Metodologia per il cybersecurity assessment con il Framework Nazionale per la Cybersecurity e la Data Protection

Centro di ricerca in
Cyber Intelligence e
Information Security

Sapienza
Università di Roma

CYBERSECURITY
NATIONAL
LABORATORY

Metodologia per il cybersecurity assessment con il Framework Nazionale per la Cybersecurity e la Data Protection

CIS-Sapienza
Centro di ricerca di Cyber Intelligence e Information Security
Sapienza Università di Roma

CINI Cybersecurity National Laboratory
Consorzio Interuniversitario Nazionale per l'Informatica

Versione 1.0
Settembre 2021

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

CYBERSECURITY NATIONAL LABORATORY

Titolo: Metodologia per il cybersecurity assessment con il Framework Nazionale per la Cybersecurity e la Data Protection – http://www.cybersecurityfracamework.it

Settembre 2021

Realizzato da:

In collaborazione con:

Autori in ordine alfabetico:

Marco Angelini
Alessandro Bruttini
Claudio Ciccotelli
Andrea Lucariello
Luisa Franchina
Leonardo Querzoni
Francesco Ressa

Con il supporto di:

Gli autori ringraziano per i commenti ed i suggerimenti ricevuti durante la stesura di questo documento:

Fabio Agnello (MPS)
Elena Mena Agresti (Poste Italiane)
Giulio Amarante (BNL)
Marika Assogna (MPS)
Gianluca Bocci (Poste Italiane)
Massimo Cappelli (Poste Italiane)
Antonella Caproni (MPS)
Andrea Cattolico (MPS)
Paolo Colombini (UBI Sistemi e Servizi)
Marco De Ritis (MPS)
Carlo Festucci (MPS)
Giuseppe Galati (Mediobanca)
Emilio Longo (MPS)
Francesca Mattei (MPS)
Benedetta Mazzolli (MPS)
Giorgio Pulino (Poste Italiane)
Roberto Rossi (MPS)
Leonardo Sisinni (MPS)
Nicola Sotira (Poste Italiane)
Salvatore Verdicchia (MPS)

Indice dei contenuti

1 Introduzione

Il rischio legato al verificarsi di attacchi informatici che possano compromettere la sicurezza di informazioni o operazioni è una realtà con cui oggi tutte le organizzazioni, sia pubbliche che private ed operanti nei più diversi settori produttivi, devono necessariamente confrontarsi. Negli ultimi anni si sono affermati, a livello globale, numerosi framework che permettono di guidare l'adozione di misure di sicurezza atte a prevenire e mitigare il rischio attraverso un opportuno meccanismo di governance. Alcuni di questi framework hanno una natura generalista e sono quindi adattabili ad ogni contesto, mentre altri sono stati pensati e sviluppati nell'alveo di determinati settori produttivi, cogliendone le specifiche caratteristiche. Alcuni sono di libera adozione (es. NIST Cybersecurity Framework [1], CIS Critical Security Controls [2]), mentre altri permettono di intraprendere un percorso di auditing indipendente che può sfociare in una vera e propria certificazione (es. ISO 27000 [3]). In generale, i framework per la cybersecurity permettono a chi li adotta di identificare un livello di sicurezza *target* e quindi definire un programma di interventi per il raggiungimento di tale obiettivo.

Il Framework Nazionale per la Cybersecurity e la Data Protection [4] ("Framework" nel prosieguo del documento) rappresenta uno strumento di misura della postura di sicurezza di un'organizzazione in termini di maturità e completamento di attività volte a ridurre il rischio cibernetico. Pubblicato in Italia nel 2015 e aggiornato nel 2019 alla versione 2.0 al fine di cogliere gli aspetti legati alla Data Protection espressi nel GDPR, il Framework consente di approfondire diverse dimensioni inerenti alla cybersecurity.

Ideato per essere fruibile da organizzazioni pubbliche e private di diverse dimensioni, il Framework è caratterizzato da una serie di elementi cardine, che riprendono e integrano quanto proposto dal NIST con il suo Cybersecurity Framework [1]:

Core	Elenco strutturato di requisiti necessari per raggiungere diversi obiettivi di sicurezza. I requisiti sono organizzati in *Function* (Identify, Protect, Detect, Respond, Recovery), *Category* e *Subcategory*.
Controlli	Insieme di azioni in cui si possono declinare i requisiti espressi dalle *subcategory*. Sono da definire in base alle caratteristiche ed alle necessità di ciascuna organizzazione.
Informative references	Riferimenti che legano ogni singola *subcategory* a pratiche di sicurezza note previste da regolamentazioni generali vigenti (es. GDPR, NIS, ecc.) e da standard di settore (es. ISO, COBIT-5, SANS20 ecc.)
Livelli di priorità	Livelli (Alto, Medio, Basso) che indicano la priorità di implementazione delle prescrizioni indicate in ogni *subcategory.*
Livelli di maturità	Livelli di maturità implementativa di *subcategory* e controlli.
Contestualizzazione	Processo di selezione delle *subcategory* di interesse per l'organizzazione e di valutazione dei livelli di priorità e di maturità per le *subcategory* selezionate.

Prototipo di contestualizzazione	*Template* di supporto per attuare una contestualizzazione, basati sulle indicazioni fornite dalle informative reference, best practice di settore e policy di sicurezza interne all'organizzazione.

Sin dal momento della sua introduzione, il Framework Nazionale per la Cybersecurity e la Data Protection ha rappresentato un punto di riferimento in Italia per realtà fortemente eterogenee (dalla grande P.A. alla piccola impresa) che lo hanno adottato come strumento per l'organizzazione della propria strategia di difesa rispetto alle minacce cibernetiche.

Qualunque sia la natura del framework di cybersecurity che un'organizzazione adotta, la stessa si confronterà inevitabilmente con la necessità di valutare quanto le misure di sicurezza attualmente implementate le permettano di soddisfare i requisiti stabiliti dall'obiettivo finale. Questa pratica è nota con il nome di *cybersecurity assessment*, e permette di valutare periodicamente il progresso nell'implementazione di un programma volto all'incremento del livello di cybersecurity. Anche in questo ambito sono state proposte nel tempo più metodologie, con diversi livelli di dettaglio, che fanno riferimento ad alcuni dei framework precedentemente citati. In generale, si distinguono due macro-approcci:

ASSESSMENT QUALITATIVO - le metodologie riconducibili a tale approccio si basano sul presupposto che le pratiche e le soluzioni oggetto della valutazione non permettano una quantificazione oggettiva della loro qualità. Preferiscono quindi andare a valorizzare elementi soggettivi e aspetti che sono difficilmente misurabili.

ASSESSMENT QUANTITATIVO - Tale approccio assume che quanto oggetto di valutazione sia misurabile attraverso una serie di metriche opportunamente definite. Tale misurazione deve essere svolta nel modo più oggettivo possibile, cercando di limitare eventuali contaminazioni del dato misurato derivanti da considerazioni di carattere soggettivo.

Le metodologie di assessment qualitativo vengono spesso adottate laddove sia preferibile un approccio alla valutazione più "snello" o dove i processi di valutazione debbano essere svolti in tempi ridotti o con costi limitati. Di converso, le metodologie quantitative sono più adatte laddove sia necessario un monitoraggio periodico delle performance di un processo di cybersecurity governance o nel caso in cui si debba procedere a una misurazione del ritorno di un investimento nell'ambito della sicurezza cyber. Pertanto, i due approcci non sono esclusivi, ma anzi costituiscono le basi per condurre un cybersecurity assessment in maniera integrata.

Diverse metodologie per il cybersecurity assessment sono oggi disponibili, seppur con alcuni limiti. Infatti, la maggior parte di esse si configurano come soluzioni chiuse, offerte esclusivamente dai vendor che hanno curato il loro sviluppo, e caratterizzate da forte eterogeneità. Tali elementi potrebbero rendere complessa la loro interoperabilità con conseguenze rilevanti sul processo di gestione della cybersecurity. In questo senso, la comparabilità dei risultati ottenuti applicando metodologie concorrenti potrebbe essere limitata o non applicabile (in particolare per gli assessment quantitativi), favorendo un meccanismo di lock-in che spingerebbe le organizzazioni a continuare a rivolgersi allo stesso vendor per garantire la corretta interpretabilità degli assessment sul lungo periodo. Come

conseguenza, organizzazioni diverse non avrebbero modo di comparare reciprocamente l'efficacia delle diverse azioni implementate nei rispettivi piani di cybersecurity, rendendo il processo di assessment una pratica circoscritta ai confini della singola organizzazione.

Questo documento introduce una metodologia di cybersecurity assessment basata sul Framework, ovvero un percorso che le organizzazioni possono seguire per applicare lo stesso al contesto di riferimento e misurare la propria postura in termini di cybersecurity. Tale metodologia introduce diversi elementi innovativi, strutturando le sue attività in tre fasi: Contestualizzazione, Misura, Valutazione.

Per quando riguarda la fase di **Contestualizzazione**, la metodologia seleziona e valuta, in termini di Priorità e Maturità, le subcategory di interesse rispetto alla realtà di riferimento attraverso la combinazione di prototipi di contestualizzazione esistenti, o la definizione di nuovi, tutti basati sulle informative reference generali e su quelle specifiche del proprio settore. Per ciascuna subcategory vengono successivamente individuati uno o più controlli (cioè azioni da intraprendere e quindi da "controllare" per la loro completa realizzazione) atti a soddisfare le prescrizioni indicate nei prototipi e, dunque, a raggiungere gli obiettivi di sicurezza fissati. Infine, vengono definite le priorità di intervento per le subcategory selezionate. Il documento propone in tal senso una metodologia specifica per la definizione del livello di priorità delle singole subcategory.

Il risultato di tale processo di selezione e individuazione rappresenta il Profilo Target ovvero l'obiettivo desiderato cui tendere e da considerare per la realizzazione dell'assessment (cioè l'analisi dinamica di quanto fatto e quanto ancora da fare) nelle fasi successive.

Durante la fase di **Misura** si rileva la distanza tra lo stato attuale e lo stato desiderato (Profilo Target). In questa fase uno o più intervistatori provvede, tramite l'utilizzo di un questionario formulato in base al Profilo Target, a valutare il livello di raggiungimento e realizzazione dei controlli individuati. L'output di questa fase è il Profilo Attuale, ovvero una sintesi della postura di sicurezza dell'organizzazione sulla base dei controlli e delle subcategory individuate al momento dell'assessment.

