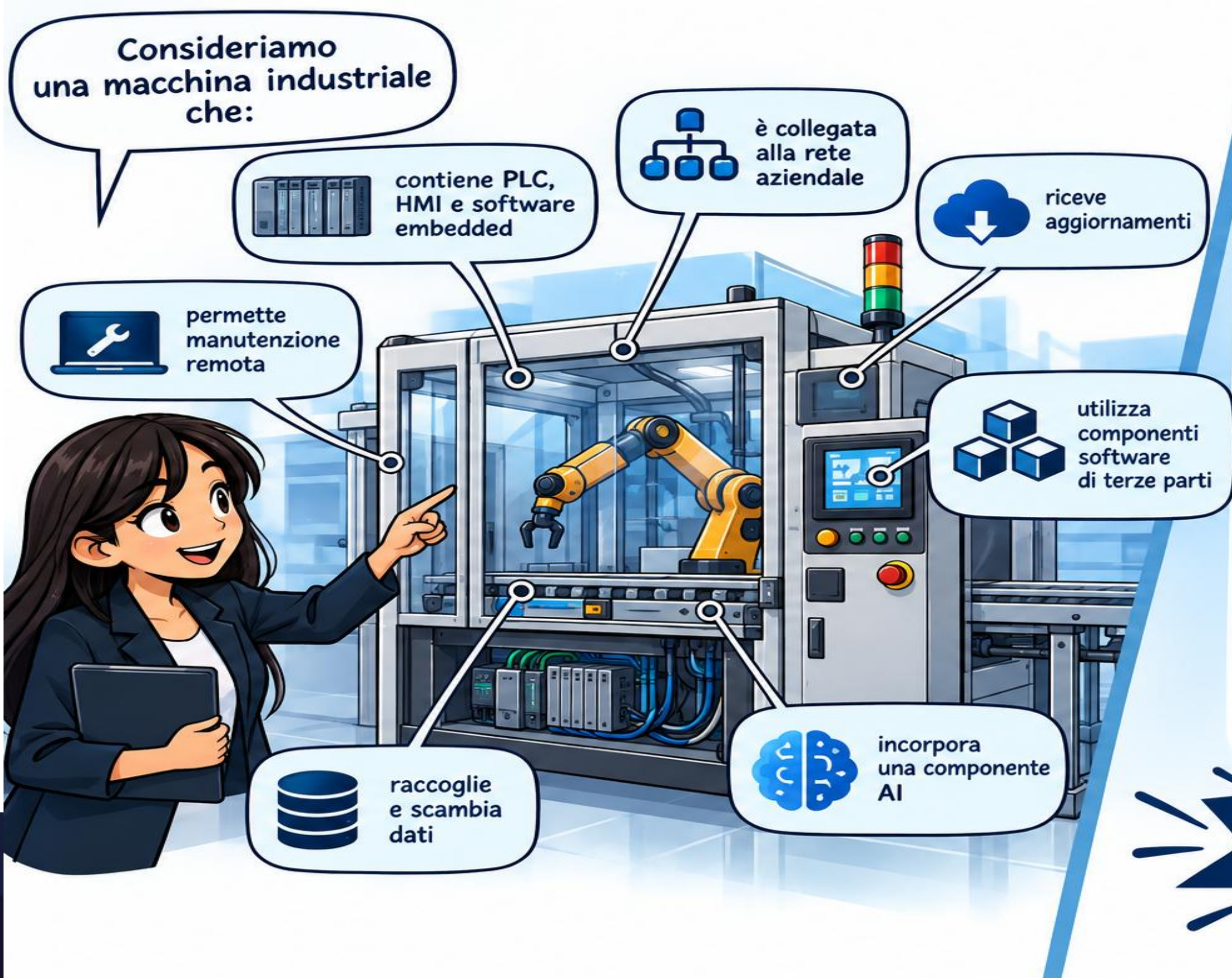
Non esiste “un solo rischio”

Integrare la governance non significa confondere le diverse valutazioni.

