

CYBERSECURITY ASSESSMENT

3 Febbraio 2025



CONFINDUSTRIA



INNOVATION HUB



**Finanziato
dall'Unione europea**
NextGenerationEU

I punti di vista e le opinioni espresse sono solo quelli degli autori e non riflettono necessariamente quelli dell'Unione europea o della Commissione europea. Né l'Unione europea né la Commissione europea possono essere ritenute responsabili per essi

Progetto realizzato da



SISTEMI
FORMATIVI
CONFINDUSTRIA



DIH
Digital Innovation Hub

Chi Siamo

CONFINDUSTRIA INNOVATION HUB è 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**.

CONFINDUSTRIA INNOVATION HUB si avvale del coordinamento operativo di **Sistemi Formativi Confindustria** e opera attraverso i **Digital Innovation Hub** (DIH) del network costituito da Confindustria nel 2017, strutture che affiancano le imprese su tutto il territorio nazionale, erogando servizi di assessment e orientamento digitale, con l'obiettivo di:

- promuovere la domanda di innovazione del sistema produttivo,
- aumentare la consapevolezza sulle opportunità offerte dalla digitalizzazione di processi e prodotti,
- operare come punto di accesso delle imprese alle tecnologie abilitanti dell'Industria 4.0.

Servizi Erogati

Nell'ambito del progetto finanziato dal MIMIT, Confindustria Innovation Hub eroga alle imprese **tre tipologie di servizi**, che permettono di realizzare, attraverso l'impiego di una **piattaforma digitale web-based**, un'approfondita analisi multidimensionale dei processi aziendali, evidenziando punti di forza e punti di debolezza sul fronte della digitalizzazione e della cybersecurity, al fine di restituire all'azienda una fotografia dettagliata del proprio status in rapporto ai relativi benchmark di settore e ai trend tecnologici:

1. SERVIZIO MODULARE DI FIRST-ASSESSMENT DIGITALE E ORIENTAMENTO

per l'analisi del livello di maturità digitale dei processi aziendali e per l'individuazione dei possibili percorsi di innovazione digitale (nell'ambito del servizio le aziende hanno la possibilità di scegliere se fruire di entrambi i moduli previsti (First Assessment + Orientamento), o anche solo di uno dei due, a seconda delle specifiche esigenze individuate con gli assessor dei DIH).

2. CYBERSECURITY ASSESSMENT

per l'analisi della resilienza aziendale sul fronte della sicurezza informatica e per introdurre nell'impresa la cultura della gestione del rischio cyber.

3. ASSESSEMENT DIGITALE DI FILIERA

per l'analisi della maturità digitale lungo l'intera catena di fornitura con l'obiettivo di individuare i gap tecnologici e restituire una visione consolidata del livello di digitalizzazione della filiera.

Progetto realizzato da



**Finanziato
dall'Unione europea**
NextGenerationEU



SISTEMI
FORMATIVI
CONFINDUSTRIA



DIH
Digital Innovation Hub

2. Cybersecurity assessment

Il servizio analizza il livello di maturità dell'azienda sul fronte della sicurezza informatica, attraverso l'impiego di uno strumento coerente con il **Framework Nazionale per la Cybersecurity e la Data Protection**, sviluppato in collaborazione con i Competence Center Cyber 4.0 e Start 4.0 e con la Fondazione Piemonte Innova.

Il **Cyberassessment** mira a identificare gli specifici rischi cyber cui è esposta l'azienda, rilevando il livello di cybersecurity attuale e individuando le eventuali remediation da porre in essere per raggiungere il livello di sicurezza auspicato.

L'analisi prevede:

- l'individuazione dello specifico **Fattore di Rischio** di cyber-esposizione dell'azienda,
- l'analisi dell'effettivo **Livello di cyber-esposizione**, rappresentato tramite radar-chart, con la valorizzazione del **Digital Cyber Score** in una scala da 1 a 5,
- la definizione e restituzione all'azienda di una roadmap con le **possibili remediation** da implementare, sotto forma di Quick Win e Next Steps.



