2015 Italian Cyber Security Report

Un Framework Nazionale per la Cyber Security

A cura di:
Roberto Baldoni
Luca Montanari

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini
Cyber Security National Lab

2015 Italian Cyber Security Report

Un Framework Nazionale per la Cyber Security

Research Center of Cyber Intelligence and Information Security
Sapienza Università di Roma

Laboratorio Nazionale CINI di Cyber Security
Consorzio Interuniversitario Nazionale per l'Informatica

Versione 1.0
Febbraio 2016

ISBN: 9788894137316
Titolo: 2015 Italian Cyber Security Report
Stampato in Italia, Febbraio 2016

Realizzato da:

CIS SAPIENZA
Cyber Intelligence and Information Security

cini
Cyber Security National Lab

Tavolo di lavoro composto da:

AON

Deloitte.

Enel

eni

hermesbay

KPMG

INTELLIUM

con la collaborazione di:

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Ministero dello Sviluppo Economico

COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE
CERT - PA
Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

CERT nazionale Italia

e:

Microsoft

pwc

Con il supporto del Dipartimento delle Informazioni per la Sicurezza della Presidenza del Consiglio dei Ministri

A cura di Roberto Baldoni e Luca Montanari

Autori in ordine alfabetico:

Luca Albertini

Stefano Armenia

Roberto Baldoni

Fabio Battelli

Luca Boselli

Stefano Buschi

Alfredo Caputi

Salvatore Carrino

Francesco Ceccarelli

Ludovica Coletta

Romina Colciago

Cosimo Comella

Fabrizio d'Amore

Ciro Di Carluccio

Rita Forsi

Luisa Franchina

Corrado Giustozzi

Davide Grassano

Michele Kidane Mariam

Alberto Marchetti Spaccamela

Carlo Mauceli

Antonino Mazzeo

Fabio Merello

Guido Milana

Luca Montanari

Paolo Prinetto

Leonardo Querzoni

Alfio Rapisarda

Andrea Rigoni

Massimo Rocca

Valeria Risuglia

Lorenzo Russo

Federico Ruzzi

Mario Terranova

Toto Zammataro

Andrea Zapparoli Manzoni

Indice

Executive Summary

Il sistema economico e sociale dei paesi avanzati è diventato fortemente dipendente dal *cyberspace*, quell'insieme di reti e sistemi informativi con i quali vengono erogati servizi indispensabili a cittadini, da parte degli enti governativi, delle infrastrutture critiche, delle imprese e della pubblica amministrazione.

I sistemi informativi sono divenuti chiave anche nella gestione di infrastrutture fisiche come reti elettriche, sistemi industriali, sistemi di trasporto, ecc. Tuttavia il cyberspace e le sue componenti essenziali sono esposti a numerosi rischi. In primis, trattandosi di sistemi complessi e in rapida evoluzione, vi è una costante presenza di vulnerabilità. Nonostante gli sforzi, siccome non vi è oggi possibilità di disporre di sistemi non vulnerabili, anche a causa della moltitudine di attacchi di tipo "0-day" disponibili nel mercato nero, occorre tenere sempre in considerazione eventuali minacce. Una o più di queste vulnerabilità possono essere sfruttate da un attaccante per entrare illecitamente nei sistemi informativi di una organizzazione permettendo quindi all'attaccante di leggere, trafugare o cancellare informazioni critiche fino a prendere il controllo dell'asset informatico o degli asset fisici. Queste vulnerabilità, insieme al fatto che la consapevolezza di questa situazione non è ancora molto elevata a tutti i livelli della società, fanno si che il rischio cyber diventi molto rilevante per una organizzazione, al pari di quello finanziario e reputazionale.

Gli attacchi informatici, cresciuti negli ultimi anni in modo esponenziale per complessità e risorse utilizzate, non possono essere fermati dalle singole organizzazioni, ma hanno bisogno di una risposta dal sistema paese, poiché tendono a diminuirne la prosperità economica e l'indipendenza. Il rischio cyber non può essere annullato ma è importante che una nazione sviluppata si doti di una serie di strumenti e metodologie per migliorare la consapevolezza, affrontare in modo strutturato la risposta e supportare le organizzazioni, gli enti e le organizzazioni pubbliche e private, residenti sul proprio territorio, per la riduzione del rischio e la mitigazione degli effetti di eventuali, possibili incidenti di sicurezza. In questo ambito emerge il tema della responsabilità che può incombere sulle organizzazioni, pubbliche o private, e sugli individui dotati di poteri rappresentativi e direzionali, per la violazione de dovere di diligenza, prudenza e perizia nella tutela delle posizioni di garanzia che l'ordinamento attribuisce ai singoli e alle persone giuridiche. L'adesione al Framework, rappresentativo delle pratiche generalmente riconosciute e internazionalmente validate, permette

una più agevole dimostrazione della applicazione della “due diligence”, riferendosi a razionali, oggettivi e misurabili, per aver posto in essere quanto era doveroso attendersi in applicazione del principio di “duty of care”.

Questo documento presenta un *Framework Nazionale di cyber security* il cui scopo è quello di offrire alle organizzazioni un approccio volontario e omogeneo per affrontare la cyber security al fine di ridurre il rischio legato alla minaccia cyber. L’approccio di questo Framework è intimamente legato a una analisi del rischio e non a standard tecnologici.

Il Framework ha molti punti in comune con il Framework di cyber security del NIST orientato alle infrastrutture critiche [15], questo anche per cercare una armonizzazione internazionale, ma è stato specializzato sulla realtà produttiva Italiana, fatta in particolare di piccole-medie imprese. Il Framework Nazionale eredita dal Framework del NIST le nozioni di Framework Core, Profile e Implementation Tier e aggiunge i livelli di priorità e i livelli di maturità alle 98 Subcategory che formano il Framework Core. Il terzo concetto introdotto in questo documento è la nozione di contestualizzazione del Framework. Una organizzazione che voglia utilizzare il Framework, come primo passo, deve identificare una contestualizzazione su cui valutare il proprio profilo di rischio attuale. Una contestualizzazione del Framework implica la selezione delle sottocategorie del Framework Core e la definizione dei relativi livelli di priorità e di maturità. La contestualizzazione viene fatta rispetto al profilo di business, alle vulnerabilità di settore, alla dimensione dell’organizzazione e ad altre caratteristiche aziendali o di settore. Contestualizzazioni del Framework possono essere create da diversi attori, quali le associazioni di settore produttivo o dalla stessa organizzazione se possiede le competenze per farlo. Nel caso di settori produttivi regolati, contestualizzazioni del Framework possono essere create dai regolatori di settore in modo da armonizzarle con le regolamentazioni di settore in materia di minaccia cyber.

A titolo di esempio, il presente documento propone una contestualizzazione per piccole-medie imprese indipendente dal settore produttivo.

Una volta che l’organizzazione adotta una contestualizzazione del Framework, può calcolare il suo *profilo attuale* rispetto al rischio cyber. Successivamente l’organizzazione dovrà individuare un *profilo obiettivo* che rispecchia il punto d’arrivo di una strategia aziendale cyber. I tempi e i modi con cui l’organizzazione pianifica il passaggio tra profilo attuale e profilo obiettivo sono di sua pertinenza.

È importante comprendere che il Framework non è uno standard di sicurezza, bensì un quadro di riferimento nel quale possono essere inquadrati gli standard e le norme di settore esistenti e future. Il compito di definire gli standard compete agli organi e agli istituti di standardizzazione nazionali e internazionali, nonché ai regolatori di settore. L’adozione del Framework è volontaria.

Oltre a discutere la relazione tra la normativa di riferimento attuale in Italia e le Subcategory def Framework Core, Il documento apre la strada anche a nuove opzioni per aumentare le capacità di tutela dal rischio cyber attraverso il trasferimento assicurativo del rischio residuo. Un sistema dove assicurazione e assicurato intraprendono un cammino virtuoso teso a ridurre le conseguenze economiche dovute al materializzarsi di tale rischio. L’organizzazione crea le condizioni affinché il rischio sia ridotto a un livello accettabile per la propria sicurezza – anche in funzione di una valutazione costo-beneficio, della propensione e tolleranza al rischio – e per il mercato assicurativo; quest’ultimo, da parte sua, condivide con l’organizzazione un processo virtuoso che operi in ottica win-win per entrambe le Parti (garanzia di tutela del bilancio per l’organizzazione; ruolo sociale e garanzia di redditività per il Mercato). Infine il Framework aiuta l’organizzazione a descrivere il livello di maturità e di rigore delle sue pratiche di gestione del rischio cyber.

Questo documento è strutturato in tre parti. Nella Parte I viene presentato il Framework Nazionale, le sue motivazioni e le guide per l’utilizzo del Framework per alcuni attori particolarmente rilevanti.