- NIS2 guarda ai rischi relativi alla sicurezza di reti e sistemi e all'impatto degli incidenti sui servizi.
- Il CRA guarda ai rischi di cybersecurity del prodotto con elementi digitali.
- L'AI Act, nei sistemi ad alto rischio, considera rischi per salute, sicurezza e diritti fondamentali.
- Il Regolamento Machine considera pericoli e rischi per salute e sicurezza.

Le analisi restano differenti, ma devono poter dialogare perché lo stesso asset, componente, software o evento potrebbe attraversare più domini di rischio.

Un esempio: la macchina connessa



Quella macchina non appartiene più soltanto al dominio della **safety**.



È contemporaneamente macchina...



...prodotto digitale...



...endpoint connesso...



...elemento della rete aziendale...



...contenitore di software...



...e potenzialmente sistema che incorpora AI.

La realtà tecnologica ha già superato **i silos normativi.**

Ora immaginate che ci sia una vulnerabilità nel software della macchina...



Questa vulnerabilità potrebbe:

compromettere la cybersecurity del prodotto



CRA

essere utilizzata come punto di accesso alla rete aziendale



**possibile
rilevanza NIS2**

alterare il comportamento della macchina generando una situazione pericolosa



**Regolamento
Macchine**

interferire con una componente AI o con i suoi dati



**possibile
rilevanza AI Act**

Questo non significa che tutte le normative si applichino automaticamente.

Significa che...



**LO STESSO EVENTO TECNICO
PUÒ DOVER ESSERE LETTO ATTRAVERSO
PIÙ PROSPETTIVE DI RISCHIO.**



La realtà tecnologica ha già superato i silos normativi:

**una stessa vulnerabilità
può coinvolgere più ambiti,
più rischi e più normative.**



Anche le norme prevedono l'integrazione

L'integrazione non è soltanto una scelta organizzativa.

L'AI Act prevede, per prodotti soggetti anche alla legislazione europea di armonizzazione pertinente, la possibilità di integrare processi di testing, reporting, informazioni e documentazione AI nei processi già esistenti, proprio per garantire coerenza, evitare duplicazioni e minimizzare gli oneri aggiuntivi.

Il Regolamento Macchine prevede inoltre, quando una macchina è soggetta a più atti UE che richiedono una dichiarazione di conformità, un'unica dichiarazione UE di conformità relativa agli atti interessati.

Il principio è chiaro: requisiti differenti possono essere governati attraverso processi coordinati.

Il Regolamento Macchine richiede che i sistemi di comando siano progettati per evitare situazioni pericolose e considera anche tentativi malevoli ragionevolmente prevedibili di terzi quando possono generare pericolo. Richiede inoltre evidenze relative a interventi legittimi o illegittimi sul software o alla sua modifica.

Il CRA, parallelamente, governa la cybersecurity del prodotto con elementi digitali.

Quindi, quando una compromissione digitale può determinare un comportamento fisico pericoloso, Security e Safety non possono più essere progettate separatamente.

Quando un sistema AI è incorporato in un prodotto soggetto anche alla legislazione europea di armonizzazione, il provider deve garantire che il prodotto soddisfi tutti i requisiti applicabili.

L'AI Act consente di integrare, dove appropriato, testing, reporting, informazioni e documentazione AI nei processi previsti dalla normativa di prodotto.

Questa è una indicazione molto importante per la governance:
non duplicare ciò che può essere integrato, ma mantenere chiaramente identificabili i requisiti specifici.

Il Risk Assessment deve produrre decisioni

Il risk assessment è il processo attraverso cui un'organizzazione identifica i rischi a cui è esposta, ne valuta probabilità e possibili impatti e determina quali richiedano un intervento prioritario. Non è quindi una semplice fotografia delle vulnerabilità, ma uno strumento decisionale che consente di stabilire quali rischi trattare, con quali misure, responsabilità e priorità, orientando in modo proporzionato investimenti e azioni di sicurezza.