<u>Strumento</u>	Cyber4.0, DIH Liguria, Fondazione Piemonte Innova (FPI) e Start4, su mandato del network dei DIH di Confindustria e di Sistemi Formativi Confindustria (SFC), hanno sviluppato uno strumento (CyberAssessment) di riconosciuta validità, configurandolo come eventuale Prassi di Riferimento UNI Riferimenti: Il CyberAssessment segue i riferimenti del Framework nazionale per la Cybersecurity e Data Protection (FNCS), che discende dal framework NIST, National Institute of Standards and Technology americano, e dello standard internazionale ISO/IEC 27001.
<u>Obiettivo</u>	Il CyberAssessment nasce per aiutare il management aziendale a comprendere l'importanza della protezione dai rischi cyber e promuovere la Data Protection. Ha quindi l'obiettivo di: • aumentare la consapevolezza delle aziende sul tema della cybersecurity • fornire una fotografia del livello di maturità cyber basata su standard di riferimento nazionali e internazionali • suggerire possibili azioni di miglioramento (remediation) che possono contribuire ad innalzare il livello della cyber security dell'azienda

Il **Digital Innovation Hub (DIH)** esegue l'assessment le cui risposte sono condivise con il team degli sviluppatori del tool (Cyber4.0, DIH Liguria, Fondazione Piemonte Innova (FPI) e Start4) e, congiuntamente, elaborano il report su livello di sicurezza e possibili remediation che viene restituito e discusso con l'azienda



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**



MISURAZIONE DEL LIVELLO CYBER

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

**IL CyberAssessment FORNISCE LA POSTURA
DI SICUREZZA DELL'ORGANIZZAZIONE**

- A LIVELLO GENERALE -
- PER CATEGORY -
- PER FUNCTION -



REMIEDIATIONS

Lo strumento fornisce suggerimenti per orientare una gap analysis e definire azioni per implementare una roadmap di remediation

Contestualizzazione

Per effettuare la **contestualizzazione** vengono utilizzati elementi quali, sedi, dimensione aziendale, settore di riferimento...

Con queste informazioni viene valutata la **probabilità** di esposizione al rischio della realtà specifica e vengono valutati gli **impatti** potenziali di un *cyber* attacco.



sulla base delle informazioni raccolte, viene definito il fattore di **rischio di *cyber* esposizione** dell'azienda

Per attribuire dei pesi alle informazioni acquisite, sono considerate le evoluzioni degli attacchi informatici, le percentuali di incidenti e l'intensità degli stessi, descritte da report di settore (vedi Clusit ed ENISA).



Con l'azienda viene definito un "**profilo target**"



I risultati sono elaborati in maniera personalizzata per individuare le evidenze specifiche e le possibili linee di intervento

		IMPATTI (I)				
		1	2	3	4	5
PROBABILITA' (P)	1					
	2					
	3					
	4					
	5					

FATTORE DI RISCHIO	3	MEDIO
--------------------	---	-------

PROFILO DI SICUREZZA TARGET	PROFILO DI SICUREZZA INTERMEDIO
-----------------------------	---------------------------------

