



CYBERSECURITY

Audit NIST 1-100



VALUTAZIONI INIZIALI

Collaborando con le aziende è possibile rilevare una serie di **problematiche comuni legata alla gestione della Cybersecurity e del trattamento dati.**

La loro osservazione ha agito da stimolo per individuare le attività risolutive che andremo a presentare in questo documento.





LE PROBLEMATICHE

- **La mappatura dello stato di fatto del livello di Cybersecurity** richiede molto tempo e non garantisce l'analisi completa di tutti gli aspetti
- Risulta **complesso riferire in maniera chiara e comprensibili i rischi e le debolezze individuate** all'interno di un sistema a funzioni che hanno ruoli decisionali, ma hanno scarsa dimestichezza con i concetti IT





LE PROBLEMATICHE

- Le **attività di monitoraggio** di un sistema e del suo livello di Cybersecurity sono effettuati in maniera **non strutturata e senza una periodicità definita**
- Spesso le attività legate alla **Cybersecurity e alla sicurezza dei dati sono demandate in maniera esclusiva al reparto IT** che risulta isolato dal resto dell'organizzazione





LE PROBLEMATICHE

- L'**errore umano** è la principale causa di incidenti, anche con gravi conseguenze. Sarebbe necessario diffondere maggiormente la cultura della **formazione continua di tutto il personale** dell'organizzazione, anche su tematiche legate alla Cybersecurity e alla gestione dei dati.





LE SOLUZIONI

Le soluzioni individuate sono due:

AUDIT NIST 1-100

UNI EN ISO 27001





AUDIT NIST 1-100

Un **ASSESSMENT** di altissimo livello



Audit NIST 1-100

Audit NIST 1-100 è un **ASSESSMENT** che consente di valutare in maniera oggettiva, secondo linee guida internazionalmente riconosciute, il **livello di cybersecurity** di una organizzazione



AUDIT NIST 1-100

Lo strumento lavora tramite una apposita **check-list** che valuta tutta una serie di aspetti assegnando dei punteggi di conformità. La somma dei punteggi sarà un voto da 1 a 100, dove **100 rappresenta la conformità massima**



AUDIT NIST 1-100

Gli aspetti di conformità e i punti di controllo si basano sul Framework nazionale per la Cybersecurity e la Data Protection, basato a sua volta sul **Cybersecurity Framework del NIST**

(National Institute of Standards and Technology),



AUDIT NIST 1-100

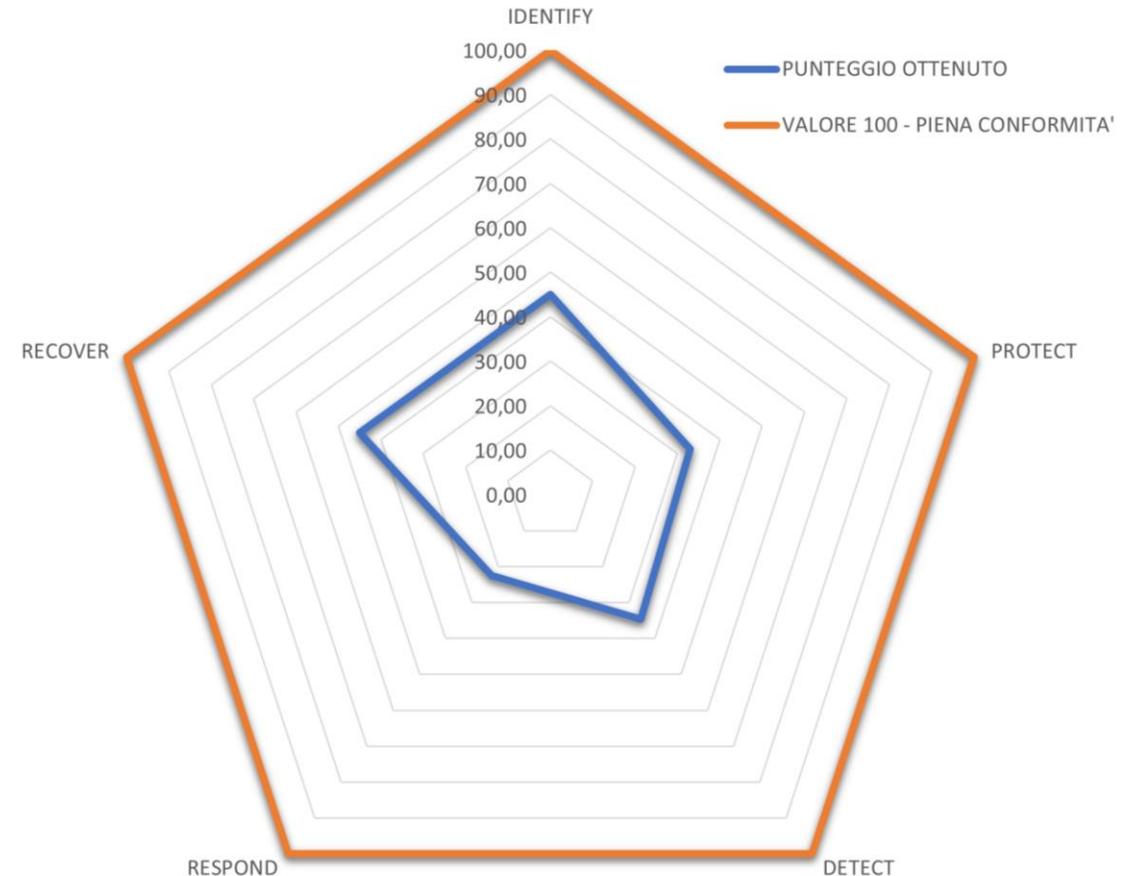
Il Framework nazionale per la Cybersecurity e la Data Protection tiene conto:

- Del Regolamento Europeo Privacy – **GDPR**
 - Delle misure minime di sicurezza **AGID** per la pubblica amministrazione
 - Dello standard **UNI EN ISO 27001** – Certificazione per i sistemi di Gestione per la Sicurezza Informatica
-

AUDIT NIST 1-100

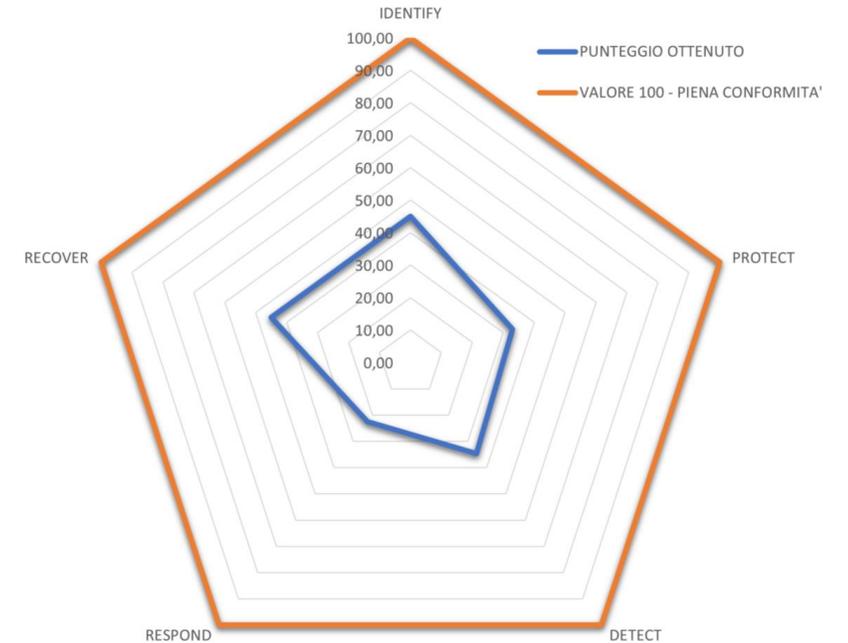
Grazie all'innovativo assessment «Audit NIST 1-100» vengono evidenziati in maniera ottimale i **punti di debolezza** di un sistema secondo le *funzioni del framework NIST** (mappa «as is»)