Il risk assessment non termina con la consegna di un report perché la finalità è produrre governance!



Chi governa il rischio?

Una governance integrata deve individuare:

- ☐ chi è owner del rischio;
- ☐ chi può accettarlo o richiederne il trattamento;
- ☐ chi implementa le misure;
- ☐ chi verifica che funzionino;
- ☐ chi gestisce anomalie, vulnerabilità e incidenti;
- ☐ chi mantiene le evidenze;
- ☐ chi deve informare il management;
- ☐ chi decide in caso di escalation.

Cybersecurity, AI, Product Security e Safety attraversano ormai R&D, engineering, operations, procurement, HR, legal, IT, OT e management.

La Governance integrata non elimina le competenze specialistiche



La governance integrata stabilisce COME queste competenze collaborano quando il rischio attraversa più domini.
Il vero valore non è creato dalla centralizzazione, ma dal corretto coordinamento delle decisioni.

Subito: identificare le responsabilità esistenti e i responsabili dei principali rischi.

Subito: individuare aree non presidiate o responsabilità sovrapposte.

Nel breve periodo: formalizzare ruoli, deleghe, escalation e reporting.

Successivamente: integrare Cyber, AI, Product e Safety nei processi di sviluppo, acquisto, change management, incident management e gestione dei fornitori.

La parte semplice è disegnare l'organigramma.

La parte complessa è far funzionare realmente le interazioni.

Policy e Procedure: qual è la differenza?

La **policy** definisce principi, obiettivi, responsabilità e regole.
Dice COSA deve accadere e PERCHÉ.

La **procedura** traduce quella regola in attività operative.
Stabilisce CHI fa COSA, QUANDO, COME, con quali INPUT, quali OUTPUT e quali EVIDENZE.

Esempio:

Policy: “Le vulnerabilità devono essere gestite sulla base del rischio.”

Procedura: chi riceve la segnalazione, chi classifica la vulnerabilità, entro quanto deve essere trattata, chi approva la remediation e come viene verificata la chiusura.

Una policy senza procedure rischia di restare un principio.

Una procedura senza governance rischia di diventare pura burocrazia.

Non una policy per ogni normativa

La compliance per silos porterebbe facilmente a creare:

Policy e procedure per compliance NIS2;

Policy e procedure per compliance CRA;

Policy e procedure per compliance AI Act;

