SECURITY SUMMIT

Security Summit

Verona 28 ottobre 2026

Clusit

ASTREA

Sessione

Se il rischio si vede, il budget arriva: come la normativa sta cambiando le priorità cyber

Alessandro Zerpelloni | Founder - Connect4 Consulting
Matteo Colella | Senior Security Advisor – Security Lab

Matteo Colella



Membro del Comitato Scientifico e
della commissione Premio Tesi del Clusit

Senior Security Advisor – Security Lab

Alessandro Zerpelloni

Founder Connect4 Consulting



Alessandro Zerpelloni opera da anni all’intersezione tra diritto, tecnologia e cybersecurity. Consulente in ambito privacy, sicurezza informatica e governance del rischio, supporta aziende e organizzazioni nel trasformare obblighi normativi e requisiti tecnici in modelli concreti di gestione del rischio digitale. Alla solida preparazione giuridica affianca competenze informatiche maturate fin dai primi studi e successivamente approfondite attraverso formazione specialistica e certificazioni in ambito cybersecurity. La sua attività si concentra sulla compliance normativa in materia di protezione dei dati, cybersecurity e intelligenza artificiale, accompagnando le organizzazioni nell’interpretazione dei requisiti e nella loro attuazione sul piano organizzativo, contrattuale e operativo.

Minacce e spesa crescono insieme

+49%

incidenti gravi noti nel mondo nel 2025

Clusit 2026

1 su 10

di questi incidenti colpisce l'Italia (9,6%)

Clusit 2026

2,78 mld

di euro di spesa cyber in Italia nel 2025: +12%, ma il ritmo rallenta

Politecnico di Milano 2026

La domanda non è se spendere, ma se la spesa segue il rischio.

Fonti: Clusit, Rapporto 2026 (incidenti gravi di dominio pubblico) · Politecnico di Milano, Osservatorio Cybersecurity & Data Protection, 26/2/2026

Spendiamo di più. Sappiamo per quale processo?

16%

delle PMI nella fascia di maturità più alta

Cyber Index PMI 2025

24%

delle PMI attaccate almeno una volta negli ultimi tre anni

Cyber Index PMI 2025

46%

delle grandi imprese usa la BIA per definire gli investimenti

Osservatorio Polimi 2026

38%

PMI prive di un Responsabile IT e di budget cyber

PID Cyber Check

Tre campioni differenti, un problema ricorrente: trasformare consapevolezza, responsabilità e misure in priorità verificabili.

Fonti: Cyber Index PMI 2025, pp. 6, 11, 12, 24–25 · Politecnico di Milano, 26/2/2026 · plenaria Clusit, 17/3/2026

Dove arriva la norma, qualcosa cambia

ITALIA REGOLATA

Finanza, operatori essenziali, perimetro nazionale

Clusit legge segnali di miglioramento: la finanza è al 10° posto tra i settori colpiti in Italia, contro il 6° a livello mondiale.