Nella fase finale, quella della **Valutazione**, è possibile leggere i risultati ottenuti nella fase precedente tramite una valutazione della distanza tra il Profilo Attuale e il Profilo Target. Il risultato si sostanzia in un punteggio di completamento delle azioni individuate e in un ulteriore punteggio che rappresenta il grado di maturità con cui le suddette azioni sono realizzate.

1.1 Vantaggi derivanti dall'uso della metodologia

Un vantaggio fondamentale di questa metodologia è la capacità di effettuare una sola volta la fase di misura, e successivamente poter interpretare i risultati ottenuti secondo diversi punti di vista, denominati in questo documento "ambiti". Ad esempio, il settore di un'organizzazione che si occupa di risk management darà particolare rilevanza agli aspetti inerenti alla gestione del rischio, mentre il settore legale porrà particolare attenzione agli aspetti di compliance. Ciascun settore assegnerà differenti pesi ai controlli di maggiore interesse e, dunque, comportando una modifica dei punteggi risultanti evidenziando i controlli specifici del proprio ambito di competenza. Questa attività abilita una visione

unificata, declinabile opportunamente su determinati ambiti, che non necessita di assessment ripetuti e specifici per l'ambito.

Ulteriore punto di forza ed elemento di innovazione della metodologia presentata in questo documento è l'opportunità di confrontare la propria postura in termini di cybersecurity rispetto a quella di altre organizzazioni. La metodologia è aperta e adottabile da chiunque: dalla singola organizzazione che decide di sviluppare internamente un processo di assessment, al vendor che offre la sua applicazione come servizio verso terzi. La metodologia proposta abilita la condivisione, lo scambio ed il confronto dei risultati, anche tra attori diversi. Tale confronto può supportare la creazione di un benchmark di valutazione tra aziende operanti nello stesso settore, ed una condivisione di best practice di cybersecurity.

Questi vantaggi possono essere analizzati anche rispetto al livello dell'organizzazione su cui agiscono in modo principale, come riportato di seguito ed in Figura 1:

Figura 1 - Legame tra la metodologia di assessment ed i livelli di un'organizzazione

- *Livello tecnico.* Al livello tecnico, la metodologia fornisce la capacità di organizzare e tracciare lo stato dei singoli controlli operativi e la loro semantica in relazione alla tipologia di requisito collegato (regolamenti tecnici, normativa, best practices)
- *Livello esecutivo*. Al livello esecutivo, la metodologia permette di ottenere una visione dello stato di sicurezza di un'organizzazione interpretabile rispetto ai diversi ambiti che trattano la sicurezza informatica, come ad esempio la compliance oppure la gestione dei rischi, permettendo a diversi attori di ragionare sull'assessment rispetto al loro ambito di competenza in modo unificato rispetto ai controlli effettuati.
- *Livello dirigenziale*. Al livello dirigenziale, la metodologia permette di ottenere una visione generale, non legata ai singoli aspetti tecnici, dello stato di sicurezza dell'organizzazione, tramite l'utilizzo del Framework Nazionale di Cybersecurity e Data Protection. La comparabilità che la metodologia fornisce permette di informare processi di decision making con opportune valutazioni sullo stato di operatività sia rispetto al proprio settore di afferenza che rispetto ad attori similari.

Infine, questa metodologia viene rilasciata in forma completamente gratuita e aperta, per favorire la sua adozione, ma anche la sua evoluzione, grazie al contributo di esperienza e conoscenza che tutti i suoi utilizzatori vorranno dare.

Il resto di questo documento è strutturato come segue: la sezione 2 introduce la metodologia di assessment, descrivendo le sue fasi e dettagliando le operazioni da svolgere; la sezione 3 individua le condizioni necessarie affinché i risultati di più assessment siano confrontabili nonché la modalità di svolgimento del confronto stesso; infine sono presenti due Appendici che focalizzano l'attenzione su possibili criteri per l'assegnazione di livelli di maturità e per la rimodulazione dei livelli di priorità.

Il documento è scritto assumendo che il lettore abbia una conoscenza basilare degli strumenti messi a disposizione dal Framework. Per i relativi dettagli il lettore è invitato a consultare il documento che introduce il Framework stesso [4].

2 Descrizione della metodologia

La metodologia prevede tre principali fasi operative:

1. Contestualizzazione
2. Misura
3. Valutazione

La Figura 2 riporta schematicamente come le tre fasi citate interagiscano nello sviluppo della metodologia.

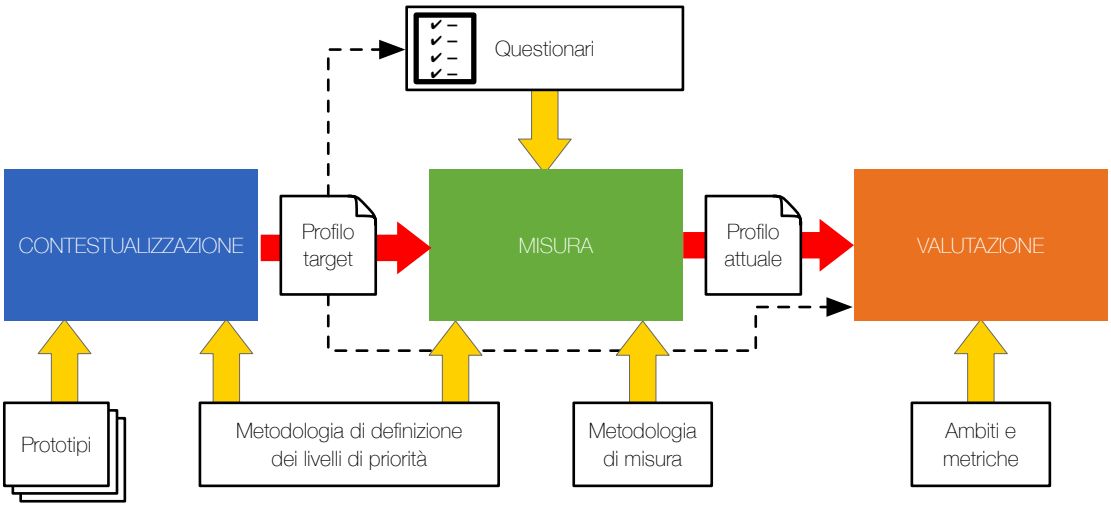

Figura 2 - Overview della metodologia.

FASE 1 - Contestualizzazione. Questa prima fase ha l'obiettivo di contestualizzare il Framework alla realtà di interesse. Tale fase, come dettagliato in [4], può avvalersi di specifici strumenti di supporto denominati prototipi di contestualizzazione, già pubblicati o definiti ad hoc dall'organizzazione. Il prodotto di questa fase sarà un *Profilo Target*, ovvero il riferimento desiderato, al quale tendere e sul quale viene realizzato l'assessment. La sua corretta definizione è quindi funzionale allo svolgimento delle successive due fasi.

FASE 2 - Misura. In questa seconda fase si procede a individuare l'attuale postura di sicurezza cyber dell'organizzazione rispetto a quanto definito nel Profilo Target. Tale processo avviene attraverso interviste a soggetti competenti per le specifiche esigenze di analisi. Il risultato delle interviste viene espresso in termini di *copertura* e *maturità* per ogni controllo individuato.

FASE 3 – Valutazione. Nella terza fase i risultati della fase di misura vengono valutati secondo diversi possibili ambiti. Tale operazione permette di calcolare, a partire dai valori di copertura e maturità di ogni subcategory, delle metriche di interesse per l'ambito stesso. Tali metriche possono considerare in modo opportunamente pesato i contributi delle varie subcategory al raggiungimento di determinati obiettivi per l'ambito stesso, permettendo quindi di analizzare i risultati dell'assessment da differenti punti di vista.

Nel prosieguo di questa sezione vengono dettagliati i passaggi metodologici necessari allo svolgimento di ciascuna fase.

2.1 Contestualizzazione

L'obiettivo di questa prima fase è quello di contestualizzare il Framework alla realtà di interesse e definire su di essa (almeno) un Profilo Target, che rappresenta la postura di sicurezza cyber desiderata. In questa fase viene dunque definito il perimetro entro il quale

l'organizzazione intende muoversi (la contestualizzazione), in termini di postura di sicurezza cyber, e l'obiettivo che l'organizzazione si prefigge di raggiungere (il Profilo Target), che verrà poi confrontato, nella fase di valutazione, con l'attuale postura dell'organizzazione (colta nella fase di misura).

Una contestualizzazione è una selezione delle subcategory del Framework che sono pertinenti per la realtà di interesse. Tale selezione dipende da molti fattori, sia legati in modo specifico all'organizzazione, sia trasversali rispetto alle singole realtà, quali, ad esempio, regolamenti, normative e standard di settore e/o generali. Per questo motivo, la fase di contestualizzazione deve essere affidata a personale con una conoscenza approfondita delle specificità della realtà di interesse e può avvalersi dei prototipi di contestualizzazione eventualmente disponibili.

Nella sezione 2.1.1 verrà descritto il processo di creazione di una contestualizzazione a partire da una selezione dei prototipi di contestualizzazione inerenti alla realtà di interesse. Nella sezione 2.1.2 verrà descritto il processo di definizione del Profilo Target.

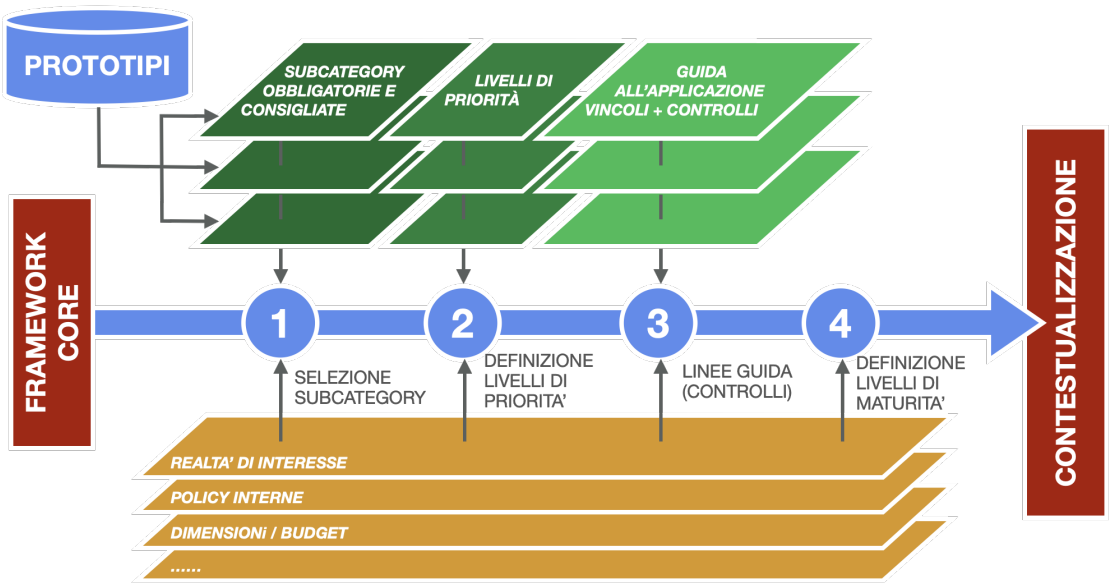

Figura 3 - Processo di contestualizzazione attraverso la combinazione di prototipi.