La Parte II presenta il Framework Core, una contestualizzazione del Framework per piccole-medie imprese e una serie di raccomandazioni per le Grandi Imprese su come applicare il processo di gestione del cyber risk. La Parte III mostra come il Framework si relaziona con il panorama normativo Italiano e con specifiche regolamentazioni di settore. La parte III contiene anche un approfondimento sulla gestione del rischio cyber e la relazione con il mercato assicurativo.

Considerando la particolare natura dinamica delle minacce nel cyber space e dei tumultuosi cambiamenti tecnologici, questo documento sarà in continua evoluzione integrando ad intervalli regolari feedback, best practices e lezioni che verranno apprese nel tempo. L'adozione di questo Framework da parte delle organizzazioni residenti nel nostro paese può portare ad un irrobustimento dell'intero sistema paese rispetto ad attacchi di tipo cibernetico.

1. Introduzione e guida alla lettura

Tutta l'economia e i servizi di welfare di un paese avanzato ormai si poggiano su infrastrutture e servizi erogati tramite il cyber space, quell'insieme di reti, protocolli e applicazioni informatiche eterogenee e interconnesse che ci circonda. Incidenti informatici che impattino tali infrastrutture e servizi possono avere conseguenze economiche molto rilevanti, a livello di nazione, di imprese e di singoli cittadini. Tali incidenti non investono solo il piano cibernetico, possono infatti partire da questo per poi arrivare ad avere impatti sulle infrastrutture fisiche, provocando indisponibilità di servizi anche essenziali e quindi perdite economiche, fino a possibili perdite umane. Gli incidenti possono essere naturali o provocati da terroristi, cybercriminali, attivisti o da nazioni straniere (cyber-warfare). In questi ultimi casi, se la vittima è una impresa, oltre al danno reputazionale, si possono avere danni finanziari ingentissimi: dalla semplice perdita di competitività fino alla completa perdita del controllo degli asset strategici (IPR, metodologie di processo, sistemi informativi ecc). Nel caso di una nazione si potrebbe arrivare a una diminuzione delle capacità difensive, fino a una perdita di indipendenza. Per un cittadino la minaccia cyber può prendere la forma di danni a diritti e interessi di rango costituzionale come la vita, l'incolumità fisica, le libertà fondamentali incluso il diritto alla riservatezza, oltre che impatti di natura economica. In questo documento la cyber security è definita come segue:

La cyber security è quella pratica che consente a una entità (ad esempio, organizzazione, cittadino, nazione ecc.) la protezione dei propri asset fisici e la confindezialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal cyber space. A sua volta, *il cyber space viene definito come il complesso ecosistema risultante dall'interazione di persone, software e servizi su Internet per mezzo di tecnologie, dispositivi e reti ad esso connesse*[1].

Le minacce cyber non possono certamente essere affrontate rinunciando alle potenzialità offerte dai sistemi informatici e dalla loro interconnessione in rete perdendo quindi l'aumento della produttività ed efficienza che l'informatizzazione porta con sé. La risposta deve essere sistemica, mirata ad aumentare la consapevolezza dei cittadini, la "duty of care" delle imprese e la "due diligence" internazionale del paese rispetto alla minaccia cyber. Come rilevato molto

[1] Rispetto alla definizione introdotta dagli standard ISO/IEC 27000:2014[10] e ISO/IEC 27032:2012[11], da cui questa è derivata, la definizione esplicita la protezione degli asset fisici aziendali oltre a quelli informativi.

puntualmente in un rapporto dell'OCSE [23] e ripetuto diverse volte dal nostro rapporto negli anni passati [5, 6] , è di fondamentale importanza che in questo processo di presa di coscienza collettiva si passi dal concetto di "sicurezza dei sistemi informatici" o "sicurezza IT" a quello di "gestione del rischio cyber". Questo significa, tra le altre cose, definire un processo che risulti rispettoso del dettato costituzionale, che riguarda ad esempio, l'esercizio dell'attività d'impresa che si svolga in modo da non contrastare l'utilità sociale o da recar danno alla sicurezza, alla libertà e alla dignità umana. Tale considerazione implica che la prospettiva della cyber security non sia considerata semplicemente un aspetto tecnologico, ma impone piuttosto la considerazione dei doveri complessivi di natura giuridico-formale e i principi di utilità sociale verso cui pubblico e privato, per necessità e doverosità, devono convergere. Per tale ragione il dovere di protezione deve entrare a far parte del set di responsabilità dei vertici delle organizzazioni, richiedendo una specifica e puntuale valutazione da parte dei soggetti rivestiti di poteri di indirizzo e gestione[24].

Come ogni rischio aziendale, il rischio cyber non può essere eliminato e ha quindi bisogno di un insieme di azioni coordinate per poter essere gestito. Azioni che coinvolgono gli ambiti organizzativi e tecnologici dell'azienda, oltre che di gestione finanziaria del rischio, anche attraverso la definizione di una strategia di gestione del rischio residuo, abilitando in tal modo l'adozione di un approccio integrato di prevenzione del rischio e di protezione del bilancio dell'impresa. Inoltre, il rischio cyber è intrinsecamente altamente dinamico. Esso cambia al cambiare delle minacce, delle tecnologie e delle regolamentazioni. Per iniziare ad approcciare questo problema in modo che sia utile al sistema paese (stato, aziende e cittadini) c'è bisogno di definire un terreno comune, un Framework, dove diversi settori produttivi, pubbliche amministrazioni e settori regolati possano riconoscersi e allineare le loro pratiche di cyber security in un processo di evoluzione continua. Per raggiungere tale obiettivo *un Framework comune deve innanzitutto essere neutrale tanto rispetto alle pratiche di risk management aziendali quanto rispetto alla tecnologia*, in modo che ogni attore possa continuare a usare i propri strumenti di gestione del rischio e a gestire i propri asset tecnologici continuando anche a mantenere la conformità agli standard di settore.

In questo documento viene proposto un Framework Nazionale di cyber security con l'intento, innanzitutto, di costruire un linguaggio comune per confrontare le pratiche aziendali di prevenzione e contrasto dei rischi cyber. Il Framework può aiutare una impresa a organizzare un percorso di gestione del rischio cyber, sviluppato nel tempo, in funzione del suo business, della sua dimensione e di altri elementi caratterizzanti e specifici dell'impresa. L'adozione del Framework è pertanto su base volontaria.

Il Framework che proponiamo si basa sul "Framework for Improving Critical Infrastructure Cybersecurity" emanato dal NIST[15], riprendendone i concetti base di Framework Core, Framework Implementation Tier and Framework Profiles. Ne eredita quindi il sistema di Function e Category del Framework Core che di fatto rappresenta quel terreno comune che crea il punto d'incontro tra Framework e standard aziendali sia tecnici sia di gestione del rischio.

La scelta di partire dal Framework statunitense è stata fatta ritenendo che la risposta alle minacce cyber debba prevedere un allineamento a livello internazionale oltre che a livello di sistema paese. Questo anche per permettere a imprese multinazionali di allineare i loro processi di gestione della cyber security in modo più semplice su scala internazionale.

Il Framework del NIST propone un quadro d'insieme altamente flessibile diretto principalmente alle infrastrutture critiche; noi lo abbiamo evoluto nella direzione delle caratteristiche del sistema socio-economico del nostro Paese ottenendo un Framework cross-settoriale che può essere contestualizzato su settori produttivi specifici o su tipologie di aziende con determinate caratteristiche. Questo permette di trasferire pratiche e conoscenze da un settore all'altro in modo semplice ed efficace, In questa direzione abbiamo inserito nel Framework Nazionale tre concetti importanti:

I livelli di priorità. I livelli di priorità definiscono qual è la priorità con cui si deve affrontare ogni singola Subcategory del Framework Core. Da notare che ogni organizzazione è libera di contestualizzare i propri livelli di priorità in base al tipo di business, alla dimensione, al suo profilo di rischio.

I livelli di maturità. I livelli di maturità definiscono le diverse modalità con cui si può implementare ogni singola Subcategory del Framework Core. Il livello di maturità selezionato deve esser valutato attentamente dalla singola azienda in base al suo business e alla sua dimensione nonché al suo profilo di rischio. Tipicamente livelli di maturità maggiori richiedono effort maggiore, sia dal punto di vista economico che di gestione. Per alcune Subcategory non è possibile definire livelli di maturità.

Contestualizzazione del Framework Creare una contestualizzazione del Framework (per un settore produttivo, per tipologie di azienda o per una azienda singola), significa selezionare le Function, Category e Subcategory del Framework Core pertinenti, specificandone livelli di priorità e di maturità adatti al contesto di applicazione.