ITALIA NON REGOLATA

PMI manifatturiere, filiere di subfornitura

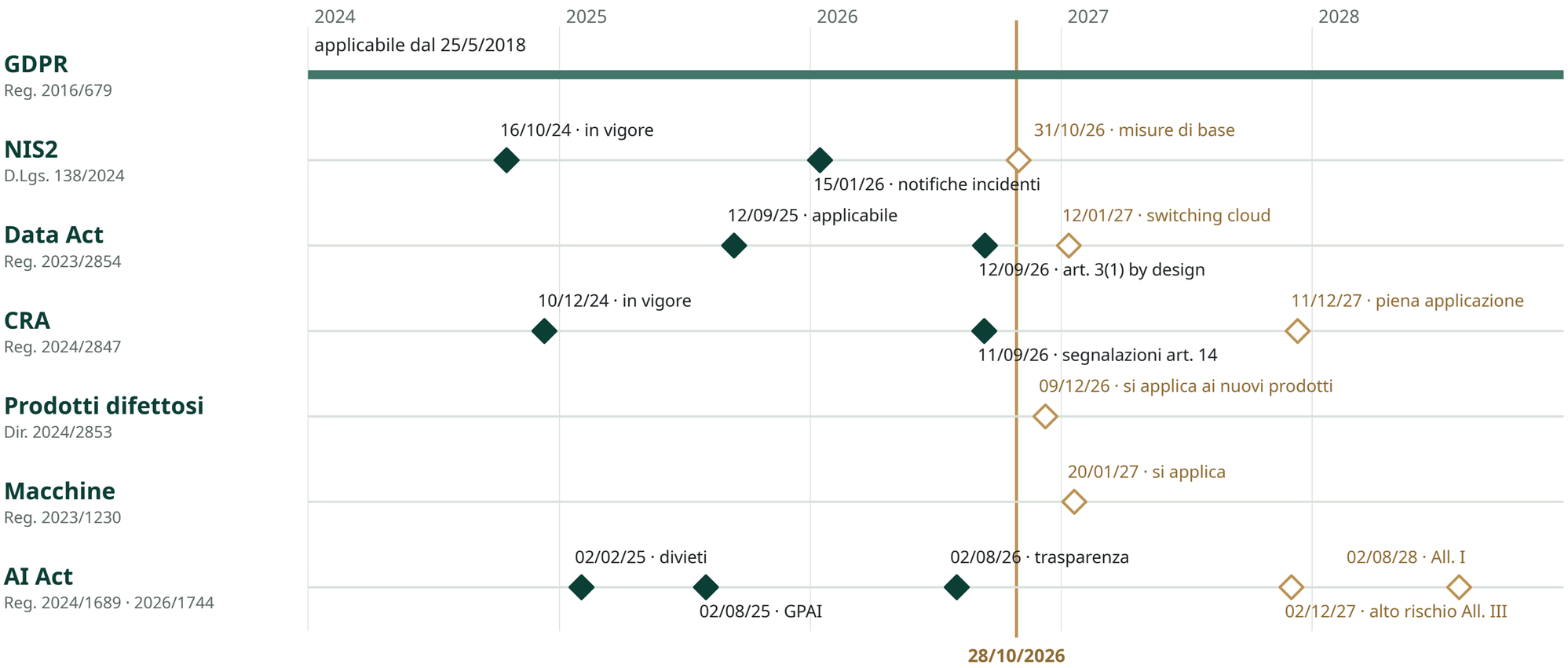
Crescita degli incidenti «reale e strutturale» dovuta anche all'AI.

L'81% delle PMI lavora in filiere con grandi organizzazioni.

Una correlazione, non una prova: ma è il motivo per cui la norma entra in questo discorso.

Fonti: plenaria Clusit, Security Summit Milano, 17/3/2026 («Due Italie digitali») · Cyber Index PMI 2025, p. 12

Dove siamo il 28 ottobre 2026



Fonti: EUR-Lex (testi e date di applicazione), Reg. (UE) 2026/1744 (GU UE 24/7/2026), ACN · Date in formato gg/mm/aa

Stesso verbo, oggetti diversi: dimostrare scelte motivate

PERSONE	SERVIZI	PRODOTTI	DATI	DANNO
GDPR	**NIS2 · D.Lgs. 138/2024**	**CRA · Reg. Macchine · AI Act**	**Data Act**	**Dir. 2024/2853**
Protegge Diritti e libertà degli interessati	**Protegge** Reti, sistemi, continuità del servizio	**Protegge** Sicurezza del prodotto, safety, sistemi AI	**Protegge** Accesso, condivisione, portabilità	**Protegge** Risarcimento da prodotto difettoso
Obbliga Titolari e responsabili	**Obbliga** Soggetti essenziali e importanti	**Obbliga** Fabbricanti, fornitori, deployer	**Obbliga** Fabbricanti di prodotti connessi, cloud	**Obbliga** Fabbricanti e catena di fornitura

Fonti: Reg. (UE) 2016/679; Dir. (UE) 2022/2555 e D.Lgs. 138/2024; Reg. (UE) 2024/2847, 2023/1230, 2024/1689, 2023/2854; Dir. (UE) 2024/2853

GDPR e NIS2: obiettivi diversi, una sola responsabilità

GDPR · L'OBIETTIVO

Proteggere le persone e i loro dati

Il titolare deve poter dimostrare che le misure sono adeguate al rischio per gli interessati.