Progetto realizzato da

Il **CyberAssessment** restituisce un **DIGITAL CYBER SCORE**

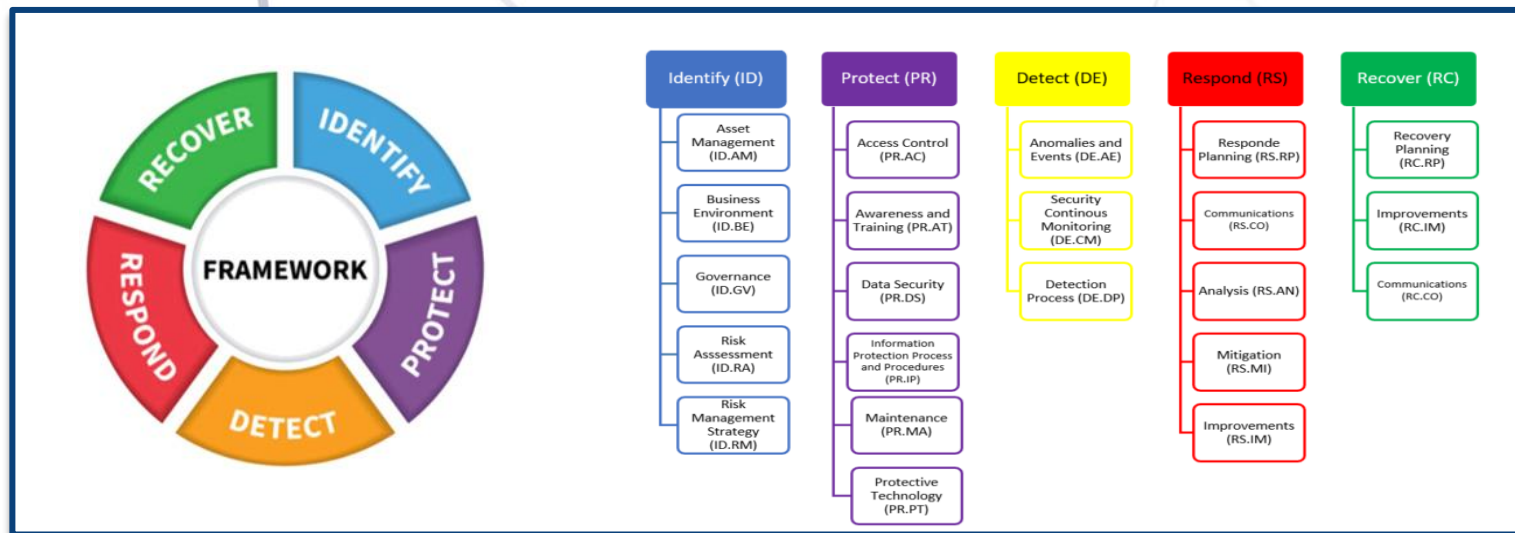
I **livelli di maturità considerati** si riferiscono ai livelli CMMI (*Capability Maturity Model Integration*) e sono:

MATURITY LEVEL	TITLE	DESCRIPTION
INCOMPLETE	Ad hoc and unknown	Incomplete approach to meeting the intent of the Practice Area. May or may not be meeting the intent of any practice. Work may or may not get completed.
INITIAL	Unpredictable and reactive	Initial approach to meeting the intent of the Practice Area. Not a complete set of practices to meeting the full intent of the Practice Area Work gets completed but is often delayed and over budget.
MANAGED	Managed on the project level	Subsumes level 1 practices. Simple, but complete set of practices that address the full intent of the Practice Area. Does not require the use of the organizational assets. <u>Projects are planned, performed, measured, and controlled.</u>
DEFINED	Proactive, rather than reactive.	Builds on level 2 practices. Uses organizational standards and tailoring to address project and work characteristics. Projects use and contribute to organization assets. Organization-wide standards provide guidance across projects, programs, and portfolios.
QUANTITATIVELY MANAGED	Measured and controlled	Organization is data-driven with quantitative performance improvement objectives that are predictable and align to meet the needs of internal and external stakeholders.
OPTIMIZED	Stable and flexible	Organization is focused on continuous improvement and is built to pivot and respond to opportunity and change. The organization's stability provides a platform for agility and innovation.

Function e Category FNCS

Il **CyberAssessment** segue nel suo sviluppo e nella relativa analisi le **function (5)** del Framework nazionale per la *Cybersecurity* e *Data Protection*: **identify, protect, detect, respond, recover** che vengono analizzate, valutate e approcciate in modo integrato per consentire all'azienda di identificare, gestire e reagire ai rischi e agli attacchi *cyber* e/o di mitigarne gli effetti

Ciascuna Function è, a sua volta, suddivisa in **Category**.



Il report

Il report prevede la descrizione dell' «AS IS» tramite appositi chart e la proposta di possibili ed eventuali azioni di rimedio

I risultati evidenziano il livello di maturità raggiunto dall'azienda tenendo in considerazione:

- le dimensioni "**People, Process & Technology**"
- le *Category* e le *Function* (**identify, protect, detect, respond, recover**) del *Framework Nazionale di Cybersecurity e Data Protection*.