2.1.1 Combinazione dei prototipi

Dopo aver identificato i prototipi di contestualizzazione di interesse, la creazione della contestualizzazione avviene attraverso un processo che prevede i seguenti passi (si veda Figura 3):

1. **Selezione delle subcategory**: Il processo di selezione è guidato dalla classe associata a ciascuna subcategory nei prototipi selezionati. Quando una stessa subcategory è classificata diversamente in prototipi differenti, la classe risultante della combinazione è quella più alta, secondo il seguente ordinamento "obbligatoria" > "consigliata" > "libera". Tutte le subcategory che risultano "obbligatorie" devono necessariamente essere selezionate se si vuole creare una contestualizzazione coerente con la combinazione dei prototipi selezionati. L'individuazione del sottoinsieme più opportuno di subcategory la cui classificazione risulta "consigliata" o "libera" è a discrezione dell'organizzazione in base alle proprie necessità.

2. **Definizione dei livelli di priorità**: in questa fase la definizione dei livelli di priorità avviene considerando: (i) i livelli di priorità eventualmente assegnati dai prototipi stessi (se più prototipi assegnassero priorità diverse alla stessa subcategory, la priorità risultante dovrebbe essere quella più alta). Tali livelli sono da intendersi come "suggerimenti", in quanto guidati da driver necessariamente non legati al contesto specifico dell'organizzazione. (ii) Informazioni di contesto provenienti dalla specifica realtà che crea la contestualizzazione. Combinando opportunamente i fattori (i) e (ii) deve essere dunque effettuata una prima assegnazione dei livelli di priorità, eventualmente integrabile e revisionabile dopo la fase di misura come descritto nella sezione 2.2.4.
3. **Applicazione linee guida**: applicazione delle linee guida contenute nei documenti di accompagnamento dei prototipi, eventualmente riportanti ulteriori vincoli circa la selezione delle subcategory e la definizione dei livelli di priorità, oltre a controlli associati alle stesse, che possono essere considerati per la fase di definizione dei controlli e del Profilo Target (si veda la sezione successiva).
4. **Definizione livelli di maturità**: eventuale definizione di livelli di maturità per ciascuna subcategory selezionata. La descrizione dei livelli di maturità per ciascuna subcategory definisce i criteri da rispettare per raggiungere i differenti livelli di maturità previsti. Nella presente metodologia i livelli di maturità devono essere coerenti con la scala CMMI, come descritto in sezione 2.1.2.

2.1.2 Definizione controlli e Profilo Target

Il Profilo Target rappresenta il profilo rispetto al quale vengono calcolati i risultati dell'assessment. Come verrà descritto più in dettaglio nella sezione 2.3, infatti, la fase di valutazione effettua un'analisi di gap tra il Profilo Attuale individuato nella fase di misura e uno o più profili target definiti in fase di contestualizzazione.

Un Profilo Target definisce un insieme di controlli di sicurezza che devono essere implementati per raggiungere la postura di sicurezza cyber desiderata mappandoli sulle subcategory del Framework. Come si vedrà nelle sezioni successive la fase di misura è volta a stimare il *grado di copertura* di ciascun controllo e il relativo *livello di maturità* implementativa, permettendo di ottenere il Profilo Attuale dell'organizzazione.

Il grado di copertura associato a un controllo è un valore numerico compreso tra 0 e 1, dove 0 indica una totale mancanza di implementazione del controllo (nessuno degli elementi del controllo risulta neanche parzialmente implementato) e 1 indica una piena implementazione.

Il livello di maturità nell'implementazione del controllo è invece espresso attraverso la scala del Capability Maturity Model Integration (CMMI) [5] che prevede cinque livelli:

Livello CMMI	Descrizione
1 - Iniziale	L'implementazione del controllo è affidata a processi, procedure e soluzioni tecniche con risultati non prevedibili, non documentati, non organizzati e spesso eseguiti *ad-hoc*. Il successo della gestione è affidato alle singole competenze del personale e non all'uso comprovato di processi ben definiti.
2 - Ripetibile	L'implementazione del controllo si avvale di processi, procedure e soluzioni tecniche ben definiti e documentati in ciascuna o in un sottoinsieme delle funzioni dell'organizzazione coinvolte, ma in modo non consistente a livello di normativa aziendale (ciascuna funzione gestisce i propri processi, procedure e soluzioni tecniche in modo indipendente).
3 - Definito	L'implementazione del controllo si avvale di processi, procedure e soluzioni tecniche ben definiti, documentati e standardizzati a livello di normativa aziendale. Le varie funzioni possono specializzare i propri processi, partendo da quelli standardizzati a livello di normativa aziendale.
4 - Gestito	Oltre ad includere gli aspetti del livello di maturità "Definito", sono fissati degli obiettivi quantitativi per quanto riguarda le performance dei processi, delle procedure e delle soluzioni tecniche alla base dell'implementazione del controllo. L'efficacia di processi, procedure e soluzioni tecniche è monitorata e misurata quantitativamente.
5 - Ottimizzato	Oltre ad includere gli aspetti del livello di maturità "Gestito", i processi, le procedure e le soluzioni tecniche alla base dell'implementazione del controllo sono sottoposti a miglioramento continuo in risposta a cambiamenti nell'organizzazione e considerando le esperienze passate.

Più formalmente un profilo è una quadrupla $P = (C, M, X, Y)$ dove:

- $C = \{c_1, \ldots, c_n\}$ è un insieme di controlli;
- M è una matrice le cui righe sono associate ai controlli in C, le colonne rappresentano le subcategory del Framework selezionate nella contestualizzazione, ed ogni cella (i, j) della matrice contiene il valore 1 se il controllo c_i concorre alla implementazione della subcategory s_j, 0 altrimenti;
- $X = \{x_1, \ldots, x_n\}$ è un insieme di valori, uno per ogni controllo in C, tale che il valore x_i, compreso tra 0 ed 1, rappresenta il grado di copertura con cui è implementato il controllo c_i;
- $Y = \{y_1, \ldots, y_n\}$è un insieme di valori, uno per ogni controllo in C, tale che il valore y_i, intero compreso tra 1 e 5, rappresenta il livello di maturità con cui è implementato il controllo c_i.

Un Profilo Target P^T è un profilo in cui sono elencati in C i controlli che si intendono implementare per raggiungere il livello di sicurezza desiderato, in coerenza con la contestualizzazione. Per ciascuno di questi controlli deve essere definito in X un grado di

copertura desiderato, che, in assenza di altri vincoli, dovrebbe sempre essere 1 (il controllo deve essere implementato completamente). In un Profilo Target l'insieme Y, non è invece significativo. Il principale razionale dietro questa scelta risiede nel fatto che l'implementazione di un controllo deve rimanere efficace rispetto allo stesso anche al minimo livello di maturità. Chiaramente, livelli di maturità superiori renderanno più efficiente l'implementazione del controllo. Un secondo motivo risiede nel fatto che realtà differenti potrebbero necessitare di livelli di maturità differenti, ed indicarne uno solo per un profilo target potrebbe non catturare in modo corretto le differenti realtà di applicazione, anche all'interno di uno stesso settore.

2.2 Misura

La fase di misura viene svolta dall'assessor sulla base della contestualizzazione definita nella fase precedente, e del relativo Profilo Target

Partendo da questi 2 input, l'assessor deve eseguire i seguenti 4 passi, di cui i primi 3 obbligatori e l'ultimo opzionale:

Passo 1: Creazione del questionario

Passo 2: Somministrazione del questionario

Passo 3: Consolidamento del questionario e ottenimento del Profilo Attuale

Passo 4: Rimodulazione dei livelli di priorità (opzionale)

Nel seguito sono trattati in dettaglio i singoli passi.

2.2.1 Creazione del questionario

In questa fase l'assessor definisce il questionario da somministrare alle diverse figure individuate. La creazione del questionario muove a partire dal Profilo Target. Per ogni controllo l'assessor definisce una o più domande volte a misurare il grado di copertura del controllo stesso e la relativa maturità. Il questionario deve definire per ogni controllo i seguenti campi:

- **risposta:** campo necessario a riportare le informazioni collezionate durante la somministrazione del questionario. Il contenuto è testo libero, inserito secondo la sensibilità dell'intervistatore.
- **note copertura:** campo necessario a riportare, in forma testuale, informazioni circa lo stato di copertura del controllo da parte dell'assessor.
- **grado di copertura**: campo necessario a riportare, in forma numerica, il grado di copertura del controllo (quanto il controllo è soddisfatto). Tale grado deve essere espresso con un valore coerente con la seguente scala qualitativa:

Grado di copertura	Descrizione	Criterio qualitativo associato
0	**Nullo**	Il controllo non è implementato in alcuna sua parte.
0.2	**Insufficiente**	Implementazione iniziale di alcuni aspetti fondamentali del controllo, o implementazione di soli aspetti marginali.
0.4	**Iniziale**	Il controllo risulta parzialmente implementato nei suoi aspetti fondamentali, ma gli elementi mancanti non rendono l'implementazione efficace rispetto agli obiettivi.
0.6	**Incompleto**	Il controllo risulta parzialmente implementato e gli elementi implementati riguardano tutti gli aspetti fondamentali. L'implementazione risulta parzialmente efficace rispetto agli obiettivi.
0.8	**Avanzato**	Il controllo risulta implementato ad eccezione di qualche elemento marginale.
1	**Completo**	Controllo completamente implementato.

L'adozione di una scala standard comune aiuta a rendere il confronto dei risultati di diversi assessment più oggettivo, eliminando quelle differenze che emergono quando vengono utilizzate scale a granularità diversa.