NIS2 · L'OBIETTIVO

Garantire la continuità dei servizi

Gli organi di amministrazione approvano le misure, ne sovrintendono l'attuazione e ne rispondono.

In entrambi i casi risponde l'organizzazione

1 Conoscere i propri rischi

valutare i rischi per persone e servizi, con criteri dichiarati e riesaminati

GDPR artt. 24, 32 · NIS2 art. 21(2)(a)

2 Saper ripristinare, e provarlo

ripristinare in tempi adeguati e verificare con test che le misure funzionino

GDPR art. 32(1)(c)-(d) · NIS2 art. 21(2)(c), (f)

3 Decidere e documentare

scelte approvate, responsabilità assegnate, evidenze conservate

GDPR art. 5(2) · D.Lgs. 138/2024 art. 23

Risk Assessment e BIA sono il modo più diretto per rispondere a queste tre richieste.

Fonti: Reg. (UE) 2016/679, artt. 5(2), 24, 32; Dir. (UE) 2022/2555, artt. 20–21; D.Lgs. 138/2024, artt. 23–24 · NIS2 solo per i soggetti nel perimetro

La sicurezza entra nel prodotto e lo segue nel tempo

Progettazione

CRA art. 13(2)

valutazione dei rischi cyber del prodotto, integrata in progettazione e sviluppo

Macchine RESS 1.1.9 e 1.2.1

protezione contro la corruzione; sistemi di comando affidabili anche contro tentativi dolosi

Immissione sul mercato

CRA · Macchine

conformità, documentazione tecnica, marcatura CE

Uso e vulnerabilità

CRA art. 14

segnalazione di vulnerabilità sfruttate e incidenti gravi: applicabile dall'11/9/2026

Aggiornamenti

CRA Allegato I

gestione delle vulnerabilità e aggiornamenti per il periodo di supporto

Danno

Dir. 2024/2853

il software è un prodotto (art. 4); la cybersecurity pesa sulla difettosità (art. 7); niente esimente se il difetto dipende da aggiornamenti mancanti (art. 11)

Per chi gestisce una fabbrica: chi apporta una modifica sostanziale a una macchina può assumere gli obblighi del fabbricante (Reg. 2023/1230, art. 18). Il retrofit e la connessione di impianti OT diventano scelte da valutare anche sotto il profilo cyber.

Fonti: Reg. (UE) 2024/2847 (CRA), artt. 13–14, Allegato I, art. 71; Reg. (UE) 2023/1230, Allegato III e art. 18; Dir. (UE) 2024/2853, artt. 4, 7, 11

Dalle norme ai processi, dai processi ai ruoli



Applicabilità → **Responsabilità** → **Processo** → **Controllo** → **Evidenza** → **Riesame**

Ogni norma arriva in un processo, con un responsabile e un'evidenza

Rappresentazione Connect 4 · per i soggetti NIS: D.Lgs. 138/2024, art. 23

Persone e fornitori: dove il rischio esce dal perimetro IT

PERSONE

96% **dei CISO indica la gestione del fattore umano come prima criticità**

e il 60% è preoccupato dall'uso di AI consumer in azienda

COSA CHIEDONO LE NORME

NIS2 art. 21(2)(g)	igiene informatica e formazione
D.Lgs. 138/2024 art. 23	formazione obbligatoria degli organi di amministrazione
AI Act art. 4	misure per l'alfabetizzazione AI (testo 2026)

La formazione diventa una misura con owner, contenuti ed evidenze, a partire dal vertice.

