



CONFININDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

CYBERSECURITY ASSESSMENT

**Analisi della resilienza aziendale sul fronte della sicurezza informatica
per introdurre la cultura della gestione del rischio cyber**

11 novembre 2025

L'INIZIATIVA:

REALIZZATA TRAMITE CONFININDUSTRIA INNOVATION HUB, il Polo Nazionale di Innovazione digitale
creato da Confindustria nell'ambito del progetto finanziato dal Ministero delle Imprese e del Made in Italy
a valere sul PNRR

PENSATA PER LE PMI con l'obiettivo di fornire una misura del posizionamento tecnico organizzativo
dell'impresa ed aumentare il livello di consapevolezza del rischio cyber. Sempre di più la Cybersicurezza sarà
un vantaggio competitivo.

LO STRUMENTO si sviluppa partendo da una verifica di trenta controlli essenziali di Cybersicurezza.

PROCESSO- FASE1:



INDIVIDUAZIONE PROFILO DI RISCHIO

Lo strumento individua il profilo di rischio dell'impresa andando a individuare un livello di maturità target da raggiungere

IL CYBER ASSESSMENT si adatta allo specifico contesto dell'azienda



MISURAZIONE DEL LIVELLO CYBER

Lo strumento misura il livello Cybersicurezza che raggiunge l'impresa e indica se il livello di maturità minimo è superato o meno

IL CYBER ASSESSMENT fornisce la postura di sicurezza dell'organizzazione analizzandola

- a livello generale,
- per Category,
- per Function.



SUGGERIMENTI PRATICI: «QUICK WIN» e «NEXT STEPS»

Lo strumento fornisce suggerimenti per orientare una gap analysis e definire azioni per superare il livello di maturità target e implementare una roadmap di remediation

IL CYBER ASSESSMENT restituisce «Quick Wins» e «Next Steps»

CONTESTUALIZZAZIONE:

PER ESSERE APPLICABILE IL FRAMEWORK DEVE ESSERE CONTESTUALIZZATO

Nella prima fase di valutazione, per effettuare la contestualizzazione vengono utilizzati elementi quali, ad esempio, sedi, dimensione aziendale, settore di riferimento... Con queste informazioni viene valutata la probabilità di esposizione al rischio della realtà specifica.

Successivamente, attraverso un altro set di domande, vengono valutati gli impatti potenziali di un *cyber* attacco. Mediante queste informazioni è definito il fattore di **rischio di Cybersicurezza** dell'azienda.

		IMPATTI (I)					FATTORE DI RISCHIO (NORMALIZZAZIONE P*I)	
		1	2	3	4	5	MOLTO BASSO	1
PROBABILITA' (P)	1						BASSO	2
	2						MEDIO	3
	3						ALTO	4
	4						CRITICO	5
	5							



Progetto realizzato da

PROCESSO- FASE2:



INDIVIDUAZIONE PROFILO DI RISCHIO

Lo strumento individua il profilo di rischio dell'impresa andando a individuare un livello di maturità target da raggiungere

IL CYBER ASSESSMENT si adatta allo specifico contesto dell'azienda



MISURAZIONE DEL LIVELLO CYBER

Lo strumento misura il livello Cybersicurezza che raggiunge l'impresa e indica se il livello di maturità minimo è superato o meno



SUGGERIMENTI PRATICI: «QUICK WINS» e «NEXT STEPS»

Lo strumento fornisce suggerimenti per orientare una gap analysis e definire azioni per superare il livello di maturità target e implementare una roadmap di remediation

IL CYBER ASSESSMENT fornisce la postura di sicurezza dell'organizzazione analizzandola

- a livello generale,
- per Category,
- per Function.

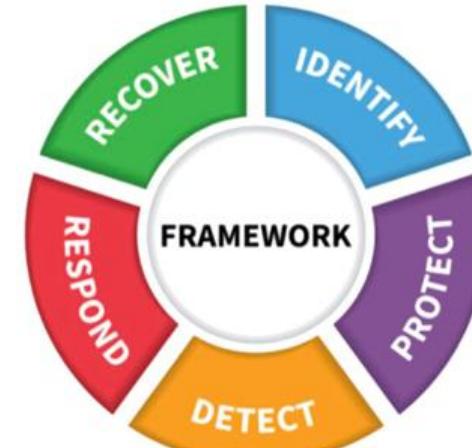
IL CYBER ASSESSMENT restituisce «Quick Wins» e «Next Steps»

FUNCTION E CATEGORY:

Il **cyber assessment** segue le **5 Function** del Framework nazionale per la Cybersicurezza e Data Protection:

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

che devono integrarsi in modo sequenziale per identificare, gestire e reagire ai rischi e agli attacchi cyber.