- **note maturità**: campo in cui riportare, in forma testuale, dettagli circa lo stato di maturità con cui è implementato un controllo o parte di esso.

- **livello di maturità**: campo necessario a riportare il livello di maturità per l'intero controllo. La valorizzazione di questo campo è basata sui cinque livelli definiti dal Capability Maturity Model Integration (CMMI). Nel caso in cui i controlli abbiano copertura nulla, il campo del livello di maturità non può essere valorizzato e, dunque, deve essere considerato come "Non Applicabile" (N/A).

- **evidenze**: in tale campo verranno riportate le evidenze a supporto del grado di copertura e del livello di maturità stimati, in termini di riferimenti a documenti, informazioni tecniche di rilievo o eventuali valutazioni quantitative utili per la fase di creazione del Profilo Attuale.

- **note**: campo in cui riportare eventuali ulteriori note dell'assessor.

2.2.2 Somministrazione del questionario

In questa fase l'assessor somministra il questionario alle persone precedentemente identificate come referenti. La modalità di svolgimento di questa fase riveste una particolare importanza: qualora i risultati dell'intervista fossero parziali o poco accurati rispetto alle domande poste dall'assessor, le valutazioni effettuate a margine dell'intero processo di applicazione della metodologia risulterebbero poco affidabili. La correttezza delle informazioni ottenute nel corso dell'intervista rappresenta, pertanto, un elemento di particolare importanza.

Durante la somministrazione, l'assessor, per ogni controllo riportato nel questionario, effettuerà una o più domande ai soggetti referenti al fine di cogliere il maggior numero di dettagli possibili circa il controllo in questione. Il numero di referenti intervistati può variare a seconda della contestualizzazione definita e, dunque, delle subcategory selezionate per l'assessment. In particolare, l'individuazione dei referenti può essere effettuata a margine di un'analisi delle tematiche affrontate da ciascun quesito. Ad esempio, le domande relative a controlli afferenti a una subcategory dedicata alla formazione del personale dell'organizzazione possono essere rivolte a un referente dell'ufficio Risorse Umane. Informazioni rispetto a controlli di natura prettamente tecnica possono invece essere richieste ai Responsabili del Reparto IT, così come elementi di natura normativa possono essere colti in maniera efficace da un incontro con un referente dell'Ufficio Legale o Compliance.

Un'accurata individuazione degli interlocutori aiuta a ridurre la possibilità di incorrere nelle problematiche precedentemente elencate. Anche di fronte a soggetti competenti rispetto alle tematiche trattate nell'intervista è consigliabile procurarsi e analizzare, quando possibile, una o più evidenze per corroborare, migliorare o rettificare la risposta ricevuta. Tali evidenze possono essere ricavate sia a partire da attività di sicurezza informatica quali Vulnerability Assessment e/o Penetration Test sia a partire da un'analisi documentale svolte in parallelo alle fasi di intervista.

Durante questa fase l'assessor riporterà nel campo dedicatogli elementi fondamentali della risposta, in forma testuale, e chiederà ogni volta al soggetto referente di fornire una o più evidenze a sostegno delle informazioni comunicate, da riportare nel campo "evidenze". L'assessor potrà considerare, inoltre, l'eventuale assenza o non conoscenza di evidenze a supporto di quanto dichiarato dal soggetto referente. La rilevazione di tali evidenze rappresenta un metodo utile per rendere maggiormente oggettiva la fase di somministrazione del questionario e di raccolta delle risposte, in quanto incentivano l'assessor e l'intervistato a concentrarsi su elementi fattivamente riconoscibili che supportino la valutazione proposta. La loro eventuale assenza, in ogni caso, non impedisce l'applicazione della procedura di assessment, ma impatta potenzialmente solo la qualità dei risultati. Tuttavia, come si è detto, quest'ultima risulta decisiva per l'affidabilità delle valutazioni effettuate a valle dell'assessment.

Durante l'intervista l'assessor potrà in ogni momento riportare note circa dettagli di interesse emersi durante l'intervista o proprie valutazioni circa le risposte fornite dal soggetto referente.

Al termine dell'intervista, per ciascun controllo, l'assessor riporterà anche un grado di copertura preliminare, in forma testuale, nel campo "note copertura".

In merito al numero di domande da effettuare per ogni controllo, questo varia in base alla complessità dello stesso. L'assessor dovrebbe cercare di cogliere attraverso le domande tutti gli aspetti principali relativi al controllo.

Durante l'intervista l'assessor dovrà inoltre acquisire dettagli in merito al grado di maturità con cui il controllo, o parte di esso, è implementato. Queste informazioni saranno riportate, in forma testuale, nel campo "note maturità".

Al termine dell'intervista, l'assessor assegnerà un valore sia per il campo "grado di copertura" sia per il campo "livello di maturità" del controllo.

2.2.3 Consolidamento del questionario ed estrazione del Profilo Attuale

A seguito dell'intervista l'assessor revisionerà i risultati ottenuti al fine di specificare in forma definitiva il grado di copertura e il livello di maturità di ogni controllo. L'output di questa fase è il Profilo Attuale dell'organizzazione, rappresentato dall'insieme dei livelli di copertura e maturità dei controlli.

Formalmente il risultato finale è un Profilo Attuale $P^A = (C, M, X^A, Y^A)$, dove C e M sono, rispettivamente, l'insieme dei controlli e la matrice che li mappa sulle subcategory del Framework, X^A è l'insieme dei livelli di copertura definiti sulla base dell'esito delle interviste e Y^A è l'insieme dei livelli di maturità associati ai controlli definiti sulla base dell'esito delle interviste. Si noti che l'insieme di controlli C e il relativo mapping M sono gli stessi del Profilo Target P^T.

2.2.4 Rimodulazione dei livelli di priorità

Una volta ottenuto il Profilo Attuale dell'organizzazione, l'assessor potrà eventualmente procedere alla rimodulazione dei livelli di priorità della contestualizzazione.

Questa fase non è strettamente obbligatoria ai fini dell'assessment, in quanto questi livelli sono già stati definiti in fase di contestualizzazione. Tuttavia, nuovi elementi emersi in fase di misura potrebbero richiedere una revisione degli stessi. Qualora l'organizzazione non lo ritenesse necessario, potrà scegliere di mantenere inalterati questi livelli, confermandoli.

Qualora invece, dall'analisi dello stato dei controlli di una subcategory, si evincesse che il livello di priorità scelto nella contestualizzazione non sia adeguato (esempio: basso grado del livello attuale di copertura e maturità e/o costo molto elevato in termini di risorse per raggiungere quanto definito nel Profilo Target), questo potrà essere modificato nella contestualizzazione.

Diverse metodologie possono essere utilizzate per legare i risultati collezionati nella fase di misura all'eventuale rimodulazione dei livelli di priorità. L'Appendice B descrive una possibile metodologia strutturata.

2.3 Valutazione

La fase di valutazione ha l'obiettivo di analizzare il gap tra il Profilo Attuale e il Profilo Target, o più profili target, definiti in fase di contestualizzazione.

L'analisi di gap fornisce, attraverso opportune metriche definite in seguito, una misura della postura di sicurezza cyber attuale dell'organizzazione rispetto al target definito.

È importante notare che la postura di sicurezza cyber definita nella fase di valutazione è una misura relativa e non assoluta. Infatti, poiché l'analisi di gap viene effettuata rispetto a un Profilo Target, i risultati saranno diversi a seconda del profilo considerato.

L'input della fase di valutazione è costituito dal Profilo Target, così come definito in fase di contestualizzazione, e dal Profilo Attuale ottenuto dalla fase di misura.

L'output della fase di valutazione, e quindi il risultato dell'intero assessment, è espresso tramite le *metriche* definite nella sezione 2.3.2, aggregate secondo diversi criteri e proiettate su diversi ambiti (es. risk management, compliance, ecc.), descritti nella sezione 2.3.1.

2.3.1 Ambiti

Gli ambiti permettono di interpretare i risultati dell'assessment rispetto a differenti punti di vista all'interno dell'organizzazione. Ad esempio, l'ufficio che si occupa di compliance sarà interessato più agli aspetti connessi alla cybersecurity che riguardano l'ottemperanza alla normativa, mentre l'ufficio risk management potrebbe voler misurare l'efficacia delle misure adottate rispetto alla riduzione del rischio associato alle minacce cui l'organizzazione è esposta.

Ciascuno di questi punti di vista può essere colto durante la fase di valutazione attraverso il concetto di ambito. Un ambito di valutazione definisce un insieme di elementi di interesse, indica quali parti del Profilo Target sono significative per l'ambito e quantifica la rilevanza di ogni controllo su ciascun elemento di interesse.

Da un punto di vista più formale un ambito $A = (E, W)$ definisce:

- Un insieme E di elementi omogenei rispetto ai quali viene valutato il risultato dell'assessment (es. subcategory del Framework, elementi normativi, impatti delle minacce e relative probabilità di accadimento, ecc.);
- Un'assegnazione di pesi tra i controlli del Profilo Target P^T e gli elementi dell'insieme E, sotto forma di una matrice W, in cui l'elemento W_{ij} è un numero tra 0 e 1 indicante quanto il controllo i-esimo è rilevante rispetto all'elemento j-esimo di E, dove 0 indica una totale mancanza di pertinenza rispetto alle tematiche dell'elemento e 1 rappresenta una totale pertinenza.

Di seguito si elencano tre possibili ambiti di interesse per un'organizzazione. Si specifica che, in ogni caso, è facoltà delle diverse realtà organizzative identificare i propri ambiti secondo necessità.

Ambito Framework - Questo ambito permette di valutare quanto l'attuale postura di sicurezza cyber dell'organizzazione sia distante dagli obiettivi posti dal Profilo Target. Considerato che la metodologia di assessment descritta in questo documento è incentrata sul Framework Nazionale per la Cybersecurity e la Data Protection, e che la valutazione secondo

questo ambito non richiede ulteriori elementi rispetto quanto già definito, la valutazione secondo l'ambito Framework dovrebbe essere presa in considerazione per qualsiasi applicazione della metodologia.

In termini formali, in questo ambito E coincide con l'insieme delle subcategory del Framework selezionate nella contestualizzazione. La matrice W è definita, coerentemente con la matrice M così come definita nel Profilo Target P^T, in modo tale che il peso W_{ij} indichi quanto il controllo i-esimo è centrale rispetto alle tematiche della subcategory j-esima.