FORNITORI

81% **delle PMI lavora in filiere con grandi organizzazioni**

e il 73% delle grandi imprese valuta anche la provenienza geografica dei fornitori cyber

COSA CHIEDONO LE NORME

NIS2 art. 21(2)(d)	sicurezza della catena di approvvigionamento
GDPR art. 28	responsabili del trattamento e garanzie
CRA · Data Act	requisiti dei prodotti acquistati; cambio di fornitore cloud

Il fornitore entra nella BIA (dipendenze, SLA) e nel Risk Assessment (scenari): il contratto diventa un controllo.

Fonti: Politecnico di Milano, 26/2/2026 · Cyber Index PMI 2025, p. 12 · Dir. (UE) 2022/2555; D.Lgs. 138/2024; GDPR; AI Act come modificato dal Reg. (UE) 2026/1744

Un processo, non una formula matematica

VALUTAZIONE DEL RISCHIO (RISK ASSESSMENT)

Contesto e criteri	Identificazione	Analisi	Ponderazione	Trattamento	Accettazione
perimetro, obiettivi, criteri di valutazione e di accettazione approvati prima di stimare	scenari per eventi o per asset: sorgente, condizione abilitante, evento, conseguenze	probabilità e conseguenze motivate da evidenze; controlli esistenti e loro efficacia	confronto con i criteri, priorità; rischio inerente e residuo	modificare, evitare, condividere, ritenere; piano con owner, tempi, costi	il risk owner accetta formalmente il rischio residuo

Comunicazione e consultazione con process owner, direzione, fornitori

Monitoraggio e riesame: nuove minacce, cambi di perimetro, esiti dei test, incidenti

Output: registro dei rischi, piano di trattamento, decisioni tracciabili con data di riesame

Riferimento: ISO/IEC 27005:2022, clausole 6–10; ISO/IEC 27001:2022, 6.1.2–6.1.3 · Schema di sintesi Connect 4

Uno scenario è una catena causale verificabile

SORGENTE

Gruppo ransomware con credenziali VPN acquistate

→

CONDIZIONE ABILITANTE

VPN senza MFA; rete IT e OT non segmentate

→

EVENTO

Accesso, movimento laterale, cifratura dei server MES

→

CONSEGUENZA

Linee ferme, ordini non evasi, dati di produzione persi

CONTROLLI CHE AGISCONO SU OGNI ANELLO

Prevenire

MFA su VPN · patching · segmentazione IT/OT

Rilevare

EDR · log VPN e accessi anomali · monitoraggio 24/7

Rispondere

playbook ransomware · isolamento dei segmenti · decisione di fermo

Ripristinare

backup immutabili e testati · ordine di ripristino · DR

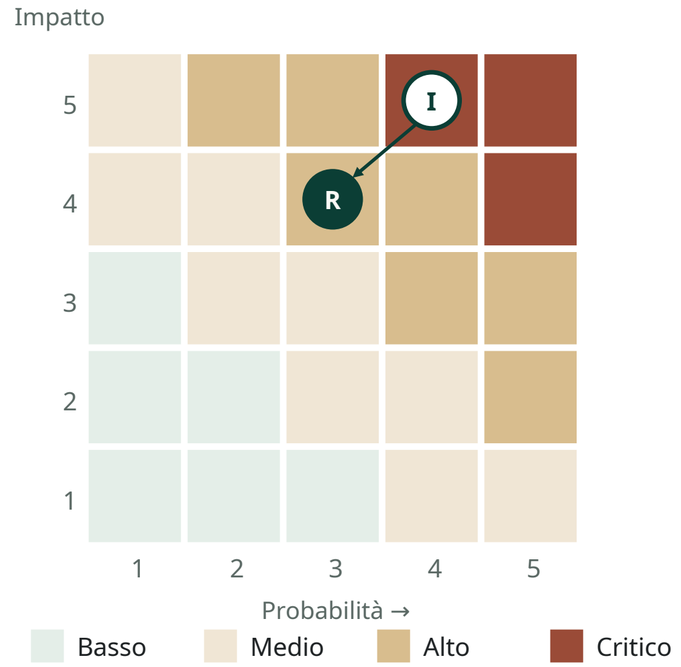
Riferimento metodologico: ISO/IEC 27005:2022, approccio per eventi · Azienda manifatturiera ipotetica