Questo documento fornisce una contestualizzazione per Piccole-Medie Imprese, ovvero una contestualizzazione per tipologia di azienda quindi indipendente dal settore di business (dettagli nel Capitolo 6). La scelta di fornire una contestualizzazione per le PMI è legata al fatto che queste aziende possono appartenere a settori come quello alimentare, manifatturiero, logistico o meccanico che possono non essere particolarmente sensibili alle tematiche di cyber security. L'obiettivo è quello di fornire loro degli strumenti pratici necessari per intraprendere un cammino virtuoso di rafforzamento delle loro difese cyber. Queste PMI sviluppano servizi e/o prodotti di altissima qualità realizzati spesso attraverso processi o metodologie raffinate nel tempo e che rappresentano il vero valore dell'azienda. Qualora tali asset strategici venissero compromessi da attacchi cyber, verrebbe messa a repentaglio la sopravvivenza stessa dell'azienda, spesso senza che quest'ultima possa a rendersi conto in tempo dell'accaduto.

Altre contestualizzazioni potrebbero essere fatte in modo mirato da associazioni di categoria o da enti regolatori, in modo da essere riconosciute da tutto un settore produttivo o da un settore regolato. Per quanto riguarda i settori regolati in alcuni casi le priorità nell'implementazione di alcuni controlli di sicurezza a un livello di maturità base potrebbero diventare obblighi in funzione delle loro regolamentazioni di settore. La Sezione 3.4 fornisce dettagli su chi può creare una contestualizzazione del Framework e su come farlo.

Ogni organizzazione può allineare le proprie pratiche di cyber security basandosi sul proprio business, la propria tolleranza al rischio e le risorse che è in grado di mobilitare, definendo eventualmente strategie di gestione del rischio residuo. Questo concetto viene espresso dalla nozione di *profilo corrente* dell'organizzazione. Il profilo corrente viene creato confrontando i programmi esistenti di cyber security con le Subcategory del Framework e i relativi livelli di maturità. Mediante questo confronto si selezionano le Subcategory già implementate dalle pratiche esistenti con relativo livello di maturità. Questa selezione crea il profilo corrente, da confrontarsi con il *profilo target*. Il profilo target consiste nella selezione delle Subcategory e dei livelli di maturità desiderati, in base alle esigenze dell'organizzazione. Avere profilo corrente e profilo target agevola il processo di gap analysis e di definizione di una roadmap da seguire per ottenere il livello di cyber security desiderato. Nella definizione della roadmap, le Subcategory a *priorità alta* sono quelle da implementare per prime. Le Subcategory a *priorità media* e a *priorità bassa* devono essere selezionate in base alle proprie esigenze e implementate successivamente.

Inoltre il Framework aiuta l'azienda a valutare il proprio processo di gestione del rischio cyber attraverso una valutazione basata su *implementation tiers* che viene ereditata dal Framework del NIST. Tier 1 identifica un risk management fatto ad-hoc per la cyber security. Tier 2 corrisponde

al livello “risk informed” ovvero un livello dove i processi di risk management sono funzionanti ma non integrati. Tier 3 corrisponde al livello “ripetibile (repeatable)” dove policy formali per il risk management sono funzionanti e integrati e Tier 4, “adattivo (adaptive)” dove i processi di risk management sono inseriti all’interno della cultura aziendale. Esempi di contestualizzazione di questi Tier sono stati realizzati da Intel [9], Langner [26] e da The Communications Security, Reliability and Interoperability Council [18]. Anche in questo caso le organizzazioni devono valutare il loro processo di risk management e programmare un percorso per portarsi nel tempo verso i Tier 3 e 4. Per maggiori dettagli sugli implementation tier si rimanda al documento del Framework NIST[15].

La Figura 1.1 mostra la relazione tra Framework Nazionale di Cyber Security e le caratteristiche specifiche di una organizzazione: pratiche di Enterprise Risk Management adottate, standard di sicurezza informatica utilizzati o di cui si ha la certificazione, dimensione della organizzazione e settori produttivi. In particolare, il Framework, salendo nel livello di astrazione, agisce da ponte tra strumenti di Enterprise Risk Management e IT & Security Standards. Nella Figura vengono indicate contestualizzazioni di settore produttivo e contestualizzazioni basate sulla tipologia di azienda. Da notare come per ogni settore produttivo o per ogni tipologia di azienda potrebbero essere definite più contestualizzazioni. Un’azienda come primo passo nel processo di adesione del Framework dovrà selezionare una contestualizzazione da utilizzare (vedere Capitolo 3 per maggiori dettagli).

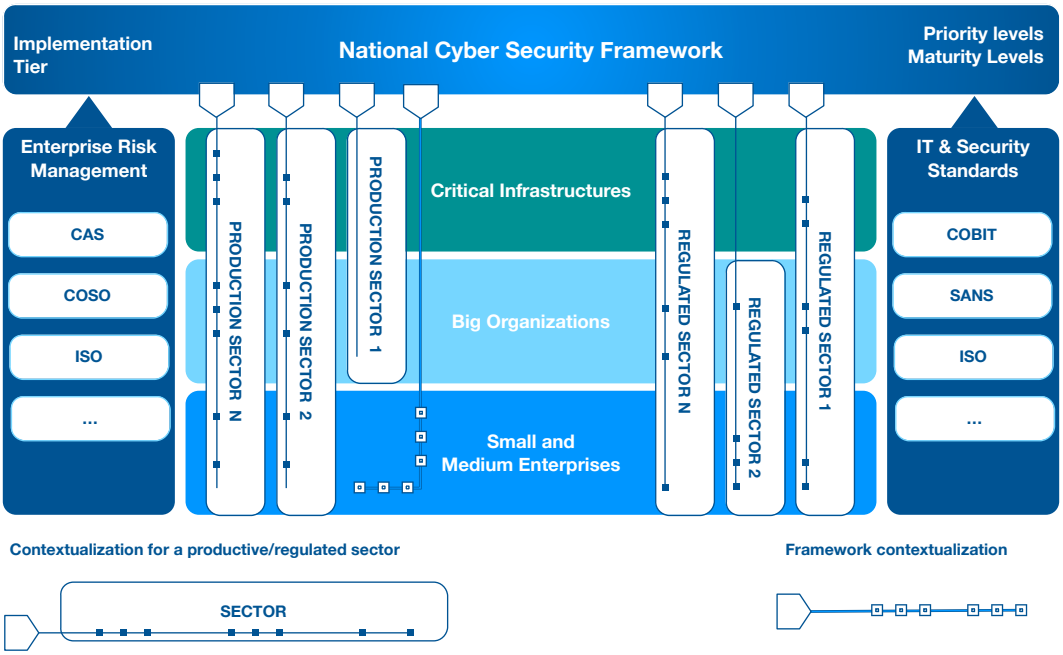

Figura 1.1: Framework Nazionale per la Cyber Security e sua relazione con Enterprise Risk Management, standard e altri framework, dimensione delle imprese e settori produttivi.

Facciamo notare che il Framework Nazionale per la Cyber Security non è un documento statico, bensì vivo che deve essere aggiornato in base all’evoluzione della minaccia, delle tecnologie di cyber security e delle tecniche di risk management. Tale aggiornamento andrebbe assicurato da organi istituzionali responsabili per il suo mantenimento nel tempo.

Guida alla lettura del documento

Questo documento è stato strutturato in tre parti. Nella Parte I viene presentato il Framework Nazionale, le sue motivazioni e le linee guida per l'utilizzo del Framework per alcuni attori particolarmente rilevanti (Capitolo 3 e Capitolo 4). La Parte II presenta il Framework Core (Capitolo 6), una contestualizzazione del Framework per Piccole-Medie Imprese e una serie di raccomandazioni per le Grandi Imprese su come applicare il processo di gestione del cyber risk. La Parte III fornisce alcuni aspetti legati al contesto di applicazione nazionale del Framework. In particolare contiene dettagli sull'Enterprise Risk Management, un approfondimento sul mercato assicurativo e delle polizze cyber, la relazione con il panorama normativo Italiano e alcuni approfondimenti riguardo specifici settori regolati.

Di seguito vengono identificate delle guide alla lettura delle Parti I e II del documento per diverse tipologie di lettori:

Piccole-Medie Imprese. Il Capitolo 6 mostra una contestualizzazione del Framework per Piccole-Medie Imprese. La contestualizzazione fornita per le PMI si compone di: una selezione di Subcategory (Sezione 6.1), dei livelli di priorità da seguire nell'applicazione delle Subcategory selezionate (Sezione 6.2), livelli di maturità per le Subcategory a priorità alta (Sezione 6.3) e una guida all'implementazione di queste (Sezione 6.4). Le PMI interessate a definire una propria strategia di cyber security e a implementarla potranno avvantaggiarsi di tali strumenti.