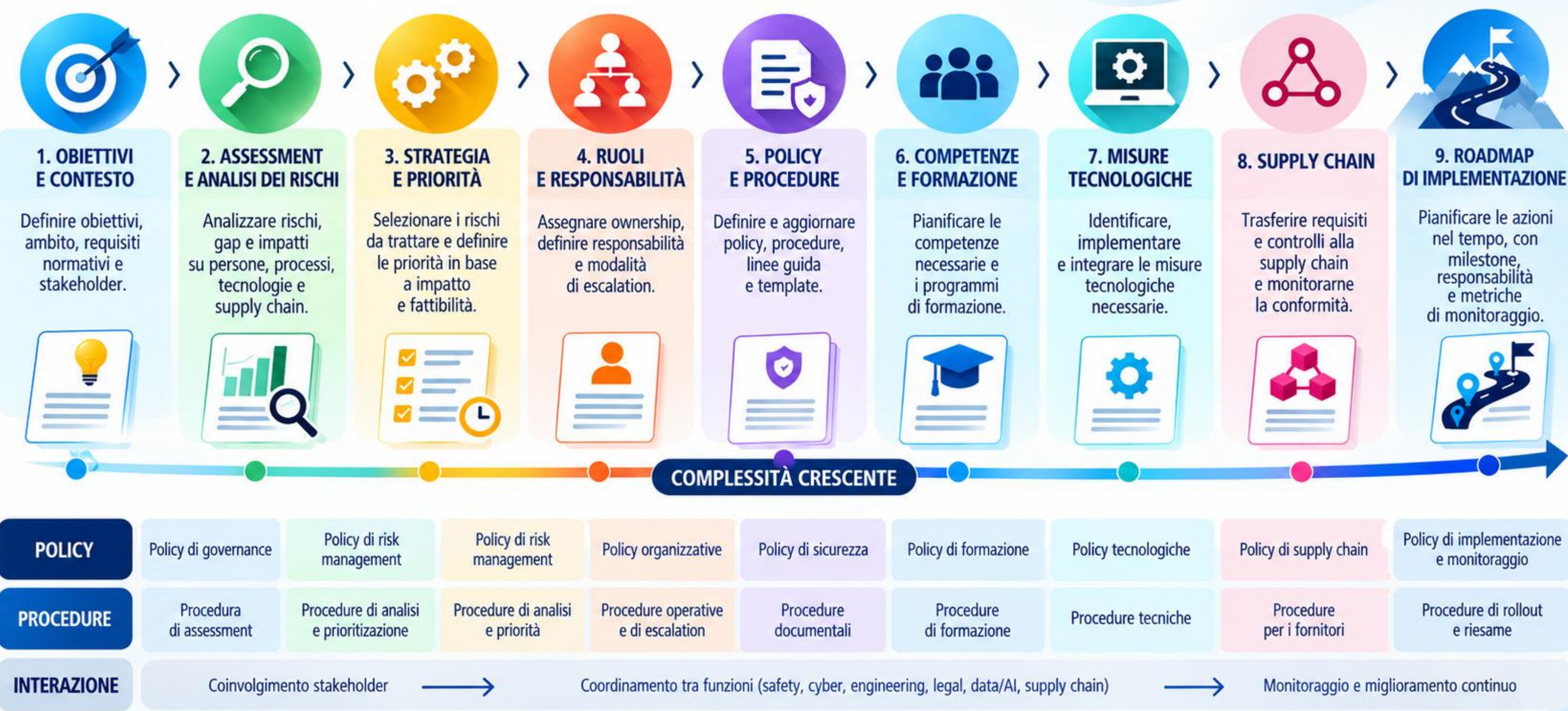
Policy e procedure per compliance Regolamento macchine.

Ma abbiamo visto che molti processi sono trasversali e correlati.

È quindi molto più efficace costruire policy aziendali su:

Risk Management; Cybersecurity; AI Governance; Product Security; Secure Development; Vulnerability Management; Incident Management; Supply Chain; Data Governance; Access Control; Business Continuity; Change Management; OT Security e, successivamente mappare ogni policy e procedura sui diversi requisiti normativi applicabili.

Roadmap Policy & Procedure e relativa complessità



NIS2 richiede formazione agli organi di gestione e incoraggia formazione periodica dei dipendenti affinché acquisiscano conoscenze e competenze per identificare i rischi e valutare le pratiche di gestione del rischio cyber.

L'AI Act richiede a provider e deployer misure per assicurare, per quanto possibile, un livello sufficiente di AI literacy, tenendo conto delle conoscenze tecniche, esperienza, istruzione, formazione e contesto d'uso delle persone coinvolte.

Formare non significa quindi erogare lo stesso corso a tutti. La formazione deve essere coerente con rischio, ruolo e responsabilità.



1. FORMAZIONE IN AMBITO CONSAPEVOLEZZA

Per tutti: cyber hygiene, phishing, incident reporting, uso responsabile dell'AI, gestione dei dati e comportamenti sicuri.

2. FORMAZIONE PER RUOLO

Board, procurement, HR, R&D, engineering, IT, OT, manutentori, utilizzatori AI devono comprendere i rischi e gli obblighi pertinenti alle proprie attività.

3. FORMAZIONE SPECIALISTICA

Secure Development, Product Security, AI Risk Management, OT Security, Vulnerability Management, Incident Response, Safety/Security Engineering.

Più aumenta la responsabilità, più la formazione deve diventare specifica.