Criteri ancorati al business, non colori arbitrari

ESEMPIO DI SCALA · da tarare e approvare per ogni organizzazione

Livello	Operativo	Legale e contrattuale	Persone e safety
1 Trascurabile	fermo assorbibile con workaround	nessun obbligo attivato	nessun effetto
2 Limitato	fermo entro l'RTO	obblighi interni, nessuna notifica	disagio operativo
3 Rilevante	fermo oltre l'RTO, entro l'MTPD	notifica all'autorità o al cliente	esposizione a rischio gestita
4 Grave	fermo oltre l'MTPD	penali, contestazioni, sanzioni possibili	rischio per la salute
5 Critico	perdita della capacità minima (MBCO)	contenzioso o sanzioni rilevanti	danno alle persone

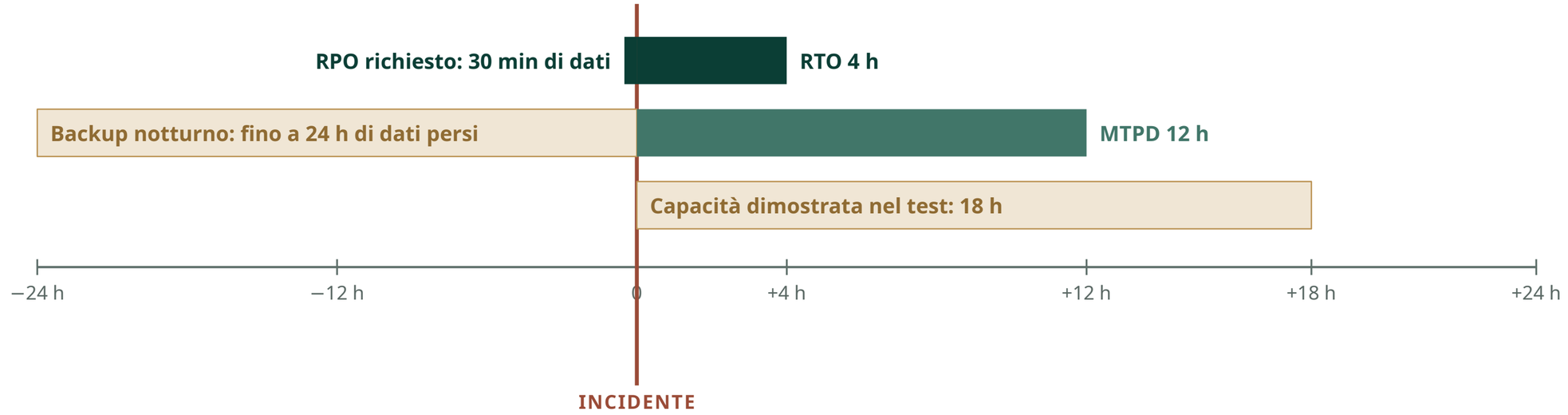
La scala operativa usa le soglie della BIA: RA e BIA parlano la stessa lingua.



I = inerente (critico) dello scenario ransomware · R = residuo dopo MFA e segmentazione (alto). Livelli da tabella approvata, non dal prodotto P × I.