Progetto realizzato da

PROCESSO- FASE3:



INDIVIDUAZIONE PROFILO DI RISCHIO

Lo strumento individua il profilo di rischio dell'impresa andando a individuare un livello di maturità target da raggiungere

IL CYBER ASSESSMENT si adatta allo specifico contesto dell'azienda



MISURAZIONE DEL LIVELLO CYBER

Lo strumento misura il livello Cybersicurezza che raggiunge l'impresa e indica se il livello di maturità minimo è superato o meno

IL CYBER ASSESSMENT fornisce la postura di sicurezza dell'organizzazione analizzandola
- a livello generale,
- per Category,
- per Function.



SUGGERIMENTI PRATICI: «QUICK WINS» e «NEXT STEPS»

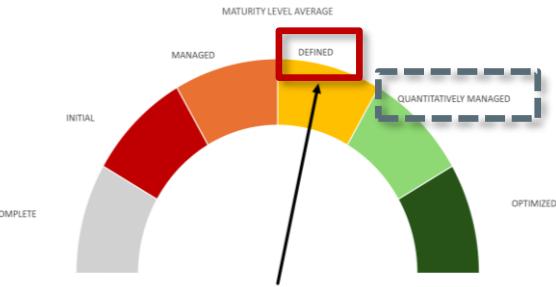
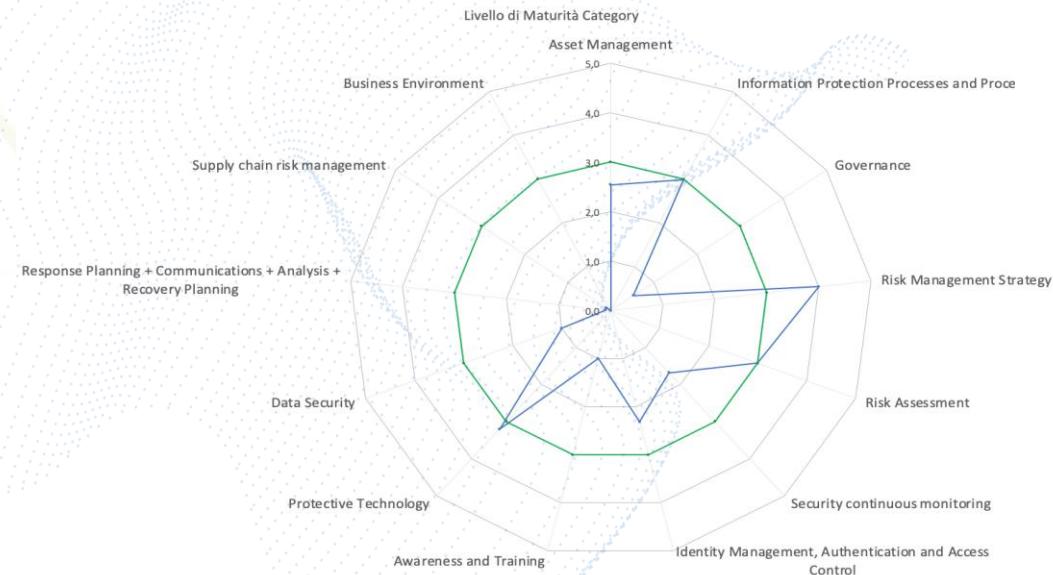
Lo strumento fornisce elementi per orientare una «gap analysis» e definire azioni per superare il livello di maturità target e implementare una roadmap di «remediation»

IL CYBER ASSESSMENT restituisce
«Quick Wins» e «Next Steps»

Progetto realizzato da

IL REPORT DI RESTITUZIONE:

- Livello complessivo di maturità Cyber dell'azienda rilevato mediante l'assessment e indicazioni di eventuali gap



Per informazioni sulle agevolazioni e per attivare il servizio:
ricercainnovazione@confindustriavenest.it