- ✓ **Immediato:** formazione di Board e C-level sui rischi e sulle responsabilità.
- ✓ **Immediato:** awareness generale e AI literacy pertinente.
- ✓ **Breve periodo:** mappatura di ruoli e competenze necessarie.
- ✓ **Breve/medio periodo:** formazione role-based.
- ✓ **Medio periodo:** percorsi specialistici per le funzioni tecniche.
- ✓ **Continuativo:** aggiornamento e misurazione dell'efficacia.

Uno degli errori più comuni è trasformare la compliance in misure puramente tecnologiche e trasformarli in una lista di prodotti da acquistare.

Ma la sequenza corretta è:

RISCHIO → MISURA → CONTROLLO → TECNOLOGIA

Diventano misure efficaci soltanto se sappiamo quale rischio devono ridurre, quale processo supportano, chi li governa e come ne misuriamo l'efficacia.

**Non esiste una tecnologia “richiesta dalla compliance” in assoluto:
gli adeguamenti tecnologici devono derivare dai rischi individuati e dalle misure necessarie per trattarli.**

Quali adeguamenti tecnologici possono emergere?

Gestire meglio identità e accessi

Rafforzare l'autenticazione, controllare chi può accedere a sistemi e dati e proteggere in particolare gli account con privilegi elevati.

Conoscere sistemi, asset e vulnerabilità

Avere un inventario aggiornato di sistemi, dispositivi e software, individuare le vulnerabilità e gestire patch e aggiornamenti secondo il livello di rischio.

Proteggere e separare reti IT e ambienti OT

Segmentare le reti, limitare le comunicazioni non necessarie e rendere più sicuri gli accessi remoti, soprattutto quelli utilizzati da manutentori e fornitori.

Rilevare tempestivamente anomalie e incidenti

Raccogliere e analizzare log ed eventi di sicurezza per riconoscere comportamenti anomali, possibili attacchi e incidenti.

Quali adeguamenti tecnologici possono emergere?

Garantire continuità e capacità di ripristino

Proteggere dati e sistemi attraverso backup adeguati, verificare periodicamente il ripristino e predisporre soluzioni di continuità operativa e disaster recovery.

Integrare la sicurezza nello sviluppo di software e prodotti

Introdurre controlli di sicurezza durante progettazione, sviluppo, test, rilascio e aggiornamento, anziché intervenire soltanto sul prodotto finito.

Conoscere e governare i componenti software del prodotto

Tenere traccia di librerie, componenti di terze parti e open source, delle relative vulnerabilità e degli aggiornamenti necessari.

Proteggere sistemi, modelli e dati AI

Controllare accessi, dati, modelli e pipeline AI e monitorarne nel tempo sicurezza, integrità e comportamento.

Roadmap tecnologica: cosa viene prima?

Prima: interventi relativamente semplici che riducono rischi significativi come inventory, MFA, access review, verifica dei backup, protezione degli accessi remoti, dove pertinenti.

Poi: vulnerability e patch management, hardening, logging e controllo degli accessi di terze parti.

Successivamente: IAM/PAM strutturati, segmentazione, SIEM/SOC, OT monitoring.

Più strutturali: Secure Development Lifecycle, Product Security Lifecycle, SBOM governance, AI lifecycle security.

Ma la priorità non può essere identica per tutte le imprese e, come già sottolineato, deve derivare dal rischio effettivamente identificato.

Il rischio non finisce al confine dell'organizzazione

Oggi sistemi e prodotti dipendono da:



NIS2 include espressamente la supply-chain security nelle misure di gestione del rischio.

Il CRA richiede inoltre ai fabbricanti di governare anche il rischio derivante dall'integrazione di componenti di terze parti. Il procurement diventa quindi parte del sistema di sicurezza e governance.

Cosa significa governare la Supply Chain?

Governare la Supply Chain significa conoscere e valutare i rischi introdotti da fornitori, componenti, software, servizi e accessi di terze parti.

Significa anche saper trasferire nei contratti requisiti di sicurezza chiari definendo responsabilità, livelli di servizio, gestione delle vulnerabilità e degli incidenti, obblighi di notifica, aggiornamenti, diritto di verifica e condizioni di continuità e uscita dal rapporto.