ISO/IEC 27005:2022 non prescrive matrici né scale: criteri, livelli e soglie sono scelte dell'organizzazione

RPO guarda indietro, RTO e MTPD guardano avanti



RPO

punto a cui i dati devono essere ripristinati: misura i dati che si possono perdere

RTO

tempo entro cui l'attività riprende, a una capacità minima concordata; sta dentro l'MTPD

MTPD

oltre questo tempo gli impatti del fermo diventano inaccettabili

MBCO

capacità minima accettabile durante l'interruzione (es. una linea, ordini prioritari)

Definizioni: parafrasi di ISO 22300:2021 e ISO 22301:2019 §8.2.2 · Valori ipotetici

La BIA collega processi, asset e fornitori

Servizi → Attività prioritarie → Impatti nel tempo → Soglie → **Dipendenze** → Convalida

PROCESSO CRITICO · BIA

Produzione

MTPD 24 h
RTO 8 h
RPO 30 min

soglie approvate dalla direzione

DIPENDE DA

Asset

MES · ERP · identità (AD) · rete e VPN · dati di produzione · persone chiave

Fornitori

ERP in cloud · manutentore OT · MSP

SLA del manutentore 12 h > RTO 8 h

SCENARI · RISK ASSESSMENT

R1 Ransomware cifra il MES

R2 Accesso remoto del manutentore OT compromesso

R3 Indisponibilità prolungata dell'ERP in cloud

impatto e priorità letti dalla BIA

La BIA dice cosa proteggere e entro quando, e da quali asset e fornitori dipende.

Il Risk Assessment costruisce gli scenari su asset e fornitori: da cosa, e con quale probabilità.

Riferimenti: ISO 22301:2019, §8.2.2; ISO/TS 22317:2021; ISO/IEC 27005:2022 · processo, asset e fornitori ipotetici

Dove interveniamo prima?

ESEMPIO ILLUSTRATIVO · non è un caso aziendale reale

VULNERABILITÀ A

CVSS 9,8

Server di test

Rete isolata, nessun dato di produzione, nessuna dipendenza critica

VULNERABILITÀ B

CVSS 7,2

Server MES

Raggiungibile dalla rete IT; processo con RTO 4 h e MTPD 12 h

La risposta non è nel punteggio. È nei fattori che il punteggio non misura:

Gravità tecnica	Sfruttamento	Esposizione	Criticità del processo	Controlli esistenti
CVSS: severità, non rischio (FIRST)	noto (CISA KEV) o probabile (EPSS)	raggiungibilità reale, percorso d'attacco	dalla BIA: RTO, MTPD, dipendenze	compensativi: segmentazione, monitoraggio

Nessun ordine automatico: se A fosse esposta su Internet e sfruttata attivamente, la priorità si invertirebbe.

FIRST, CVSS v4.0 Specification (2023) · CISA Known Exploited Vulnerabilities · FIRST EPSS · Caso ipotetico

Il Board non sceglie il firewall. Decide il rischio

LA DOMANDA DEL BOARD		DA DOVE VIENE LA RISPOSTA	
1	**Quali processi non possono fermarsi?**	**BIA**	attività prioritarie e servizi critici
2	**Per quanto possiamo tollerare il fermo?**	**BIA**	MTPD, capacità minima, RPO
3	**Cosa può realisticamente fermarli?**	**Risk Assessment**	scenari, probabilità, controlli efficaci
4	**Quali opzioni abbiamo, e a che costo?**	**Piano di trattamento**	alternative, costi, rischio residuo atteso
5	**Quale rischio residuo accettiamo, e come lo verifichiamo?**	**Accettazione e monitoraggio**	delibera, KPI e KRI, test, riesame

Le norme possono rendere obbligatorio il confronto, tuttavia è la qualità delle analisi rende possibile la scelta.

Per i soggetti NIS: D.Lgs. 138/2024, art. 23 · Polimi 26/2/2026: 57% delle grandi imprese registra più attenzione del board dopo la NIS2

Dalla norma al miglioramento: un flusso di lavoro

COMPRENDERE

Fasi 01–03

- 01 Contesto e norme
- 02 BIA e criticità
- 03 Risk & gap

DECIDERE

Fasi 04–05

- 04 Trattamento
- 05 Board e budget

AGIRE E VERIFICARE

Fasi 06–07

- 06 Implementazione
- 07 Monitoraggio e riesame

RIESAME CONTINUO → NUOVO CONTESTO → NUOVE PRIORITÀ

Framework operativo proposto da Connect4, non uno standard né una certificazione · responsabilità decisionali in capo all'azienda

Un ciclo in sette fasi, tre competenze nello stesso processo

Clusit avverte: impostare la cyber delegata alla sola compliance rischia di produrre investimenti poco aderenti al contesto.