*Identify – Protect – Detect – Respond – Recover



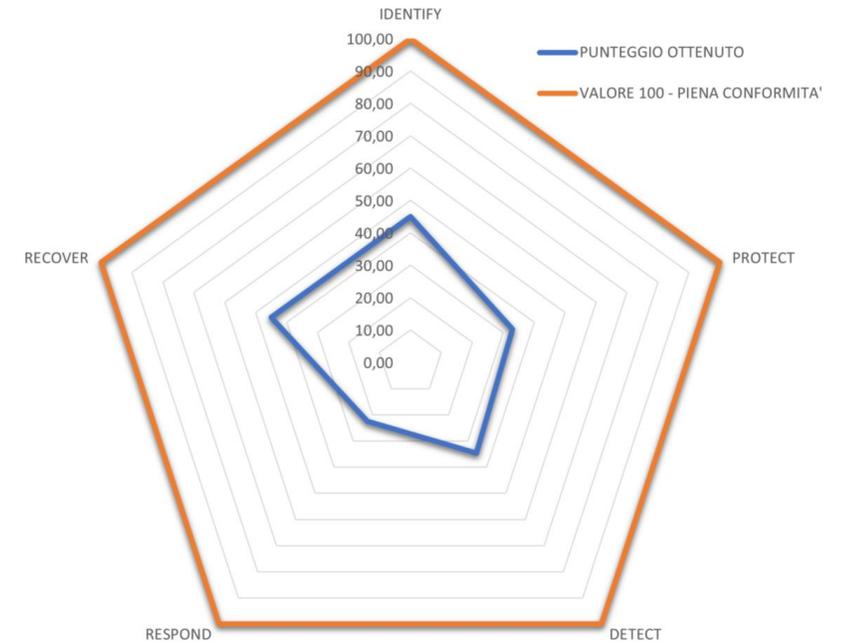
AUDIT NIST 1-100

In questo modo risulta semplice mettere in luce il **gap esistente tra situazione attuale e situazione ottimale/migliorativa**, individuando gli interventi urgenti da attuare per limitare i rischi



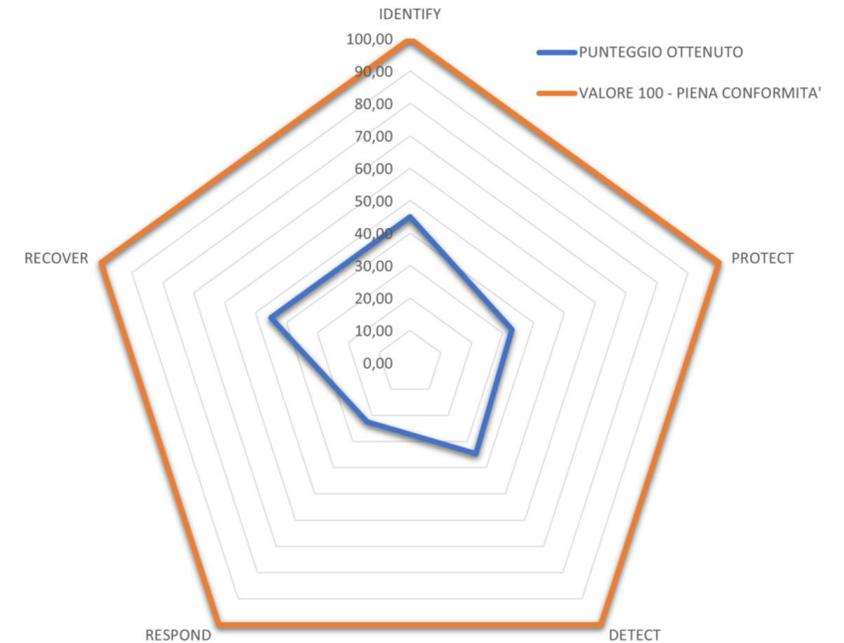
AUDITNIST 1-100

Il **BOARD** riceve i dati e le evidenze in maniera chiara e semplice, di immediata comprensione. Risultano subito evidenti gli ambiti in cui è necessario investire



AUDIT NIST 1-100

L'attività di assessment può essere reiterata negli anni come evidenza del **miglioramento continuo** e dell'evoluzione dei sistemi aziendali, compreso il «sistema privacy»





AUDIT NIST 1-100

Le evidenze dell'assessment risultano un ottimo strumento per dimostrare l'osservanza del principio di **ACCOUNTABILITY** del Regolamento Europeo Privacy (GDPR)

GDPR

EU data protection
regime





UNI EN ISO 27001

**Il valore aggiunto della
certificazione ISO 27001**

ISO 27001





UNI EN ISO 27001

L'assessment «Audit NIST 1-100» è un ottimo strumento che può riferire lo **stato di maturità di un'organizzazione** che vuole intraprendere il percorso di certificazione **UNI EN ISO 27001**.

Potresti essere molto più pronto di quello che credi!