Ambito Risk Management - Questo ambito permette di analizzare quanto l'attuale postura di sicurezza cyber dell'organizzazione sia coerente rispetto agli obiettivi di mitigazione dei rischi associati alle minacce a cui la stessa organizzazione è esposta. Tale ambito rappresenta, pertanto, uno strumento di supporto ai processi di cybersecurity risk management. La definizione degli elementi di interesse di questo ambito dovrebbe essere strettamente legata al Risk Assessment Framework adottato dall'organizzazione. Ad esempio, l'ambito Risk Management può essere utilizzato per valutare quanto il Profilo Attuale sia coerente con l'obiettivo di mitigare i rischi identificati sia dal punto di vista della probabilità di accadimento sia del loro impatto.

Più formalmente, E è un insieme costruito a partire dai rischi associati alle minacce rilevanti per l'organizzazione. Gli elementi di E corrispondono, in questo ambito, agli impatti associati all'occorrenza delle minacce e le probabilità di accadimento delle stesse. Ad esempio, $e_j, e_{j+1} \in E$, dove e_j è l'impatto associato alla minaccia k-esima ($k = j/2$) e e_{j+1} è la relativa probabilità di accadimento). Il peso W_{ij} nella matrice W indica quanto il controllo i-esimo è centrale rispetto alle misure necessarie a contenere gli impatti associati alla minaccia k-esima, mentre W_{ij+1} indica quanto il controllo i-esimo è centrale rispetto alle misure necessarie a ridurre la probabilità che la minaccia k-esima occorra.

Ambito Compliance - Questo ambito permette di valutare quanto il Profilo Attuale sia allineato rispetto ai requisiti posti dalle normative di riferimento in materia di cybersecurity del settore in cui opera l'organizzazione. Tale valutazione è abilitata a condizione che il Profilo Target sia stato costruito in modo coerente con la normativa. Tale condizione può essere soddisfatta strutturando la contestualizzazione sulla base di opportuni prototipi che colgono gli aspetti di interesse della normativa di riferimento (si veda la sezione 2.1).

In termini formali, in questo ambito gli elementi di E corrispondono ad aspetti normativi rispetto ai quali si vuole valutare il grado di ottemperanza (ad esempio regolamenti, singoli articoli, ecc.). Il peso W_{ij} indica quanto il controllo i-esimo è rilevante rispetto all'ottemperanza all'elemento normativo j-esimo.

2.3.2 Metriche

Le metriche rispetto alle quali è valutato il risultato dell'assessment possono essere calcolate per ogni ambito e sono definite a livello di elemento dell'insieme E.

Tali metriche sono le seguenti:

- *score*: permette di valutare il grado di copertura nell'implementazione delle misure necessarie a soddisfare un determinato elemento dell'insieme E (es.: copertura di una subcategory nell'ambito framework, del rischio associato ad una minaccia nell'ambito

risk management, grado di ottemperanza a un elemento normativo nell'ambito compliance).

- *maturità*: permette di valutare la distribuzione del grado di maturità con cui le suddette misure sono implementate attraverso i diversi controlli.

La Figura 4 evidenzia gli input della fase di valutazione, eseguita rispetto ad uno specifico ambito $A = (E, W)$, e il relativo output. In figura sono evidenziati (i) il Profilo Target, riportante la copertura desiderata per ciascun controllo (nell'esempio in figura possiamo notare come nel Profilo Target non sia di interesse il controllo 2, motivo per cui la sua copertura è posta a 0), (ii) il Profilo Attuale, riportante i valori di copertura e maturità rilevati in fase di misura per ciascun controllo, (iii) l'ambito A (la cui tabella in figura rappresenta la matrice dei pesi W, con gli elementi di E come colonne e i controlli come righe) e (iv) il risultato della valutazione che riporta le metriche di score e maturità per ciascun elemento dell'ambito A.

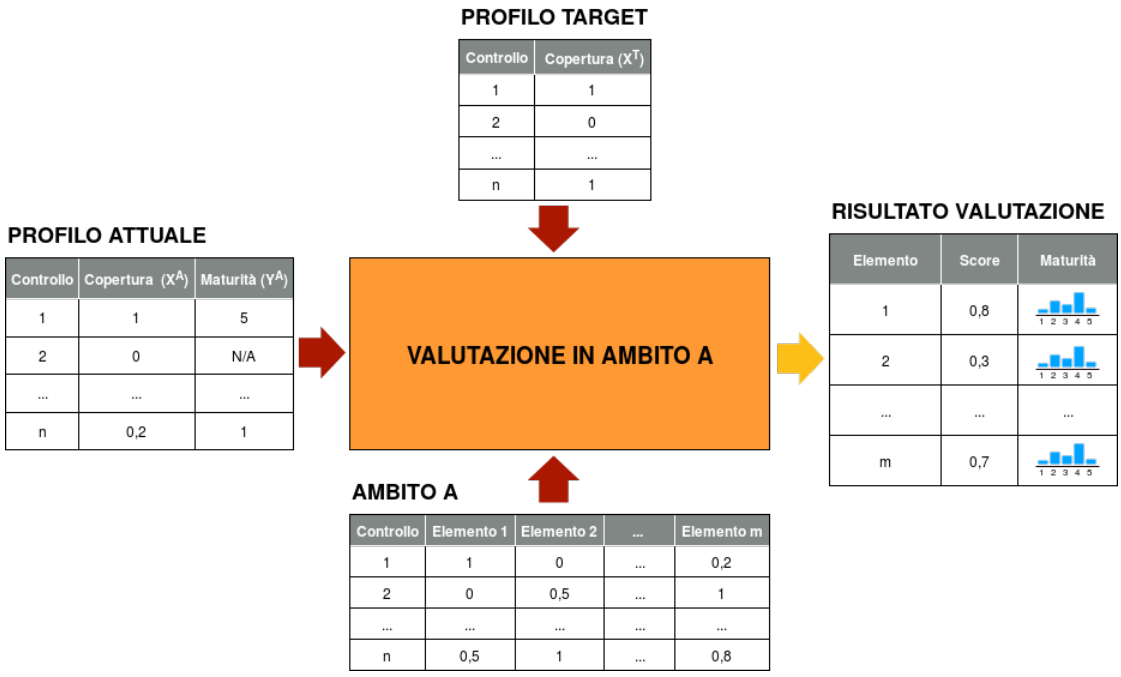

Figura 4 - Fase di valutazione eseguita per un generico ambito A.

Come dettagliato in seguito, entrambe le metriche possono essere aggregate per sottoinsiemi arbitrari di E (es. category, function, intero Framework, insiemi omogenei di elementi normativi, ecc.).

Score

Lo score è una misura del grado di copertura di un elemento dell'ambito rispetto ad un Profilo Target. Si tratta di una misura tra 0 e 1, dove 1 indica che l'elemento risulta completamente coperto (rispetto a quanto richiesto dal Profilo Target) e 0 indica che nessun aspetto relativo al Profilo Target in merito a quell'elemento è stato implementato.

In particolare, lo score è calcolabile per ogni elemento di un ambito (ad esempio, nell'ambito framework è calcolabile lo score di ogni subcategory). Lo score di un elemento e_j è dato dalla somma pesata della copertura dei controlli che incidono su e_j secondo i pesi definiti nella matrice W.

Formalmente, lo score è calcolato con la seguente formula:

$$score(e_j) = \frac{\sum_{i=1}^{n} (x_i^A / x_i^T) \cdot W_{ij}}{\sum_{i=1}^{n} W_{ij}}$$

dove e_j è l'elemento j-esimo di E, x_i^A è la copertura *attuale* del controllo i-esimo (contenuta nel Profilo Attuale P^A), $x_i^T > 0$ è la copertura *desiderata* del controllo i-esimo (contenuta nel Profilo Target P^T) e W_{ij} è il peso del controllo i-esimo rispetto all'elemento j-esimo (definito nell'ambito).

ESEMPIO 1

Supponiamo di aver definito un ambito $A = (E, W)$ in cui W è la seguente matrice (i punti di sospensione indicano un valore non significativo ai fini dell'esempio):

	e_1	...	e_7	...	e_m
c_1	...	...	0	...	...
c_2	...	...	**1**	...	...
c_3	...	...	**0.8**	...	...
c_4	...	...	0	...	...
c_5	...	...	**0.2**	...	...
c_6	...	...	0	...	...
...	...	...	...	...	...
c_n	...	...	0	...	...

Dati un Profilo Target e un Profilo Attuale, supponiamo di voler calcolare lo score dell'elemento $e_7 \in E$.

Poiché soltanto i controlli c_2 , c_3 e c_5 hanno pesi non-nulli nella colonna relativa all'elemento e_7 nella matrice W, è evidente che solo tali elementi contribuiranno al calcolo dello score dell'elemento e_7 .

Supponiamo che il Profilo Target richieda che tutti e tre questi controlli siano pienamente implementati (ossia $x_2^T = 1,\ x_3^T = 1, x_5^T = 1$). Inoltre, supponiamo che a seguito della fase di misura si sia determinato che il controllo c_2 ha un grado di copertura "nullo" (x_2^A= 0), c_3 un grado di copertura "completo" (x_3^A= 1) e c_5 un grado di copertura "incompleto" (x_5^A= 0.6).

In tal caso lo score dell'elemento e_7 sarebbe dato da:

$$score(e_7) = \frac{(x_2^A / x_2^T) \cdot W_{2,7} + (x_3^A / x_3^T) \cdot W_{3,7} + (x_5^A / x_5^T) \cdot W_{5,7}}{W_{2,7} + W_{3,7} + W_{5,7}}$$

$$= \frac{0 \cdot 1 + 1 \cdot 0.8 + 0.6 \cdot 0.2}{1 + 0.8 + 0.2} = \frac{0.92}{2} = 0.46$$

Si noti che nella formula sono stati omessi tutti i termini per cui $W_{i,7} = 0$, poiché questi non portano alcun contributo al risultato finale.

Lo score può essere aggregato a livello di un qualsiasi sottoinsieme $\hat{E} \subseteq E$(ad esempio, nell'ambito framework $\hat{E}$ potrebbe corrispondere a un'intera category, function o anche all'intera contestualizzazione), secondo la formula:

$$score(\hat{E}) = \frac{\sum_{e_j \in \hat{E}} \quad \sum_{i=1}^{n} \quad (x_i^A / x_i^T) \cdot W_{ij}}{\sum_{e_j \in \hat{E}} \quad \sum_{i=1}^{n} \quad W_{ij}}$$

Si noti che la formula di $score(e_j)$ è semplicemente un caso particolare della formula di $score(\hat{E})$ in cui $\hat{E} = \{e_j\}$.