Contesto e fattore di rischio
Livello di maturità *target*

GENERALE

Livello di maturità raggiunto
Dettaglio livello di maturità
Effort previsto per remediation

CATEGORY

Livello di maturità raggiunto
Percentuale di completamento
Effort previsto per remediation

FUNCTION

Livello di maturità raggiunto
Percentuale di completamento
Effort previsto per remediation

Remediation (Quick Win e Next Steps)

Progetto realizzato da

Contesto, fattore di rischio, target

Il fattore di rischio è calcolato sulla base delle informazioni di contesto raccolte mediante l'assessment. Il livello di rischio è calcolato come il prodotto del valore medio dei parametri di probabilità e impatto, normalizzato in scala da 1 (Rischio Molto Basso) a 5 (Rischio Critico). Nella tabella sono rappresentati i valori associati a ciascun parametro di Probabilità e Impatto. In particolare:

- il fattore di **Probabilità** indica il livello di esposizione dell'azienda alle minacce cibernetiche
- il fattore di **Impatto** misura i potenziali impatti sugli asset dell'azienda in caso del concretizzarsi di una minaccia



ILLUSTRATIVE

		IMPATTI (I)				
		1	2	3	4	5
PROBABILITÀ (P)	1					
	2					
	3					
	4					
	5					

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

FATTORE DI RISCHIO	2	BASSO
--------------------	---	-------

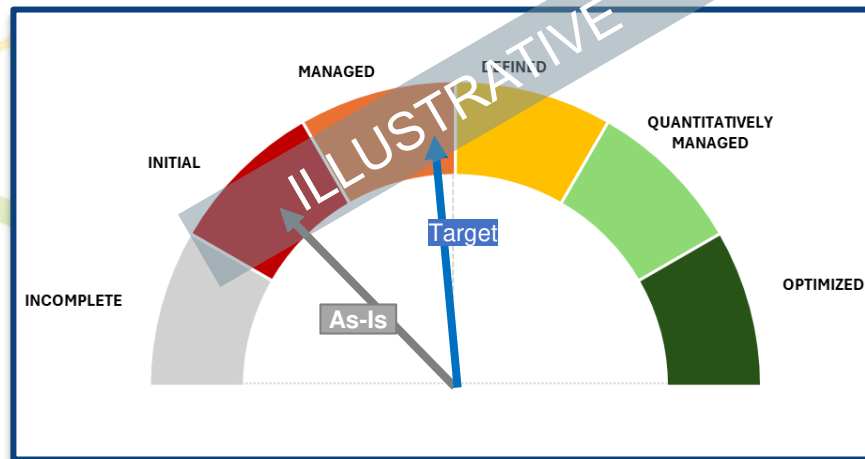
PROFILO DI SICUREZZA TARGET	PROFILO DI SICUREZZA INTERMEDIO
-----------------------------	---------------------------------

LIVELLO DI MATURITA' MINIMO RICHIESTO	MANAGED
---------------------------------------	---------

Livello di maturità raggiunto

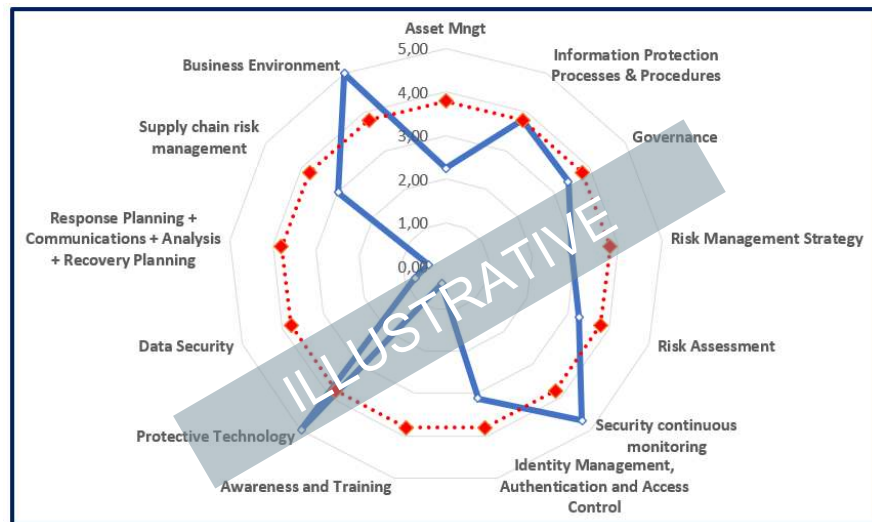
Rispetto al livello di maturità target le risposte, e i relativi «topic», si collocano come indicato nel grafico sottostante determinando a livello aziendale complessivo un indice inferiore al range identificato come target e presenta ambiti («topic») sui quali intervenire con specifiche azioni di remediation. In particolare, sulle 30 domande affrontate (riguardanti i «topic» oggetto di analisi):