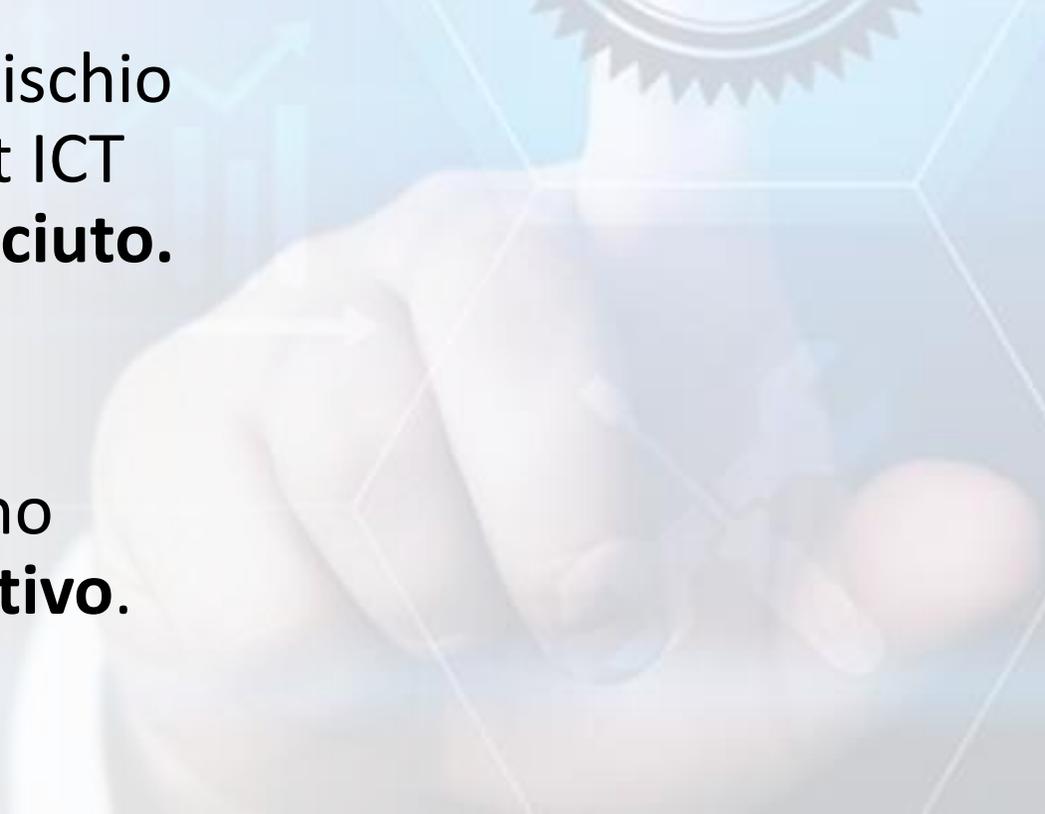




UNI EN ISO 27001

La certificazione ISO 27001 consente di implementare un sistema per la gestione del rischio e la protezione delle informazioni e degli asset ICT secondo uno **standard internazionale riconosciuto**.

Le attività implementate per raggiungere la certificazione sono di tipo strutturato e portano notevoli **vantaggi dal punto di vista organizzativo**.





UNI EN ISO 27001

Grazie ad una certificazione ISO 27001 si ottengono:

- **Maggiore protezione** delle informazioni, in qualunque forma
- **Aumento della resistenza** agli attacchi informatici
- **Protezione completa** da rischi tecnologici e da minacce più comuni
- **Procedure più efficaci** e maggiore attenzione alla **formazione** del personale



UNI EN ISO 27001

Inoltre è possibile assicurarsi la **riduzione di costi della sicurezza delle informazioni.**

Grazie alla **valutazione del rischio e all'approccio analitico** del sistema di gestione, la tua organizzazione può ridurre i costi associati ai livelli aggiuntivi di sicurezza poco efficienti.





UNI EN ISO 27001

L'approccio dello standard **copre l'intera organizzazione** aziendale, non solamente l'area IT. Tiene conto delle persone, dei processi e della tecnologia e permette al personale di comprendere quali siano i rischi e come i controlli di sicurezza come parte del lavoro quotidiano.

La conseguenza è un **miglioramento generale della cultura aziendale**



AUDIT NIST 1-100 e UNI EN ISO 27001

Due strumenti di grande efficacia che posso supportare i reparti IT a:

- Fornire evidenza sullo stato di fatto della Cybersecurity
- Individuare gli investimenti necessari e primari per aumentare il livello di sicurezza
- Implementare e mantenere un sistema di gestione della sicurezza dei dati basato su standard internazionali
- Dare evidenza delle attività di gestione ed evoluzione del sistema
- Supportare il DPO nell'ottemperare al principio di accountability del GDPR



A DISPOSIZIONE

Richiedi una **CALL gratuita di approfondimento**



info@mondo27001.it