Maturità

Dato un elemento e_j, la maturità implementativa è data da un vettore m_j a cinque elementi in cui ogni elemento è associato ad un livello del CMMI. L'elemento k-esimo di m_j (d'ora in avanti indicato con la notazione $m_j[k]$) rappresenta la proporzione di controlli associati alla subcategory (secondo il peso dato dal Profilo Target) che sono implementati al livello di maturità k.

L'elemento $m_j[k]$ è definito dalla seguente formula:

$$m_j[k] = \frac{\sum_{i \in L_k(C)} \quad W_{ij}}{\sum_{i=1}^{n} \quad W_{ij}}$$

dove $L_k(C)$ è l'insieme di controlli del Profilo Target per i quali nel Profilo Attuale è stato assegnato il livello di maturità k (o più formalmente $L_k(C) = \{c_i \in C \mid y_i^A = k\}$).

ESEMPIO 2

Supponiamo di aver definito un ambito $A = (E, W)$ in cui W è la seguente matrice matrice (i punti di sospensione indicano un valore non significativo ai fini dell'esempio):

	e_1	...	e_8	...	e_m
c_1	...	...	**0.6**	...	...
c_2	...	...	**0.3**	...	...
c_3	...	...	**1**	...	...
c_4	...	...	**0.9**	...	...
c_5	...	...	**0.2**	...	...
c_6	...	...	0	...	...
...	...	...	...	...	...
c_n	...	...	0	...	...

Dato un Profilo Attuale, supponiamo di voler calcolare il vettore maturità dell'elemento $e_8 \in E$. Poiché soltanto i controlli da c_1 a c_5 hanno pesi non-nulli nella colonna relativa all'elemento e_8 nella matrice W, solo tali elementi contribuiranno al calcolo del vettore maturità per l'elemento e_8.

Supponiamo che a seguito della fase di misura si siano determinati i seguenti livelli di maturità:

Controllo	Livello di maturità
c_1	2 - Ripetibile ($y_1^A = 2$)
c_2	3 - Definito ($y_2^A = 3$)
c_3	1 - Iniziale ($y_3^A = 1$)
c_4	N/A (controllo non implementato)
c_5	1 - Iniziale ($y_3^A = 1$)

La prima componente del vettore di maturità m_8 è data dalla formula:

$$m_8[1] = \frac{\sum_{i \in L_1(C)} W_{i,8}}{\sum_{i=1}^{n} W_{i,8}} = \frac{\sum_{i \in \{3,5\}} W_{i,8}}{\sum_{i=1}^{n} W_{i,8}}$$

$$= \frac{W_{3,8} + W_{5,8}}{W_{1,8} + W_{2,8} + W_{3,8} + W_{4,8} + W_{5,8}} = \frac{1 + 0.2}{0.6 + 0.3 + 1 + 0.9 + 0.2}$$

$$= 0.4$$

Dove nella formula sono stati omessi tutti i termini per cui $W_{i,8}$= 0, poiché non porterebbero alcun contributo al risultato finale (si noti infatti che, in generale $L_1(C) \supseteq \{3,5\}$, tuttavia, eventuali altri elementi di $L_1(C)$ sarebbero associati a pesi nulli nella colonna relativa all'elemento e_8 in W).

Analogamente si procede a calcolare tutte le altre componenti di m_8:

$$m_8[2] = \frac{\sum_{i \in L_2(C)} W_{i,8}}{\sum_{i=1}^{n} W_{i,8}} = \frac{\sum_{i \in \{1\}} W_{i,8}}{\sum_{i=1}^{n} W_{i,8}} = \frac{0.6}{3} = 0.2$$

$$m_8[4] = m_8[5] = 0$$

Si ha perciò che il vettore $m_8 = (0.4, 0.2, 0.1, 0, 0)$ indica che il 40% dell'elemento e_8 è implementato al livello di maturità "1 - Iniziale", il 20% al livello di maturità "2 - Ripetibile" e il 10% al livello di maturità "3 - Definito". Inoltre, nessuna porzione dell'elemento è implementata ai livelli di maturità superiori. Si noti inoltre che rimane un 30% scoperto, dovuto al fatto che il controllo c_4 non risulta implementato e dunque non ha un livello di maturità (N/A). Tale elemento contribuisce infatti per il 30% (0.9/3) al peso totale dei controlli che insistono sull'elemento e_8.

Anche la maturità, come lo score, può essere aggregata per qualsiasi sottoinsieme $\hat{E} \subseteq E$:

$$m_{\hat{E}}[k] = \frac{\sum_{i \in L_k(C)} \sum_{e_j \in \hat{E}} W_{ij}}{\sum_{e_j \in \hat{E}} \sum_{i=1}^{n} W_{ij}}$$

Si noti che la formula di $m_j[k]$ è semplicemente un caso particolare della formula di $m_{\hat{E}}[k]$ in cui $\hat{E} = \{e_j\}$.

2.3.3 Proiezione delle valutazioni sul Framework

Come visto nella precedente sezione, gli ambiti permettono di valutare la postura di sicurezza cyber di un'organizzazione rispetto a differenti punti di vista. Tale approccio permette alle diverse funzioni (es. compliance, risk management, ecc.) di effettuare un'analisi diversificata della postura di sicurezza cyber e del gap rispetto al profilo desiderato. Ciò è possibile pesando i controlli in base al grado di rilevanza per gli elementi di interesse dell'ambito selezionato. Da un punto di vista operativo può risultare poi utile ri-proiettare i risultati di tali analisi sul Framework, così da ottenere uno strumento operativo che possa supportare anche le

successive fasi di gestione della cybersecurity (es. pianificazione e prioritizzazione degli interventi volti a ridurre il gap col Profilo Target).

Una proiezione di un dato ambito A sul Framework è ottenuta calcolando le metriche score e maturità usando la matrice dei pesi dell'ambito framework (invece che quella dell'ambito A), ma considerando solo i controlli di interesse per l'ambito A (cioè quelli che hanno un peso non-nullo associato ad almeno un elemento di A). La proiezione di un ambito qualsiasi sull'ambito framework A, quindi, agisce come una sorta di filtro sull'ambito framework che considera solo il sottoinsieme di controlli inerenti per A.

Ad esempio, la funzione compliance di una organizzazione potrebbe voler effettuare un'analisi sugli elementi di una specifica normativa, per esempio sul GDPR. Attraverso l'ambito compliance, con un'opportuna configurazione dei pesi, è possibile calcolare le metriche di score e maturità rispetto agli elementi di tale normativa (es. articoli, sezioni, capi, ecc.) e aggregarle a livelli gerarchici superiori fino a calcolare lo score e maturità dell'intero Regolamento, così da ottenere una misura globale del grado di implementazione e di aderenza ai requisiti del Regolamento medesimo. Una proiezione dell'ambito GDPR sul Framework si ottiene calcolando score e maturità per le subcategory del Framework usando la matrice dei pesi dell'ambito framework, ma considerando solo quei controlli che incidono su almeno un elemento del GDPR.

Da un punto di vista formale, una proiezione di una valutazione svolta in un dato ambito sul Framework viene calcolata come segue. Sia $A = (E^A, W^A)$ un qualsiasi ambito e $F = (E^F, W^F)$ l'ambito framework. Scelto un qualsiasi sottoinsieme di elementi $\hat{E}^A \subseteq E^A$ le misure di score e di maturità possono essere ri-proiettate sul Framework attraverso le seguenti formule:

$$score(\hat{E}^F) = \frac{\sum_{e_j \in \hat{E}^F} \quad \sum_{c_i \in \hat{C}} \quad (x_i^A \,/\, x_i^T) \cdot W_{ij}^F}{\sum_{e_j \in \hat{E}^F} \quad \sum_{c_i \in \hat{C}} \quad W_{ij}^F}$$

$$m_{\hat{E}^F}[k] = \frac{\sum_{i \in L_k(\hat{C})} \quad \sum_{e_j \in \hat{E}^F} \quad W_{ij}^F}{\sum_{e_j \in \hat{E}^F} \quad \sum_{c_i \in \hat{C}} \quad W_{ij}^F}$$

Dove $\hat{E}^F$ è un qualsiasi sottoinsieme di E^F(es. singola subcategory, category, function, intero Framework) e $\hat{C} = \{c_i \in C \mid \exists\, e_j \in \hat{E}^A, W_{ij}^A > 0\}$ è l'insieme dei controlli che hanno almeno un peso non-nullo associato agli elementi di $\hat{E}^A$.

In altre parole, il calcolo di $score(\hat{E}^F)$ è equivalente al calcolo dello score nell'ambito framework, in cui vengono esclusi i controlli che hanno solo pesi nulli rispetto agli elementi $\hat{E}^A$ dell'ambito considerato. Lo stesso vale per il calcolo della maturità.

2.4 Attori coinvolti

Per una corretta applicazione della metodologia si suggerisce di identificare alcuni attori a cui assegnare specifiche responsabilità inerenti alle attività delle diverse fasi. La seguente lista ne elenca i principali, lasciando all'organizzazione che adotta e applica la metodologia il compito di raffinarla e integrarla anche sulla base delle proprie specifiche caratteristiche.

Owner del processo - È il responsabile dell'applicazione della metodologia di assessment. Tra le attività previste dal suo ruolo è possibile identificare:

- Assegnazione dei ruoli previsti dal processo di implementazione ed esecuzione della metodologia.
- Programmazione e supervisione dello svolgimento del processo.
- Coordinamento delle attività di definizione dei contenuti per la fase di misura.

Responsabili di ambito - Per ciascun ambito di interesse della fase di valutazione, è opportuno definire un responsabile che individui gli obiettivi della valutazione e definisca di conseguenza gli specifici dettagli relativi all'ambito di interesse.

Assessor - L'assessor definisce e somministra i questionari durante la fase di misura. Identifica, in accordo con l'owner del processo, le modalità di svolgimento della fase di misura e i soggetti da intervistare durante la stessa. È sua responsabilità svolgere le attività di misura in modo che i risultati della stessa siano il più possibile aderenti alla realtà misurata. Coerentemente con la struttura organizzativa interna, potrebbe essere opportuno individuare più assessor dedicati a specifici step della fase di misura. Per semplicità, nel prosieguo del presente documento si ipotizza il caso in cui viene identificato un unico assessor.