Dal punto di vista operativo, significa sapere:

- quali fornitori sono critici;
- quali componenti entrano nei prodotti e nei sistemi;
- quali dati e sistemi possono essere raggiunti dal fornitore;
- quali requisiti di sicurezza devono essere rispettati;
- come vengono gestite vulnerabilità e aggiornamenti;
- cosa deve essere comunicato in caso di incidente;
- cosa accade se il fornitore non è più disponibile.

Il contratto traduce una parte delle decisioni di risk management in obblighi concreti verso il fornitore.

Subito: inventario dei fornitori e classificazione per criticità.

Breve periodo: assessment dei fornitori più critici e definizione di requisiti minimi.

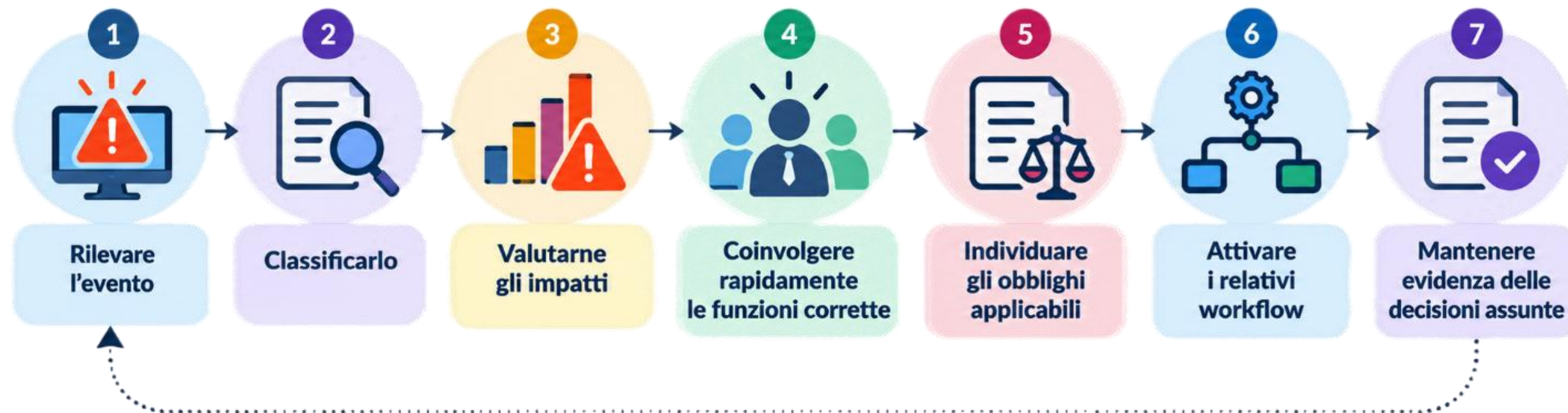
Successivamente: revisione di clausole contrattuali, accessi e obblighi di comunicazione.

Più complesso: governo delle dipendenze software, componenti e SBOM.

Livello maturo: monitoraggio continuativo, auditing ed integrazione dei fornitori nei processi di vulnerability management, incident management e business continuity.

Un unico processo di escalation, più trigger normativi

Anche a livello di notifica, integrare non significa trasformare tutti gli obblighi di notifica in uno solo, ma significa costruire un processo aziendale capace di:



Una gestione efficace degli incidenti richiede che siano chiari ruoli, responsabilità, livelli di escalation e poteri decisionali ben prima che si scateni una emergenza.