Grandi Imprese, Infrastrutture Critiche e aziende di rilevanza strategica nazionale. Il Capitolo 7 fornisce suggerimenti su come utilizzare il Framework per una grande impresa. In questo contesto noi assumiamo che le Grande Imprese abbiano competenze di risk management per poter contestualizzare il Framework. In particolare vengono definiti suggerimenti per il top management su come gestire il rischio cyber e su come organizzare il processo relativo. Si mette in evidenza la differenza tra un Security Operations Center (SOC) e un Computer Emergency Readiness Center (CERT). Infine viene presentato un processo di gestione evoluto del rischio cyber in una grande impresa.

Regolatori di settore. Per quanto riguarda i regolatori di settore, la Sezione 4.4 del Capitolo 4 presenta una guida all'applicazione del Framework. Inoltre le Sezioni 11.1 e 11.2) presentano due esempi di posizionamento rispetto al Framework di settori altamente regolati come la Pubblica Amministrazione, il settore bancario e le aziende quotate. Inoltre viene mostrato come tali settori possano trarre beneficio dall'applicazione del Framework.

Infine, i Capitoli 8,9 e 10 sono di interesse generale: il primo affronta il tema del'Enterprise Risk Management; il secondo il tema del trasferimento del rischio al mercato assicurativo; il terzo fornisce la correlazione tra le sottocategorie del Framework e il contesto normativo Italiano, in particolare quello legato al Codice della Privacy e quello derivato dal DPCM del 24/1/2013.

PARTE I - Il Framework Nazionale

2. La necessità di un Framework Nazionale

Negli ultimi tempi l'opinione pubblica è stata esposta a numerosi casi eclatanti di attacchi cyber, alcuni anche con effetti importanti. In alcuni casi si è trattato di attacchi da parte di attori collegabili a governi come, ad esempio, quello a danno di Sony Pictures a seguito della distribuzione del film "The Interview"; in altri casi si è trattato dell'utilizzo della dimensione cyber per attività e attacchi misti (terrorismo, operazioni di spionaggio, operazioni militari). Anche le piccole e medie imprese cominciano a comprendere che esiste un problema che potrebbe coinvolgerle, non sempre però capendo che le conseguenze potrebbero essere disastrose.

Il livello di consapevolezza è aumentato di conseguenza e ci si inizia a domandare quale sia il il proprio livello di preparazione. Questo processo di aumento della consapevolezza, ancora estremamente acerbo nel nostro Paese, deve essere necessariamente accompagnato da strumenti metodologici a supporto. Tali strumenti devono essere semplici, adatti a qualunque tipologia di utente, in grado di fornire una roadmap per raggiungere un livello minimo di preparazione nella protezione delle informazioni e/o della reputazione propria e della propria azienda. Il Framework Nazionale nasce proprio in quest'ottica.

Infine è fondamentale rimarcare che la minaccia cyber richiede una risposta coordinata pubblico-privato in primo luogo di tipo nazionale. Nessuno dei due attori può rispondere singolarmente a questa minaccia, poiché il privato non può controllare minacce che possono arrivare da qualunque parte del mondo e il pubblico ha bisogno del privato poiché molti servizi essenziali sono ormai gestiti/forniti da questi ultimi e un attacco potrebbe portare a conseguenze dirette per i cittadini. Come rilevato dal Libro Bianco "il Futuro della cyber security in Italia" pubblicato a Novembre 2015 [3], Il Framework Nazionale di cyber security rappresenta uno degli elementi essenziali per un aumento di resilienza domestica dei sistemi e delle reti rispetto a tale minaccia. *L'adozione di un Framework è quindi un passo fondamentale anche nell'ottica di migliorare la propria reputazione, e favorire investimenti internazionali nel nostro paese.*

2.1 I vantaggi per il panorama italiano: PMI, Grandi Imprese e regolatori di settore

Piccole Medie Imprese.

Il panorama italiano è costituito per la maggioranza da piccole-medie imprese, gran parte di queste non hanno mai affrontato il problema della sicurezza informatica. Questo è dovuto principalmente alla mancata valutazione del rischio cyber: piccole imprese talvolta sono convinte di non avere patrimonio informativo da proteggere, altre volte non sono al corrente degli innumerevoli mezzi che l'attaccante moderno è in grado di mettere in atto. Il principale problema delle piccole imprese, nel momento in cui si affacciano al mondo della sicurezza, sono i costi. Esse, in autonomia, non sono in grado di valutare quali sono le pratiche "quick-win", vale a dire quelle che con il minimo sforzo garantiscono di ottenere un salto di livello in termini di protezione. Di conseguenza, tali aziende corrono il rischio di stimare in maniera errata il costo della messa in sicurezza dei propri asset, con il risultato che spesso l'idea di incrementare la propria sicurezza viene messa da parte, correndo rischi enormi, di cui non sono consapevoli. Il Framework fornisce una serie di pratiche di sicurezza che, specialmente per le PMI, sono contemporaneamente basilari ed economiche. Tali pratiche sono state denominate "pratiche a priorità alta" (vedi Capitolo 6) e corrispondono a quell'insieme di operazioni che consentono di portare il proprio livello di consapevolezza, protezione e quindi sicurezza a un valore base, sufficiente per la maggior parte delle PMI italiane.

Grandi Imprese.

Il Framework Nazionale non ha la pretesa di guidare le Grandi Imprese e di sostituirsi alla complessa gestione del rischio di queste. Può però essere molto utile nell'affiancare, attraverso una metodologia unificata, i processi e programmi aziendali per la gestione del rischio, al fine di farli evolvere in modo coerente e strutturato (vedi Capitolo 7). Inoltre, le Grandi Imprese possono giovare della presenza del Framework in due aspetti fondamentali: l'internazionalità di questo e la possibilità di richiedere profili di sicurezza ai propri contractor. Il Framework infatti, essendo basato sul Framework del NIST, ne conserva la piena compatibilità dei profili di sicurezza e quindi ne eredita l'internazionalità. Di conseguenza, può agevolare la comunicazione dei propri livelli di sicurezza al pari degli standard noti (ad esempio quelli emanati dall'ISO), ma in maniera estremamente più economica. Dal punto di vista dei contractor, Grandi Imprese e infrastrutture critiche possono utilizzare il Framework per richiedere determinati livelli di sicurezza a tutti o ad alcuni degli attori che costituiscono la propria supply chain, oppure solo a coloro che dovranno interagire con determinate risorse. Questo meccanismo consente di incrementare la sicurezza di tutto l'ecosistema dell'impresa e di minimizzare di conseguenza la superficie vulnerabile d'attacco.

Regolatori di settore.

Per quanto riguarda i regolatori di settore, il Framework Nazionale fornisce un terreno di confronto chiaro e unico su cui operare in modo coerente sia con le aziende che regolano sia con altri regolatori. Il Framework può essere impiegato come strumento per la definizione di norme e standard in maniera strutturata e compatibile con altri regolatori. Permette di verificare la sussistenza di eventuali discipline specifiche, nazionali, europee e internazionali, generali e di dominio, evitando di imporre oneri supplementari e supportando il dialogo tra regolatore ed entità regolate. Le norme di settore, così come tutte le altre norme, restano in vigore, dopo la loro emanazione, per tempi estremamente lunghi se confrontati con i tempi di evoluzione della minaccia cyber. Diventa quindi importante istituire processi di revisione specialmente per i settori in cui è particolarmente critica la gestione della sicurezza (es. settore bancario, pubblica amministrazione, ecc.). Il Framework può essere utilizzato per una revisione preliminare dei regolamenti in un primo momento, in seguito, è possibile seguire l'evoluzione del Framework stesso per aggiornare le proprie pratiche e normative. Stabilire inoltre un mapping tra le proprie regole di settore e le pratiche del Framework rappresenta un utilissimo esercizio al fine di evidenziare le eventuali

mancanze, le quali inevitabilmente estendono il territorio di attacco per le aziende del proprio settore.

2.2 Il Framework e la gestione del rischio cyber

Il compito fondamentale della cyber security è la protezione e la tutela della missione delle organizzazioni/aziende dai rischi derivanti dal cyberspace e dai sistemi informativi. Tutte le organizzazioni sono esposte a una moltitudine di rischi di varia natura. Sebbene vi siano molte definizioni, il senso comune ci insegna che il rischio non è altro che la possibilità di perdere qualcosa di valore: questo valore può essere un oggetto fisico, del denaro, il proprio stato di salute, un valore sociale, un livello di benessere emotivo. Il rischio è quindi legato all'incertezza di eventi prevedibili o improvvisi, diretti o indiretti, misurabili o non misurabili. L'incertezza è legata sia agli eventi sia alle loro cause e ai loro effetti, non sempre facilmente identificabili e definibili. Proprio per questa caratteristica di incertezza, uno stesso rischio può essere percepito in modo molto diverso, a seconda del soggetto che ne valuta le caratteristiche.