3 Confrontabilità delle misure

La possibilità di confrontare i risultati di due assessment risulta utile per un'organizzazione per diversi motivi, tra cui:

- Misurare il progresso verso il Profilo Target attraverso assessment periodici.
- Confrontare la propria postura di sicurezza cyber rispetto a quella di altre organizzazioni (ad esempio, rispetto ad una baseline del proprio settore).

In entrambi i casi la confrontabilità dei risultati dell'assessment richiede che il Profilo Target rispetto al quale vengono calcolate le metriche sia comune ai due assessment. Ad esempio, nel primo caso, un'organizzazione potrebbe voler misurare periodicamente i progressi ottenuti durante l'applicazione di un piano di interventi finalizzato al raggiungimento di un determinato Profilo Target. In tal caso, i risultati degli assessment sarebbero confrontabili nella misura in cui il Profilo Target non venga modificato. Una volta definito un nuovo target i successivi assessment non produrrebbero risultati direttamente confrontabili con quelli ottenuti con il precedente target.

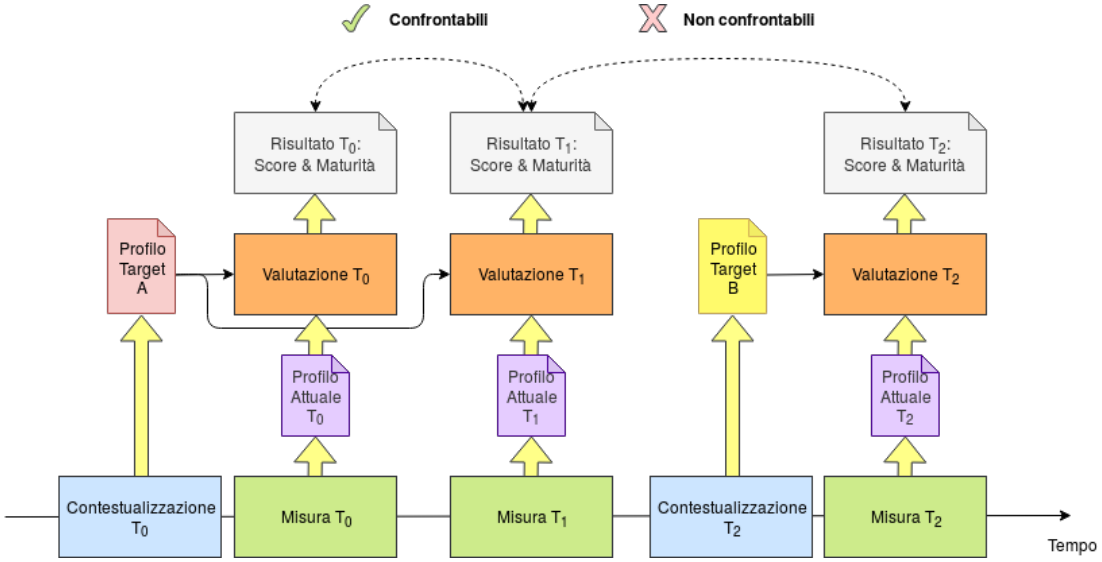

Figura 5 - Confrontabilità tra assessment successivi.

Si consideri, ad esempio, la situazione rappresentata in Figura 5. Un'organizzazione ad un certo istante temporale T_0 effettua la fase di contestualizzazione andando anche a definire il Profilo Target (Profilo Target A). Successivamente esegue la fase di misura, definendo il suo Profilo Attuale (Profilo Attuale T_0), e quella di valutazione ottenendo una analisi del gap tra il Profilo Attuale e il Profilo Target. In un secondo momento, all'istante T_1, la stessa organizzazione decide di voler ri-eseguire le fasi di misura e valutazione per determinare il progresso ottenuto nell'arco temporale che va da T_0 a T_1. Effettuare la fase di valutazione rispetto allo stesso profilo comune (Profilo Target A) abilita la confrontabilità dei risultati. All'istante T_2 l'organizzazione decide di voler ridefinire il proprio target ri-eseguendo la fase di contestualizzazione e producendo il Profilo Target B. La fase di valutazione eseguita su questo nuovo Profilo Target produrrà quindi un risultato che non è confrontabile con quelli ottenuti in T_0 a T_1.

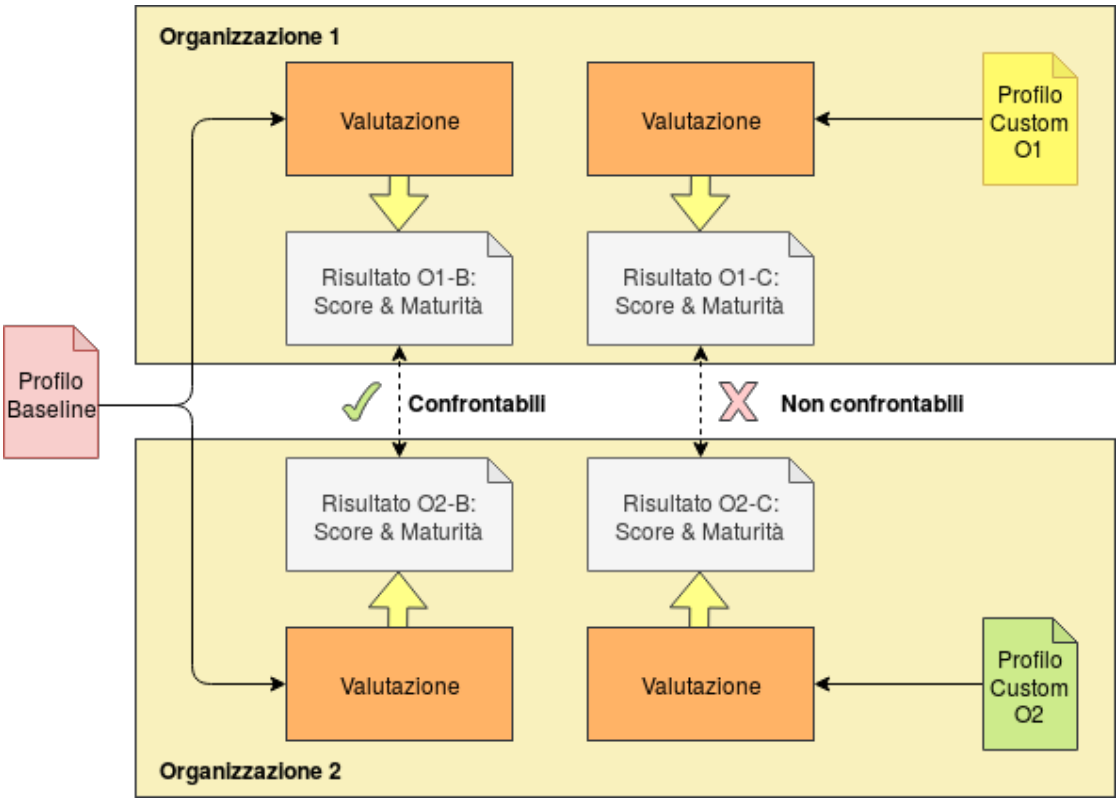

Figura 6 - Confrontabilità tra assessment eseguiti da diverse organizzazioni.

Nel caso di più organizzazioni, il confronto dei risultati dell'assessment è possibile se la valutazione viene effettuata rispetto a un Profilo Target condiviso tra le organizzazioni, come, ad esempio, un profilo che rappresenti una baseline di settore (cfr. Figura 6, Profilo Baseline). Il confronto non è invece possibile quando le organizzazioni decidono di valutarsi rispetto a profili target non condivisi (Profili Custom in Figura 6).

La condivisione di un Profilo Target è solo uno dei fattori abilitanti per la confrontabilità dei risultati di un assessment, ma non è di per sé sufficiente. Le metriche di score e maturità, infatti, sono calcolate rispetto agli ambiti e, in particolare, il calcolo è determinato dai parametri di questi ultimi. Ciò comporta che la confrontabilità dei risultati di due assessment è possibile esclusivamente sugli ambiti condivisi tra le organizzazioni.

Riassumendo, quindi, la confrontabilità tra due assessment è possibile, rispetto ad un determinato ambito $A = (E, W_{ij})$, solo se:

1. Il Profilo Target P^T rispetto al quale vengono effettuati gli assessment è lo stesso per entrambi gli assessment;
2. L'ambito rispetto al quale vengono valutate le metriche è esattamente lo stesso in termini di elementi di interesse (E) e matrice dei pesi (W_{ij}).

Ciò premesso, è opportuno sottolineare che la valutazione svolta in un assessment è fortemente dipendente dalla qualità della misura. Tale aspetto diventa particolarmente evidente in fase di confronto tra due valutazioni, dove diversi approcci nello svolgimento della fase di misura possono potenzialmente portare a risultati del confronto non necessariamente coerenti tra le due realtà considerate.

APPENDICE A. Criteri di assegnazione dei livelli di maturità

I criteri di assegnazione dei livelli di maturità devono essere coerenti con la descrizione dei livelli di maturità del Capability Maturity Model Integration (CMMI). Gli assessor chiamati a erogare il questionario devono porre, per ciascun controllo, una serie di domande all'intervistato, sulla base della descrizione di ciascun livello di maturità del CMMI, che gli permetta di identificare il livello da assegnare al controllo.

Nella prima sezione di questa appendice sono riportati degli esempi di domande che un assessor potrebbe porre per valutare il livello di maturità implementativa di un controllo. Nella sezione successiva è riportato un esempio che si concentra invece sulla valutazione del livello di maturità sulla base di una sintesi delle risposte date dall'intervistato.

A.1 Esempio di domande

In questa sezione vengono riportati degli esempi di domande che un assessor potrebbe fare all'intervistato per valutare il livello di maturità di uno specifico controllo.
Il controllo preso come riferimento nell'esempio è il seguente:

Controllo:
I prestatori di servizi di pagamento compilano e mantengono aggiornato un inventario con componenti di sistema che comprendono sia le parti hardware che quelle software e con dati e informazioni necessarie all'organizzazione

Si noti che, poiché i livelli di maturità CMMI sono incrementali, le domande sono pensate per essere poste nell'ordine in cui sono riportate. In caso di risposta negativa da parte dell'intervistato, l'assessor sarà in grado di esprimere un giudizio circa il livello di maturità da assegnare, in caso di risposta affermativa (ad eccezione dell'ultima domanda) l'assessor può constatare il raggiungimento di un livello di maturità minimo e procederà col sottoporre all'intervistato la successiva domanda o gruppo di domande.