Essere conformi significa anche poterlo dimostrare

Una governance efficace deve produrre evidenze



Devono poter essere documentati, quando pertinenti:



**Risk
assessment**



**Decisioni
sul trattamento**



Responsabilità



Formazione



Test
(es. di sicurezza
e di continuità)



Controlli
(tecnici, organizzativi,
fisici)



Vulnerabilità
(identificazione
e gestione)



Incidenti
(gestione e
lesson learned)



Aggiornamenti
(patch, versioni,
fine supporto)



**Valutazioni
dei fornitori**
(selezione, monitoraggio,
rivalutazione)



Monitoraggio
(indicatori, audit,
conformità)



Riesami
(periodici e a
seguito di cambiamenti
significativi)

Inoltre, ad esempio:



Policy



Procedure



Asset inventory
(IT/OT/IoT)



Gestione
degli accessi



Gestione
delle configurazioni



Cambiamenti
(change management)



Dati e backup
(incluso ripristino)



Business continuity
e disaster recovery



Obblighi normativi
(es. notifiche)



Altri elementi
rilevanti

Documentare una volta, utilizzare molte volte

Quando possibile, l'impresa dovrebbe evitare di produrre più volte la stessa informazione soltanto perché richiesta da normative differenti.

Un unico:

- Inventario degli asset (IT, OT, IoT, prodotti, software, dati e sistemi AI)
- Registro dei fornitori
- Registro della formazione
- Registro degli incidenti
- Registro delle vulnerabilità
- Archivio delle evidenze documentali

può supportare più processi normativi, purché siano preservati i requisiti specifici applicabili.

UNA VOLTA IL PROCESSO.

UNA VOLTA L'EVIDENZA.

PIÙ MAPPATURE NORMATIVE, OVE POSSIBILE.



Implementare una misura non significa automaticamente aver ridotto il rischio.

Una governance efficace deve quindi monitorare nel tempo l'evoluzione dei rischi, verificare le vulnerabilità ancora aperte e l'eventuale ripetersi degli incidenti, individuare criticità nei fornitori e valutare se i controlli adottati siano realmente efficaci.

Deve inoltre intercettare eventuali carenze di competenze e mantenere sotto osservazione i cambiamenti che interessano sistemi, prodotti e tecnologie, compresa l'introduzione di nuovi sistemi di intelligenza artificiale.

Ricordatevi sempre che ciò che non viene monitorato difficilmente potrà essere governato.



Non KPI per fare reporting ma informazioni per decidere

Monitorare significa raccogliere dati sull'andamento dei rischi e sull'efficacia delle misure adottate. Ma avere molti dati non significa necessariamente avere informazioni utili.

Sapere, ad esempio, che l'azienda ha 150 vulnerabilità aperte dice relativamente poco. È molto più utile sapere che 5 vulnerabilità critiche riguardino sistemi essenziali, non siano ancora state risolte entro i tempi previsti e richiedano un intervento prioritario.

Il monitoraggio deve quindi trasformare i dati in informazioni che permettano alla governance di capire dove il rischio stia aumentando, quali misure non stiano funzionando e dove sia necessario intervenire.



Il reporting non deve quindi mostrare tutto quello che si possa misurare, ma ciò che occorra per decidere.

Da dove possiamo iniziare?

1. Costruire o verificare la governance.
Chi decide? Chi coordina? Chi governa il rischio?
2. Definire il perimetro.
Sistemi, prodotti, macchine, AI, dati e fornitori.
3. Verificare quali normative e quali obblighi siano applicabili.
4. Avviare le diverse analisi del rischio necessarie, coordinandole tra loro.
5. Identificare gap e rischi prioritari.
6. Attivare i quick win in grado di ridurre rapidamente i rischi significativi.
7. Costruire una roadmap integrata di adeguamento.



Dai 3 ai 12 mesi: trasformare la Governance in operatività

Nel periodo successivo occorre progressivamente:

- ✓ formalizzare ruoli e responsabilità;
- ✓ razionalizzare policy e procedure;
- ✓ sviluppare formazione role-based;
- ✓ rafforzare vulnerability e incident management;
- ✓ integrare supply-chain risk e procurement;
- ✓ implementare i controlli tecnologici prioritari;
- ✓ rafforzare secure development e product security;
- ✓ organizzare documentazione ed evidenze;
- ✓ definire KPI e KRI;
- ✓ avviare audit, testing e riesami.