Indipendentemente dal settore e dalla tipologia di rischi, c'è una certa convergenza sul definire il rischio come la materializzazione di un evento negativo che possa inficiare gli obiettivi aziendali. Esso può essere visto come il risultato di tre fattori: la minaccia, la vulnerabilità e l'impatto. L'analisi delle tre componenti fondamentali può consentire a una organizzazione di ridurre il rischio attraverso una serie di tecniche, che vanno dalla riduzione delle vulnerabilità alla riduzione del possibile danno; in alcuni casi si può anche contemplare la riduzione della minaccia, ove sia possibile. Ogni organizzazione deve valutare i propri rischi e, in base al proprio livello di tolleranza, decidere quali contromisure adottare. In generale, essendo un concetto altamente legato all'aleatorietà delle variabili che lo determinano, non si considera possibile poter ridurre un rischio a zero, esiste di conseguenza sempre un livello di rischio residuo da considerare. Le organizzazioni devono valutare l'equilibrio tra riduzione del rischio, rischio residuo e la propria "tolleranza" al rischio. Il rischio residuo può essere quindi accettato, oppure trasferito nelle sue conseguenze economiche all'esterno, per esempio attraverso l'uso di prodotti assicurativi. Altro esempio è quello di ricorrere a un fornitore di servizi di sicurezza gestita (i c.d. Managed Security Services Provider – MSSP), al fine di presidiare i rischi in una determinata area di sicurezza: ad esempio, l'individuazione tempestiva di eventi sospetti o di compromissioni che possono nuocere l'integrità, la disponibilità e la confidenzialità delle informazioni. Tale approccio è particolarmente comune nelle PMI, per le quali può risultare sconveniente allocare risorse umane e tecnologiche al monitoraggio degli eventi di sicurezza e quindi al presidio di questa specifica area. L'insieme delle pratiche di analisi e valutazione delle opzioni di mitigazione, accettazione, trasferimento o elusione del rischio va sotto il nome di Gestione del Rischio (o Risk Management). Le valutazioni connesse alla gestione del rischio non possono essere delegate: rappresentano una componente fondamentale della conduzione di una organizzazione, la loro approvazione è una responsabilità inalienabile del top management.

Il cyber security risk management è un'applicazione della disciplina della gestione del rischio nell'ambito del cyber space. Poiché le tre caratteristiche fondamentali del rischio cyber (vulnerabilità, minacce e danno) sono spesso fortemente interrelate con altri domini di rischio, il cyber security risk management, al pari di altre tipologie di analisi e gestione dei rischi, non può essere visto come una disciplina a sé stante, ma come una delle componenti chiave del c.d. "Enterprise Risk Management". Come vedremo in seguito, il Framework fornisce un impianto metodologico attraverso il quale disegnare un processo di cyber security risk management (un esempio di tale processo viene descritto nella Sezione 7.2).

2.3 I vantaggi per il sistema paese: verso una international due diligence

Nell'ottica in cui gli aspetti economici, tecnologici e conseguentemente politici delle attività del cyber space a livello internazionale diventeranno in breve tempo un punto dominante della geo-politica, un Framework Nazionale di cyber security è uno degli elementi che un paese, nonché le aziende private che cadono sotto la sua giurisdizione, devono prevedere per mettere in sicurezza le reti e i sistemi informativi. Oltre al Framework Nazionale, gli altri elementi essenziali di un sistema nazionale di aumento di resilienza agli attacchi sono:

- una rete di CERT efficiente: L'Italia nel 2014 si è dotata di un proprio CERT nazionale[1]. Il CERT nazionale supporta cittadini e imprese attraverso azioni di sensibilizzazione, di prevenzione e di coordinamento della risposta a incidenti cyber su vasta scala. Inoltre, attraverso il collegamento con gli altri CERT governativi (CERT-PA della Pubblica Amministrazione e CERT-Difesa), potrà garantire una prospettiva aggiornata su eventi rilevanti utili alle imprese per l'aggiornamento e l'evoluzione dei propri programmi di cyber security;

- un sistema di condivisione delle informazioni pubblico-privato (con scambio bidirezionale) sul modello degli ISAC statunitensi dove riunire in tavoli di lavoro congiunti imprese dello stesso settore produttivo o con una esposizione al rischio cyber molto simile [4]. Tali tavoli hanno lo scopo di prevenire la minaccia cyber attraverso opportune azioni di intelligence;

- un sistema integrato di interazione tra pubblico-privato-ricerca nazionale fatto di poli tecnologici, centri di ricerca congiunti ecc. [3], dove avere un punto di riferimento tecnologico per le operazioni di difesa e di gestione delle crisi.

La singola organizzazione, oltre a interfacciarsi con gli elementi precedenti, dovrebbe implementare al proprio interno le best practice tecnologiche tipiche della gestione del rischio IT come: sistemi di disaster recovery e business continuity di sistemi e reti, audit, ricerca vulnerabilità sui sistemi e certificazioni di sicurezza dei propri sistemi.

Questo ecosistema di misure che vanno senza soluzione di continuità dal pubblico al privato, oltre a proteggere i nostri interessi economici nazionali, potrà essere di rilevanza cruciale all'interno di contenziosi legali tra imprese o di dispute internazionali tra stati, dovuti ad attacchi cyber. Infatti, alleviare o aggravare la propria posizione dipenderà dalla "duty-of-care" o dalla "negligence" che uno stato, una azienda o entrambi avranno seguito nel corso del tempo per minimizzare il rischio cyber. Da questo punto di vista, il Framework Nazionale di cyber security rappresenta uno strumento per identificare le eventuali lacune nella gestione della cyber security di una organizzazione, sia essa nel settore pubblico che in quello privato e per definire un percorso di gestione del rischio che perduri al cambiare della minaccia e della tecnologia.

[1] Il CERT Nazionale è raggiungibile al sito `http://certnazionale.it`. Il CERT Nazionale funge da aggregatore e da "certificatore" di contributi, segnalazioni di informazioni altamente affidabili provenienti da soggetti, pubblici e privati, nazionali e internazionali. Le imprese possono condividere in maniera protetta e tutelata informazioni proprie con il CERT nazionale e con gli altri soggetti accreditati.

3. I concetti di base

Il Framework Nazionale definito in questo documento si fonda sul "Framework for Improving Critical Infrastructure Cybersecurity" [15], sviluppato dal National Institute for Standards and Technology (NIST) statunitense, per poi essere ampliato in ragione del contesto nazionale. Questa scelta si basa sul fatto che il Framework sviluppato dal NIST, ha una copertura completa e allo stato dell'arte del ciclo di vita della sicurezza delle informazioni e dei sistemi, mantenendo quell'opportuno livello di astrazione in grado di garantire alle aziende autonomia nell' applicazione e nella contestualizzazione dei controlli. Essendo però definito per infrastrutture critiche, introduce un livello di complessità non adatto a gran parte delle aziende che costituiscono l'ecosistema delle imprese italiano. Pur trattandosi di un Framework, esso necessita di aggiornamenti in base ai commenti forniti dalle aziende che lo implementeranno, al cambiamento della minaccia, e in base agli avanzamenti tecnologici e organizzativi. Diversamente, i normatori e gli organi di standardizzazione potranno far evolvere i propri regolamenti e standard. Inoltre, il fatto che il Framework Nazionale qui definito si basa su quello del NIST, già adottato da numerosi altri paesi, è garanzia di uniformità e di facilità di utilizzo, in particolare per le aziende multinazionali, che così non si troveranno di fronte a indicazioni diverse da paese a paese.

Il cuore del Framework NIST è costituito da un insieme di 21 Category e 98 Subcategory, organizzate in 5 Function. Ogni Subcategory rappresenta un'area di raccomandazioni che l'organizzazione può decidere di implementare, se necessario riferendosi a standard o norme specifiche di settore. Il Framework NIST fornisce, per ogni Subcategory, i riferimenti agli standard e Framework esistenti: si tratta di una mappatura parziale, ma che comunque copre la quasi totalità dei riferimenti già adottati dalle organizzazioni internazionali, quali Standard NIST, Standard ISO/IEC e COBIT.

Il Framework Nazionale amplia questa struttura inserendo due nuovi concetti: i livelli di priorità e i livelli di maturità. Questi due concetti permettono di tenere conto della struttura economica del nostro Paese fatta di alcune decine di grandi aziende e infrastrutture critiche e di una galassia di piccole imprese, rendendo dunque, di fatto, il Framework adatto alle PMI, ma conservando tuttavia la sua iniziale vocazione per Grandi Imprese e infrastrutture critiche.