Si noti che (ad eccezione della prima domanda) il presente esempio si focalizza su domande volte a valutare il livello di maturità implementativa del controllo e non del grado di copertura, dando quindi per scontato che questo sia già stato valutato. Si noti, inoltre, che in caso di grado di copertura nullo, non sarà possibile valutare il livello di maturità, poiché il controllo non risulterebbe neanche parzialmente implementato.

#	Domande	Risposta Affermativa	Risposta Negativa
1	▪ I componenti hardware, software e i dati dell'organizzazione sono inventariati?	>= 1 - Iniziale	N/A
2	▪ È definito e documentato un processo di gestione dell'inventario?	>= 2 - Ripetibile	1 - Iniziale

3	▪ Esiste una politica di gestione dell'inventario definita e documentata a livello di organizzazione? ▪ I processi, le procedure, le soluzioni tecniche (quali gli strumenti utilizzati) messi in atto e le informazioni raccolte per ciascun componente sono standardizzati o comunque coerenti con tale politica in tutte le funzioni dell'organizzazione?	>= 3 - Definito	2 - Ripetibile
4	▪ I processi di gestione dell'inventario sono monitorati e periodicamente analizzati per verificarne l'efficacia e la coerenza con la politica generale dell'organizzazione? ▪ Sono definite delle metriche per misurare periodicamente l'efficacia dei processi di gestione dell'inventario?	>= 4 - Gestito	3 - Definito
5	▪ I processi di gestione dell'inventario sono aggiornati nel tempo in risposta a cambiamenti nelle esigenze dell'organizzazione e/o nel panorama tecnologico (es. disponibilità di nuovi strumenti/soluzioni tecniche più efficaci)?	5 - Ottimizzato	4 - Gestito

A.2 Esempio di risposte

Il focus del seguente esempio è sulle risposte date dall'intervistato durante l'erogazione del questionario. Per semplicità l'esempio di concentra su un singolo controllo. In questo caso immaginiamo che l'assessor, attraverso una combinazione di domande chiuse e aperte sottoposte all'intervistato, sia stato in grado di produrre una sintesi delle risposte raccolte. In base a tale sintesi l'assessor decide il livello di maturità assegnato al controllo.

Nel seguente esempio immaginiamo di avere 5 diverse organizzazioni O1, O2, O3, O4 e O5 sottoposte ad assessment. Per ciascuna di esse riportiamo la sintesi delle risposte date dagli intervistati e il livello di maturità assegnato.

Il controllo preso come riferimento nell'esempio è il seguente:

Controllo:
I prestatori di servizi di pagamento utilizzano un processo per identificare le vulnerabilità della sicurezza.

Sintesi risposta intervistato O1:	
Non esiste un processo documentato di identificazione delle vulnerabilità. Il personale occasionalmente, su propria iniziativa o istruito a voce, effettua un vulnerability scan sui sistemi per identificare vulnerabilità note.	
Livello CMMI	1 - Iniziale

Sintesi risposta intervistato O2:	
Ciascun reparto ha attivi piani di gestione delle vulnerabilità che includono l'identificazione delle vulnerabilità note attraverso strumenti di vulnerability scanning. Ciascun reparto sviluppa, documenta ed esegue il proprio piano in autonomia secondo le proprie esigenze. Non c'è coordinazione o condivisione di informazioni tra i vari reparti.	
Livello CMMI	2 - Ripetibile

Sintesi risposta intervistato O3:	
È definita e documentata a livello di organizzazione una politica di gestione delle vulnerabilità che include l'identificazione delle vulnerabilità. Ciascun reparto esegue un processo di identificazione delle vulnerabilità in conformità alla politica dell'organizzazione secondo le modalità e le tempistiche da essa definite ed eventualmente integrando il processo attraverso l'esecuzione di ulteriori procedure o l'utilizzo di strumenti tecnici aggiuntivi (rispetto a quanto richiesto dalla politica dell'organizzazione) laddove richiesto dalle specificità del reparto.	
Livello CMMI	3 - Definito

Sintesi risposta intervistato O4:	
È definita e documentata a livello di organizzazione una politica di gestione delle vulnerabilità che include l'identificazione delle stesse. Ciascun reparto esegue un processo di identificazione delle vulnerabilità in conformità alla politica dell'organizzazione. Le attività di identificazione delle vulnerabilità sono monitorate al fine di valutarne l'efficacia e periodicamente esaminate al fine di verificarne l'aderenza alla politica dell'organizzazione.	
Livello CMMI	4 - Gestito

Sintesi risposta intervistato O5:	
È definita e documentata a livello di organizzazione una politica di gestione delle vulnerabilità che include l'identificazione delle stesse. Ciascun reparto esegue un processo di identificazione delle vulnerabilità in conformità alla politica dell'organizzazione. Le attività di identificazione delle vulnerabilità sono monitorate al fine di valutarne l'efficacia e periodicamente esaminate al fine di verificarne l'aderenza alla politica dell'organizzazione. La politica di gestione delle vulnerabilità è aggiornata nel tempo, anche in risposta alle attività di monitoraggio in modo da migliorarne l'efficacia.	
Livello CMMI	5 - Ottimizzato

APPENDICE B. Rimodulazione dei livelli di priorità

La rimodulazione dei livelli di priorità delle singole subcategory è un passaggio metodologico che si colloca tra le fasi di contestualizzazione e di misura dell'assessment.

Le indicazioni e i livelli di priorità che vengono stabiliti nella fase di contestualizzazione, in base a quanto espresso dai prototipi di contestualizzazione, costituiscono una linea guida di alto livello e, dunque, raffinabile tramite personalizzazioni a seconda del contesto e delle necessità dell'organizzazione che decide di effettuare un assessment mediante l'utilizzo del Framework Nazionale per la Cybersecurity e la Data Protection. Arricchire le fasi di contestualizzazione e di misura secondo quanto espresso dalla presente metodologia, pertanto, rappresenta una possibile personalizzazione utile non solo per consentire agli assessor di realizzare un'analisi efficace, ma anche per direzionare gli sforzi, sia economici sia in termini di tempi di realizzazione delle remediation.

La metodologia si pone come supporto per la definizione di una roadmap di intervento. Il processo di strutturazione di tale roadmap può svilupparsi a partire da un confronto tra il Profilo Attuale e il Profilo Target individuato e consente di identificare le attività da intraprendere, nonché la priorità di attuazione delle stesse.

In altre parole, la presente metodologia fornisce gli strumenti utili a esprimere un giudizio circa il livello di priorità di una singola subcategory al fine di supportare il management nella scelta delle principali azioni da mettere in atto. Tale livello di priorità parte da due elementi fondamentali tra cui è stata individuata una specifica relazione:

- *livello di severità*: grado di criticità, per la specifica organizzazione, di una determinata subcategory. È definito dall'analista durante la fase di contestualizzazione, in seguito alla selezione delle subcategory di interesse. Pertanto, tale parametro risulta indipendente da qualsiasi altro elemento considerato nelle fasi successive.
- *livello di maturità*: il livello di soddisfacimento, calcolato secondo diversi fattori, dei controlli previsti dalla Subcategory. La compilazione del questionario di assessment è quindi propedeutica alla definizione del livello di maturità.

Il processo di individuazione della priorità è caratterizzato, dunque, da tre step conseguenti:

1. Definizione del livello di severità – In fase di contestualizzazione
2. Definizione del livello di maturità – In fase di misura
3. Definizione del livello di priorità – In fase di misura

Livello di severità

Il livello di severità, ovvero il grado di criticità di una specifica subcategory, deriva dall'analisi di diversi indicatori, che possono variare a seconda del contesto di riferimento in cui opera la singola organizzazione. Tali indicatori rappresentano i parametri su cui valutare la criticità dei requisiti di una subcategory per lo specifico contesto di riferimento. In altre parole, costituiscono delle metriche con cui valutare gli impatti. A ciascuno degli indicatori presi in considerazione è possibile assegnare un valore numerico concernente il grado di criticità dell'aspetto misurato dagli stessi. Tale valore numerico deve inserirsi in una scala di valori univoca, che renda gli indicatori confrontabili tra loro. È possibile determinare un indicatore

anche a partire dall'interrelazione tra vari sotto-indicatori, ovvero ulteriori fattori di analisi da associare a valori numerici a seconda del loro grado di criticità.

Una volta definiti gli indicatori nonché le relative scale di valori, sarà possibile determinare il valore complessivo di severità di ciascuna subcategory attraverso un valore di sintesi.

Livello di maturità

Sulla base delle risposte al questionario somministrato durante la fase di misura è possibile definire un livello di maturità per ciascuna subcategory di interesse. Tale livello, espressione di considerazioni analitiche e declinato seguendo una scala di valori crescente, descrive il soddisfacimento delle prescrizioni previste dalla subcategory e la qualità con cui le stesse sono attuate. Inoltre, è possibile utilizzare il risultato di eventuali attività di Vulnerability Assessment e Penetration Test per validare o modificare il livello di maturità associato a determinate subcategory.

Livello di priorità

A margine della fase di misura, una volta definiti quantitativamente i livelli di severità e i livelli di maturità, vengono messi in relazione i valori numerici associati agli stessi e determinato, sulla base di tale relazione, un livello di priorità per ciascuna Subcategory di interesse. A titolo di esempio, una Subcategory con alto livello di severità e basso livello di maturità determinerà un elevato livello di priorità. Viceversa, una Subcategory con basso livello di severità e alto livello di maturità determinerà un livello di priorità trascurabile.

I livelli di priorità identificati attraverso la presente metodologia possono andare a sostituire quanto definito in fase di contestualizzazione. In questo modo, si potrà procedere all'individuazione di una roadmap di adeguamento che tenga conto delle specificità dell'organizzazione.

Bibliografia

[1] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, vol. v1.1, 2018.

[2] CIS Critical Security Controls for Effective Cyber Defense, *https://www.cisecurity.org/controls/*, v8, 2021.

[3] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary, *https://www.iso.org/standard/73906.html*, 2018.

[4] CIS Sapienza e CINI - Laboratorio Nazionale di Cybersecurity, Framework Nazionale per la Cybersecurity e la Data Protection, *https://www.cybersecurityframework.it* , 2019.

[5] Capability Maturity Model Integration, *https://cmmiinstitute.com/learning/appraisals/levels*.