I progetti più complessi devono essere pianificati presto proprio perché richiederanno più tempo.

Dalla Compliance alla Strategia: un breve quadro d'insieme

La Governance definisce come agiamo. Il rischio determina dove interveniamo.
Gli adempimenti trasformano le decisioni in organizzazione, processi, competenze e tecnologia.
Il monitoraggio dice se le misure messe in atto funzionano. Il riesame del rischio riavvia il ciclo.

Quindi:

Un unico sistema di Governance capace di gestire requisiti diversi e le loro interdipendenze.

E da qui partono gli approfondimenti:

CYBER RESILIENCE ACT

Governare la cybersecurity del prodotto lungo tutto il lifecycle.

REGOLAMENTO MACCHINE

Governare la convergenza tra safety e cybersecurity.

AI ACT

Governare rischi, responsabilità e ciclo di vita dell'intelligenza artificiale.

Quando la compliance diventa competitività

Da obbligo normativo a valore strategico per un'impresa più sicura, innovativa e resiliente.



Stesse normative.
Più valore per il tuo business.

1 Riduce costi e duplicazioni

Processi, assessment, policy, formazione, controlli ed evidenze condivisi evitano di replicare attività analoghe per ogni normativa e consentono di concentrare investimenti e risorse sui rischi realmente prioritari.



Meno burocrazia, più efficienza.

2 Aumenta resilienza e continuità

Gestire in modo integrato rischi, vulnerabilità, incidenti, dipendenze e supply chain significa ridurre la probabilità che un evento cyber, tecnologico o operativo interrompa il business o comprometta prodotti, servizi e reputazione.



Un business più stabile e continuo.

3 Migliora prodotti e processi

Security, safety e compliance integrate fin dalla progettazione favoriscono prodotti più robusti, aggiornabili e affidabili e processi più efficienti, riducendo il costo di correggere problemi quando il prodotto è già sul mercato.



Prodotti più sicuri, qualità più elevata, costi inferiori nel tempo.

4 Aumenta fiducia e accesso al mercato

Clienti, grandi imprese, pubbliche amministrazioni e filiere chiedono sempre più evidenze di sicurezza, resilienza e capacità di governo del rischio. Essere in grado di dimostrarle può facilitare l'ingresso nelle supply chain più strutturate e rafforzare la relazione con clienti e partner.



Più opportunità commerciali e partnership più solide.

5 Rende possibile innovare con più velocità e consapevolezza

Una governance matura non serve a bloccare l'AI, nuovi prodotti o nuove tecnologie: permette di sapere a quali condizioni possono essere adottati, riducendo incertezza, rischi e rilavorazioni.



Innovazione sicura e sostenibile.

6 Trasforma gli investimenti obbligatori in capacità permanenti

Competenze, processi, tecnologie e governance costruiti oggi per rispondere a CRA, AI Act, NIS2 e Regolamento Macchine rimangono patrimonio dell'organizzazione anche quando il quadro normativo evolve, rafforzando la capacità di adattarsi a nuove sfide.



Un'organizzazione più pronta al futuro.



COMPLIANCE
Obbligo normativo da rispettare



GOVERNANCE
Decisioni, ruoli, processi e controllo



RESILIENZA
Meno rischi, maggiore continuità



FIDUCIA
Clienti, partner, supply chain



INNOVAZIONE
Nuove tecnologie e nuovi mercati



COMPETITIVITÀ
Crescita sostenibile e valore nel tempo

La compliance è il punto di partenza. Il vero vantaggio competitivo nasce quando ciò che siamo obbligati a fare diventa il modo migliore con cui decidiamo, progettiamo, innoviamo e facciamo impresa.





CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

Dalla compliance alla strategia

CRA, AI Act, NIS2 e Regolamento Macchine letti insieme per passare dall'obbligo normativo alla visione di crescita.

Ing. Georgia Cesarone
CTO

Centro di Competenza START4.0