3.1 Framework Core, Profile e Implementation Tier

Il Framework Nazionale eredita le tre nozioni fondamentali del Framework NIST: Framework Core, Profile e Implementation Tier. Di seguito ne diamo una breve descrizione autocontenuta, rimandando al documento originale [15] per maggiori dettagli.

Framework Core. Il core rappresenta la struttura del ciclo di vita del processo di gestione della cyber security, sia dal punto di vista tecnico sia organizzativo. Il core è strutturato gerarchicamente in Function, Category e Subcategory. Le Function, concorrenti e continue, sono: Identify, Protect, Detect, Respond, Recover e costituiscono le principali tematiche da affrontare per operare una adeguata gestione del rischio cyber in modo strategico. Il Framework quindi definisce, per ogni Function, Category e Subcategory, le quali forniscono indicazioni in termini di specifiche risorse, processi e tecnologie da mettere in campo per gestire la singola Function. Infine, la struttura del Framework core presenta degli *informative reference*, dei riferimenti informativi che legano la singola Subcategory a una serie di pratiche di sicurezza note utilizzando gli standard di settore (ISO, SP800-53r4, COBIT-5, SANS20 e altri). La struttura del Framework Core del NIST è riportata in Figura 3.1.

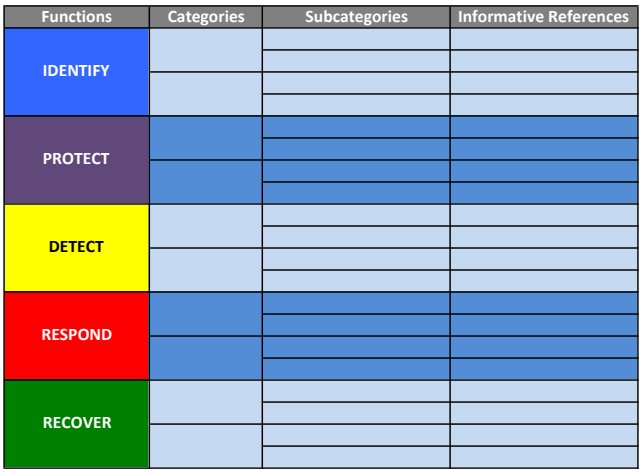

Figura 3.1: Struttura del Framework Core del NIST(da [15]).

Di seguito è riportata una breve descrizione delle 5 Function:
Identify. La Function *Identify* è legata alla comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati. Tale comprensione permette infatti a un'organizzazione di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali. Le Category all'interno di questa Function sono: Asset Management; Ambiente di business; Governance; Valutazione del rischio; Strategia di gestione del rischio.

Protect. La Function *Protect* è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica. Le Category all'interno di questa Function sono: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Detect. La Function *Detect* è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica. Le Category all'interno di questa Function sono: Anomalies and Events; Security Continuous Monitoring; and Detection Processes

Respond. La Function *Respond* è legata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica. Le Category all'interno di questa Function sono: Planning; Communications; Analysis; Mitigation; and Improvements.

Recover. La Function *Recover* è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente. L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle business operations. Le Category all'interno di questa Function sono: Recovery Planning; Improvements; and Communications.

Profile. I Profile rappresentano il risultato della selezione, da parte di un'organizzazione, di specifiche Subcategory del Framework. Tale selezione può avvenire in base a diversi fattori, guidati principalmente dal risk assessment, dal contesto di business, dall'applicabilità delle varie Subcategory. I profili possono essere utilizzati come opportunità per migliorare lo stato di sicurezza mettendo a confronto un profilo attuale (anche detto corrente), con un profilo desiderato (anche detto target). Per sviluppare un profilo, un'organizzazione deve esaminare ciascuna delle Subcategory e, sulla base di driver di business e della valutazione dei propri rischi, determinare quali sono da implementare e quali non sono applicabili nel proprio contesto. Le Subcategory potranno essere integrate con ulteriori pratiche non previste dal Framework al fine di gestire in maniera completa il rischio. Il profilo attuale può quindi essere utilizzato per definire priorità e misurare i progressi verso il profilo desiderato. I profili possono essere utilizzati, inoltre, per effettuare un'autovalutazione o per comunicare il proprio livello di gestione del rischio all'interno o all'esterno dell'organizzazione. Un utilizzo da non sottovalutare è, infine, quello della definizione di profili minimi richiesti da un'organizzazione per poter usufruire di servizi offerti da terzi. Utilizzo questo che rafforza l'intera supply chain in caso di particolari criticità.

Implementation Tier. Gli implementation Tier forniscono contesto su come l'azienda, nel suo complesso, veda il rischio cyber e i processi posti in essere per gestirlo. Sono previsti quattro livelli di valutazione, dal più debole al più forte: (1) Parziale, (2) Informato, (3) Ripetibile, (4) Adattivo. In particolare:

Parziale. Un modello di gestione del rischio di cyber security di una organizzazione è parziale se questo non tiene conto in modo sistematico del rischio cyber o delle minacce ambientali.

Informato. Un modello di gestione del rischio cyber di una organizzazione è informato se l'organizzazione ha dei processi interni che tengono conto del rischio cyber, ma questi non sono estesi a tutta l'organizzazione.

Ripetibile. Un modello di gestione del rischio cyber di una organizzazione è ripetibile se l'organizzazione aggiorna regolarmente le proprie pratiche di cyber security basandosi sull'output del processo di risk management.

Adattivo. Un modello di gestione del rischio cyber di una organizzazione è adattivo se l'organizzazione adatta le sue procedure di cyber security frequentemente attraverso l'utilizzo delle esperienze passate e degli indicatori di rischio.

3.2 I livelli di priorità

I livelli di priorità permettono di supportare le organizzazioni e le aziende nell'identificazione preliminare delle Subcategory da implementare per ridurre maggiormente i livelli di rischio a cui sono sottoposte, bilanciandone l'impegno da profondere per la loro attuazione. Il Framework suggerisce l'utilizzo di una scala di priorità a tre livelli tra le Subcategory. L'obiettivo è quello di:

- semplificare l'individuazione delle Subcategory essenziali da implementare immediatamente e inderogabilmente;
- supportare le organizzazioni durante il processo di analisi e gestione del rischio.

Figura 3.2: Framework Nazionale con livelli di priorità relativi alle Subcategory e con linee guida.

La determinazione dei livelli di priorità assegnati alle Subcategory deve essere effettuata sulla base di due specifici criteri:

- capacità di ridurre il rischio cyber, agendo su uno o più dei fattori chiave per la determinazione, ovvero:
  - esposizione alle minacce, intesa come l'insieme dei fattori che aumentano o diminuiscono la facilità con cui la minaccia stessa può manifestarsi;
  - probabilità di loro accadimento, ovvero la frequenza con cui una specifica minaccia può verificarsi nel tempo;
  - impatto conseguente sulle Business Operations o sugli Asset aziendali, intesa come l'entità del danno conseguente al verificarsi di una minaccia;
- semplicità di implementazione delle Subcategory, anche considerando il livello di maturità tecnica e organizzativa tipicamente richiesto per realizzare la specifica azione.

La combinazione dei due criteri sopra descritti ha permesso di definire tre livelli distinti di priorità:

- Priorità Alta: interventi che permettono di ridurre sensibilmente uno dei tre fattori chiave del rischio cyber. Questi interventi sono prioritari e per loro natura sono da attuare indipendentemente dalla complessità realizzativa degli stessi;
- Priorità Media: interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber e che risultano generalmente anche di semplice implementazione;
- Priorità Bassa: interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber, ma la cui complessità realizzativa è generalmente considerata elevata (ad esempio cambiamenti organizzativi rilevanti e/o modifiche infrastrutturali significative).

Da notare che le Subcategory assumono priorità specifica per la contestualizzazione adottata oppure assumono priorità specifica al contesto dell'organizzazione (eventualmente basati sulla valutazione del rischio associato), pertanto ogni organizzazione, nell'adozione del Framework o nel corso dell'attività di contestualizzazione, potrebbe ridefinire specifici livelli di priorità per ogni Subcategory.
L'appendice 6 presenta una contestualizzazione del Framework per le PMI, con la definizione del livello di priorità per ogni Subcategory e una guida all'implementazione.

3.3 I livelli di maturità

I livelli di maturità permettono di fornire una misura della maturità di un processo di sicurezza, della maturità di attuazione di una tecnologia specifica o una misura della quantità di risorse adeguate impiegate per l'implementazione di una data Subcategory.