01	02	03	04	05	06	07
Contesto normativo	**BIA**	**Risk Assessment e Gap Analysis**	**Piano di trattamento**	**Decisioni del Board**	**Implementazione delle misure**	**Monitoraggio e miglioramento**
norme applicabili a processi, prodotti e dati; ruoli e responsabilità	processi critici, impatti nel tempo, MTPD, RTO, RPO, dipendenze	scenari, controlli esistenti, rischio inerente e residuo, gap	modificare, evitare, condividere, ritenere. include costi, tempi, target	valuta gli scenari, assegna risorse, accetta il rischio residuo	policy, contratti, formazione e misure di sicurezza	servizi gestiti, verifica KPI, audit, test di ripristino, riesami
OUTPUT **matrice norme × processi × owner**	OUTPUT **priorità e obiettivi di ripristino**	OUTPUT **registro rischi e non conformità**	OUTPUT **roadmap e business case**	OUTPUT **Delibera budget e KPI**	OUTPUT **misure attuate ed evidenze**	OUTPUT **nuove evidenze per il ciclo**

riesame continuo · BIA e Risk Assessment iterano tra loro

	01	02	03	04	05	06	07
Legal & Compliance	**applicabilità, ruoli, obblighi**	obblighi contrattuali e di notifica	gap normativi e documentali	contratti, clausole, policy	responsabilità e delibere	policy, formazione, contratti	audit e aggiornamento normativo
Cybersecurity	minacce di settore	**metodo e criteri**	**scenari, controlli, VA**	priorità e rischio target	rischio residuo	MFA, VA, awareness, IR	Virtual CISO, monitoraggio, KPI
IT & Infrastructure	inventario e architetture	dipendenze e capacità attuali	verifica tecnica dei controlli	fattibilità, costi, tempi	opzioni tecniche comparate	**implementazioni tecniche**	managed IT, test di ripristino
Azienda	direzione	process owner	risk owner	direzione	**decide il Board**	funzioni aziendali	riesame della direzione

Modello di lavoro Connect4, non uno standard · celle piene = guida, chiare = contribuisce · le decisioni restano all'azienda · Clusit, 17/3/2026

Se il rischio resta tecnico,
il budget sembra un costo.

Quando il rischio diventa d’impresa,
il budget diventa una decisione.

Alessandro Zerpelloni · Connect4 Consulting

Q&A

Contatti:

a.zerpelloni@c4consulting.it
info@c4consulting.it

Venite a trovarci al nostro Stand!

Fonti

Clusit, Rapporto 2026 sulla sicurezza ICT in Italia (dati 2023–2025) e plenaria Security Summit Milano, 17/3/2026 — api.securitysummit.it

Clusit, Rapporto 2025, capitolo PID Cyber Check · Camere di Commercio, Report PID Cyber Check 2025

Confindustria–Generali, Cyber Index PMI 2024 e 2025 — public.confindustria.it

Politecnico di Milano, Osservatorio Cybersecurity & Data Protection, comunicato del 26/2/2026 — osservatori.net

Reg. (UE) 2016/679 · Dir. (UE) 2022/2555 · D.Lgs. 4/9/2024 n. 138 · Det. ACN 379907/2025

Reg. (UE) 2024/2847 · Reg. (UE) 2023/1230 · Dir. (UE) 2024/2853 · Reg. (UE) 2024/1689 e 2026/1744 · Reg. (UE) 2023/2854 — eur-lex.europa.eu

ISO/IEC 27005:2022 · ISO/IEC 27001:2022 · ISO 22301:2019 · ISO/TS 22317:2021 · ISO 22300:2021

FIRST, CVSS v4.0 Specification e EPSS · CISA, Known Exploited Vulnerabilities Catalog