- il 25% supera il livello *target*
- il 28% si colloca nel range del livello *target*
- il 47% presenta un indice inferiore al livello *target*



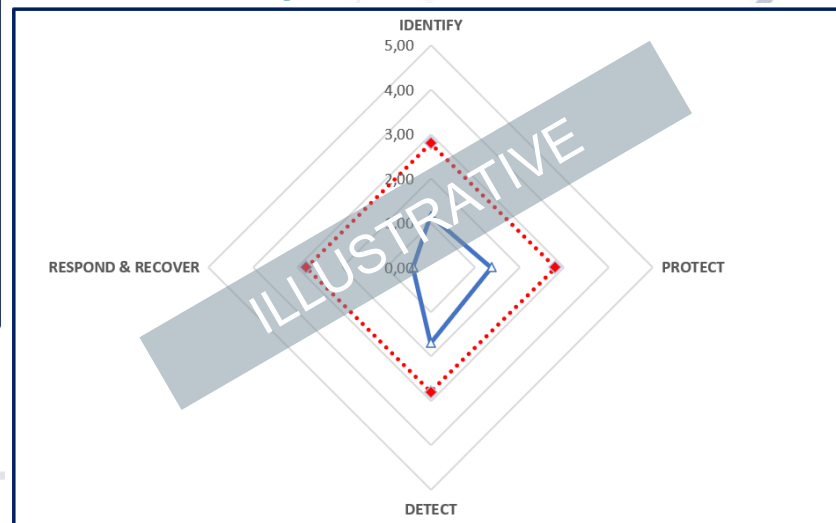
Livello di maturità raggiunto

per CATEGORY



In rosso il **livello target**,
in blu il **livello di maturità attuale** dell'azienda.

per FUNCTION



Progetto realizzato da

Interventi suggeriti volti alla mitigazione del rischio cyber

Ambito di intervento	Remediation (descrizione)	CATEGORY FNCS
Formazione	ILLUSTRATIVE	• Awareness and Training
Ruoli e Responsabilità		• Governance • Asset Management • Identity Management, Authentication and Access Control • Data Security
Piano operativo Budget		• Risk Management Strategy
Normative cyber		• Governance
Back-up		• Information Protection Processes and Procedures

Servizi Erogati

Costo dei servizi (con e senza il finanziamento MIMIT)	Costo con finanziamento MIMIT (oltre IVA)			Costo da listino (oltre IVA)		
	Micro/ Piccola impresa	Media Impresa	Grande Impresa	Micro/ Piccola impresa	Media Impresa	Grande Impresa
Servizio modulare di First-Assessment digitale e Orientamento	0 €	1.038,50 €	8.445,60 €	10.005,00 €	10.385,00 €	14.076,00 €
solo modulo di First-Assessment digitale	0 €	728,00 €	6.210,00 €	6.900,00 €	7.280,00 €	10.350,00 €
solo modulo di Orientamento digitale	0 €	310,50 €	2.235,60 €	3.105,00 €	3.105,00 €	3.726,00 €
Servizio di Cybersecurity Assessment	0 €	402,50 €	2.415,00 €	4.025,00 €	4.025,00 €	4.025,00 €
Servizio di Assessment digitale di filiera	0 €	728,00 €	18.285,00 €	6.900,00 €	7.280,00 €	Costo variabile in relazione al numero di aziende coinvolte



Contatti



Associazione Territoriale Confindustria di riferimento
oppure

assessment@dihlombardia.com

Grazie

innovationhub.confindustria.it



Finanziato
dall'Unione europea
NextGenerationEU

Progetto realizzato da



SISTEMI
FORMATIVI
CONFINDUSTRIA



DIH
Digital Innovation Hub