I livelli di maturità forniscono un punto di riferimento in base al quale ogni organizzazione può valutare la propria implementazione delle Subcategory e fissare obiettivi e priorità per il loro miglioramento. I livelli devono essere in progressione, dal minore al maggiore. Ogni livello deve prevedere pratiche e controlli incrementali rispetto al livello di maturità inferiore. Un'organizzazione valuterà la soddisfazione dei controlli per identificare il livello di maturità raggiunto (Figura 3.3). Per alcune Subcategory potrebbe non essere possibile definire livelli di maturità (si veda la Subcategory ID.GV-3 in 6.3 come esempio).

Figura 3.3: Framework Nazionale con introduzione dei livelli di maturità.

Nelle Tabelle 3.1 e 3.2 sono forniti due esempi di livelli di maturità per due Subcategory del Framework, mentre nella Sezione 6.3 sono riportati i livelli di maturità per tutte le Subcategory a priorità alta della contestualizzazione per PMI fornita.

Tabella 3.1: Esempio di livelli di maturità per Subcategory “PR.AC-1: PR.AC-1:Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate”.

Livello	Descrizione
M1	Le identità e le credenziali sono amministrate localmente su ciascun dispositivo o sistema IT.
M2	Le identità e le credenziali sono amministrate attraverso una directory aziendale che consente l’applicazione omogenea di regole e livelli minimi di sicurezza.
M3	Specifiche soluzioni tecnologiche sono adottate per gestire in maniera specifica e appropriata le utenze privilegiate (es. Amministratori di Sistema).

Tabella 3.2: Esempio di livelli di maturità per la Subcategory “ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell’organizzazione”.

Livello	Descrizione
M1	M1.1. L’azienda ha definito una strategia per la cyber Security.
M2	M2.1. All’interno della strategia sono definiti gli obiettivi e le attività di cyber Security dell’organizzazione. M2.2. La strategia è allineata con gli obiettivi strategici e rischi aziendali. M2.3. La strategia definisce l’approccio per la Governance della cyber security. M2.3. La strategia definisce la struttura e l’organizzazione per la realizzazione del programma. M2.4. La strategia è approvata dal Consiglio di Amministrazione.
M3	M3.1. La strategia è aggiornata regolarmente per tenere conto dei cambiamenti di business, cambiamenti nel contesto operativo, e cambiamenti nel profilo di rischio.

Si devono prevedere le seguenti caratteristiche nella definizione dei livelli di maturità:

- Specificità per Subcategory. Un’organizzazione potrà avere livelli differenti di maturità per Subcategory differenti;
- Completezza delle pratiche di sicurezza. Il livello di maturità di una Subcategory è almeno quello in cui tutte le relative pratiche di sicurezza sono effettuate.

Questo consente di:

- Definire il proprio livello di maturità in maniera parziale o complessiva;
- Identificare il livello desiderato: parziale o complessivo;
- Identificare le pratiche di sicurezza necessarie per raggiungere il livello desiderato.

In generale il Framework fornisce solo delle regole per la definizione dei livelli di maturità e di priorità, poiché questi e i relativi controlli sono estremamente caratterizzati dalla natura dell’organizzazione, dal settore in cui opera, dalla struttura e dalla sua dimensione, nonché dal modello di business che segue. Relativamente al contesto delle PMI, invece, il presente documento presenta una contestualizzazione specifica in cui vengono presentate le priorità per questo segmento di aziende e il minimo livello di maturità da prevedere per innalzare la propria capacità di gestione del rischio Cyber.

3.4 Come contestualizzare il Framework

Contestualizzare un Framework per un settore produttivo o per una categoria omogenea di organizzazioni significa specificare il suo core (ovvero selezionare le Function, Category e Subcategory) e specificare i livelli di priorità e maturità per le Subcategory selezionate. Fino a questo momento, tutte le nozioni introdotte sono agnostiche rispetto, ad esempio, al settore produttivo, alla tipologia degli impiegati, alla dimensione e alla dislocazione sul territorio dell'organizzazione. Quando si contestualizza il Framework, tutti o alcuni degli elementi precedentemente descritti devono essere tenuti in considerazione. Una caratterizzazione del Framework si crea attraverso i seguenti passi:

1. selezionare l'elenco delle Function/Category/Subcategory che sono pertinenti per l'organizzazione in base a tutti o alcuni dei precedenti elementi (settore produttivo, dimensione e dislocazione sul territorio dell'organizzazione, ecc.);

2. definire i livelli di priorità per l'implementazione per le Subcategory selezionate;

3. definire delle linee guida almeno per le Subcategory a priorità alta;

4. specificare i livelli di maturità almeno per le Subcategory a priorità alta.

Tutte le organizzazioni che si appoggiano a una specifica contestualizzazione del Framework devono sempre implementare le Subcategory a priorità alta, almeno al livello minimo di maturità.

3.4.1 Chi può creare una contestualizzazione del Framework

Le operazioni precedenti devono essere implementate in funzione delle specifiche caratteristiche di business dell'organizzazione. Di seguito una lista di casistiche relative ai soggetti cui può essere demandata la contestualizzazione del Framework. Il Framework può essere contestualizzato:

1. dalla singola azienda per la gestione del suo programma di cyber security, Questo prevede che l'azienda sia abbastanza matura da poter gestire i passi precedenti e il successivo modello di gestione del rischio associato. Ad esempio, Intel è stata una delle prime a fornire un caso di studio su come contestualizzare il Framework Nazionale di cyber security del NIST [9];

2. da una associazione di settore produttivo, per rendere la contestualizzazione del Framework disponibile a tutte le aziende del settore. Questa contestualizzazione può anche tenere conto della dimensione delle aziende. Ad esempio, il gruppo di lavoro IV del CSRIC (The Communications Security, Reliability and Interoperabiity Council) ha fornito una contestualizzazione del Framework per il settore delle comunicazioni che include produttori di satelliti, di reti televisive, di reti fisse e di reti wireless negli Stati Uniti [18];

3. da un regolatore di settore per rendere la contestualizzazione del Framework disponibile a tutte le organizzazioni del settore. La contestualizzazione può anche tenere conto della dimenzione delle aziende oltre che delle specificità del settore regolato;

4. da un qualsiasi attore che definisce una contestualizzazione del Framework in funzione di una o più caratteristiche che accomunano delle aziende, come ad esempio, dislocazione geografica, dimensione, tipologia del personale ecc. Un caso tipico può essere quello di un raggruppamento locale di piccole-medie imprese che usufruiscono di servizi da parte di un consorzio. Quest'ultimo può contestualizzare per tali aziende il Framework. In ultimo, questo documento presenta, nella Parte II, una contestualizzazione del Framework per PMI fatta da un gruppo misto di accademici e professionisti della sicurezza informatica. Questa contestualizzazione rientra quindi in questa categoria.

Da notare che ogni singola organizzazione, anche se viene fornita di una contestualizzazione da parte di un regolatore o da una organizzazione di settore, può definire e includere ulteriori Subcategory o specializzarne di esistenti in base ai propri obiettivi di business e di cyber security.

3.5 Come aggiornare il Framework

Il Framework è un documento vivo e come tale va regolarmente aggiornato in base al cambiamento della minaccia e degli avanzamenti tecnologici e organizzativi. Quindi devono essere periodicamente rivisti il core (category e Subcategory), le priorità, i livelli di maturità e l'implementation Tier. Gli organi istituzionali sono i responsabili per la definizione delle contestualizzazioni del Framework e della loro evoluzione e mantenimento nel tempo. Gli organi istituzionali sono anche responsabili di stabilire appropriate relazioni internazionali in modo da tenere il Framework allineato con evoluzioni che possono avvenire in altri paesi. Inoltre, tali organi dovrebbero gestire regolari revisioni coinvolgendo le principali aziende italiane e i regolatori di settore. L'individuazione degli specifici soggetti che potranno compiere queste azioni è al di là dello scopo del presente documento.

Le associazioni di categoria di specifici settori produttivi, se decidono di contestualizzare il Framework, dovranno poi recepirne i cambiamenti avvenuti a livello istituzionale e dovranno aggiornare la loro contestualizzazione. Lo stesso vale per gli enti regolatori che dovranno emettere regolamenti specifici che specializzino gli aggiornamenti. Le aziende dovranno anche loro recepire le nuove contestualizzazioni o direttamente dall'ente istituzionale o dall'ente di settore e provvedere all'implementazione del Framework.

In ultimo, durante il processo di contestualizzazione del Framework, si potrebbero anche definire Subcategory che non fanno parte del Framework Core originale. A questo punto gli estensori del Framework dovrebbero contattare l'organizzazione che gestisce il Framework per un possibile inserimento della Subcategory in una futura versione. In Figura 3.4 vengono riassunti i vari livelli di aggiornamento del Framework Nazionale nel caso dei settori regolati.

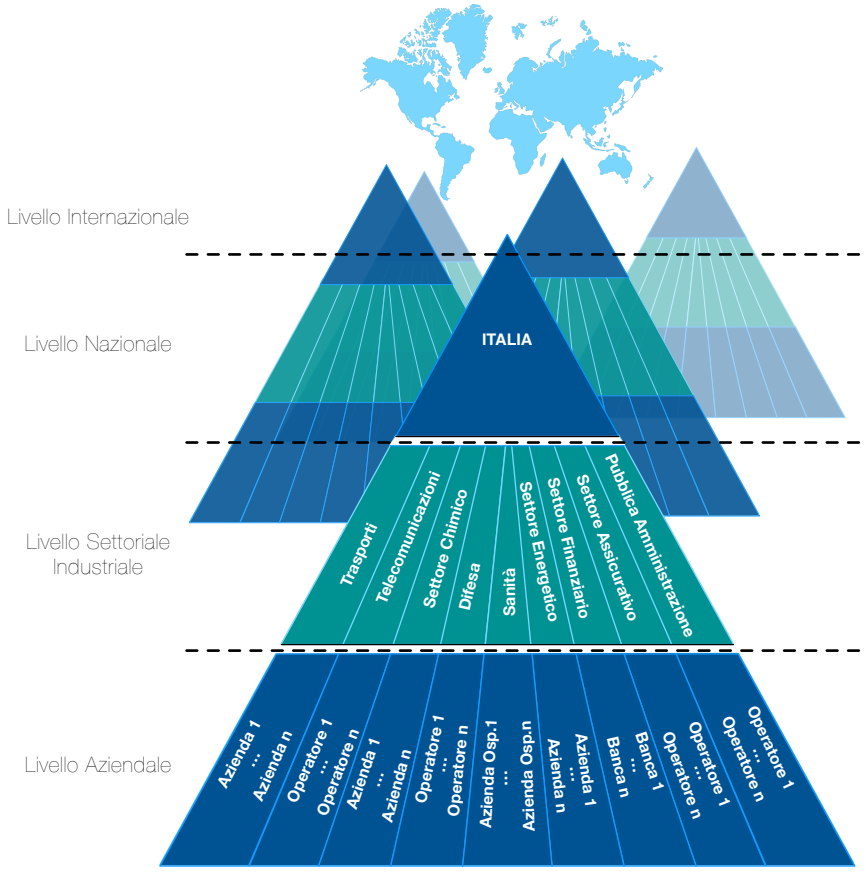

Figura 3.4: Contesto internazionale, nazionale, di settore e aziendale per i settori regolati.

4. Linee guida per l'applicazione del Framework

Questo Capitolo complementa il precedente fornendo una guida all'utilizzo del Framework per diversi attori. In particolare vengono considerate le piccole-medie imprese, le Grandi Imprese, le infrastrutture critiche e le infrastrutture critiche per il paese. Infine viene anche analizzato come il Framework possa essere usato da un regolatore di settore.

4.1 Piccole-Medie Imprese

Figura 4.1: Processo di adozione del Framework Nazionale di cyber security da parte delle PMI.

L'applicazione del Framework da parte di una PMI dovrebbe avvenire in sei passaggi, illustrati in Figura 4.1. In particolare:

1. *Identificare una contestualizzazione del Framework.* La PMI deve definire la contestualizzazione più adatta ai propri obiettivi di business e alle proprie criticità. Questa attività può essere anche svolta partendo da una contestualizzazione pubblicamente disponibile,

adattandola alla specifica realtà in cui la PMI opera. Nel caso la PMI operi in un settore regolato, questa potrà fare riferimento aduna contestualizzazione eventualmente definita dall'ente regolatore;

2. *Implementare le Subcategory a priorità alta*. La PMI dovrebbe iniziare l'applicazione del Framework implementando le Subcategory a "priorità alta" (Sezione 3.2). Tali Subcategory vanno implementate almeno al primo livello di maturità (Sezione 3.3). Questo è un passo critico nell'implementazione del Framework e consente di ottenere un livello base di preparazione e consapevolezza del rischio cyber;

3. *Identificare sistemi e asset*. L'individuazione dei sistemi ICT e delle informazioni che la PMI ritiene vitali o comunque critiche per garantire l'operatività della PMI stessa. Tale passaggio è importante soprattutto per le fasi successive, in quanto consente di valutare propriamente gli impatti durante l'analisi dei rischi e di agevolare pertanto la comprensione delle effettive necessità di protezione;

4. *Analizzare il rischio e il profilo corrente.* Determinare il *profilo corrente* basato sulla contestualizzazione del Framework adottato dalla PMI e analizzare il rischio associato. Sebbene il Framework contenga una lista di misure di sicurezza prioritarie rispetto alle altre, ciascuna organizzazione ha le sue peculiarità esterne (ad esempio mercato in cui opera, tipologia di clienti, ecc.) e interne (ad esempio modello organizzativo e gestionale, prodotti o soluzioni offerte, distribuzione territoriale, ecc.). Tutto ciò determina livelli di esposizione a rischi differenti per ciascuna organizzazione, che devono essere determinati mediante un'analisi specifica dei rischi cyber. Si precisa che la metodologia con cui determinare e valutare i rischi dovrebbe essere individuata da ciascuna organizzazione in relazione alle specifiche caratteristiche organizzative e di mercato nel quale si opera. Analogamente la PMI dovrebbe valutare il livello di attuazione delle singole Subcategory del Framework, con l'obiettivo di determinare il profilo di protezione attuale;

5. *Individuare il profilo target e determinare il gap rispetto al profilo corrente*. Una volta individuato il proprio profilo corrente e in funzione dei livelli di rischio individuati, la PMI dovrebbe essere in condizione di stabilire le proprie necessità di protezione. Ciò significa definire un *profilo target*: un insieme di Subcategory correlato, per ognuna di queste, dal livello di maturità che si vuole raggiungere. Il profilo target costituisce la base con cui comparare il profilo corrente, determinando quindi i gap esistenti nella gestione della cyber security;

6. *Definire e attuare piano di azione per raggiungere il profilo target*. L'ultima fase nel processo di adozione del Framework consiste nel definire l'insieme di attività necessarie a raggiungere il profilo target di protezione definito nella fase precedente. Ciò significa elaborare un piano specifico per implementare le pratiche di sicurezza del Framework, secondo un piano temporale che varierà in relazione agli effettivi rischi individuati e in funzione delle condizioni specifiche in cui opera la PMI.

È chiaro che sarebbe auspicabile una continua evoluzione nell'implementazione del Framework, anche successivamente al raggiungimento del profilo target, in linea con le cicliche fasi di risk assessment e le conseguenti azioni di miglioramento continuo.

L'adozione del Framework potrà essere ulteriormente semplificata impiegando strumenti informatici specifici, in grado di guidare le aziende nella corretta esecuzione dei passaggi descritti. Infine, da notare che nelle PMI è anche importante definire chi ha la responsabilità di implementare i passi del Framework. Infatti le PMI potrebbero non avere figure come il CISO dedicate a questo

ambito nelle Grandi Imprese. In questo caso è l'amministratore delegato che dovrà individuare la o le persone responsabili di questa implementazione nella azienda.

4.2 Grandi Imprese

Le Grandi Imprese potranno impiegare il Framework come strumento a supporto del processo di gestione e trattamento del rischio cyber. È plausibile che in queste realtà si siano già avviati da tempo programmi di cyber security, in ragione dei quali l'introduzione del Framework è da intendersi non tanto per sostituire quanto già in essere, ma come ulteriore riferimento al fine di:

- migliorare o definire, se non presente, un programma di cyber security in maniera strutturata e integrata, fondato sulla gestione del rischio, che possa essere implementato in presenza di modelli preesistenti di governance della security;
- permettere di determinare agevolmente il livello di maturità delle attività di cyber security identificando, a seconda dei casi, gli interventi migliorativi o di razionalizzazione dei costi di sicurezza, a favore di una redistribuzione ragionata delle risorse;
- completare benchmark tra aziende e organizzazioni operanti in settori specifici o aventi analoghe caratteristiche che possano, a livello nazionale, favorire il miglioramento dei livelli di sicurezza, abilitando contestualmente il mercato della cyber insurance;
- agevolare e facilitare la comunicazione con il top management (ad esempio amministratori e consigli di amministrazione, azionisti ecc.) e con gli interlocutori esterni (ad esempio agenzie di rating, fornitori e partner), affinché siano rappresentati chiaramente i livelli di rischio cyber al quale le organizzazioni sono esposte e affinché siano identificati gli investimenti e le risorse da mettere in campo per un adeguata riduzione del rischio.

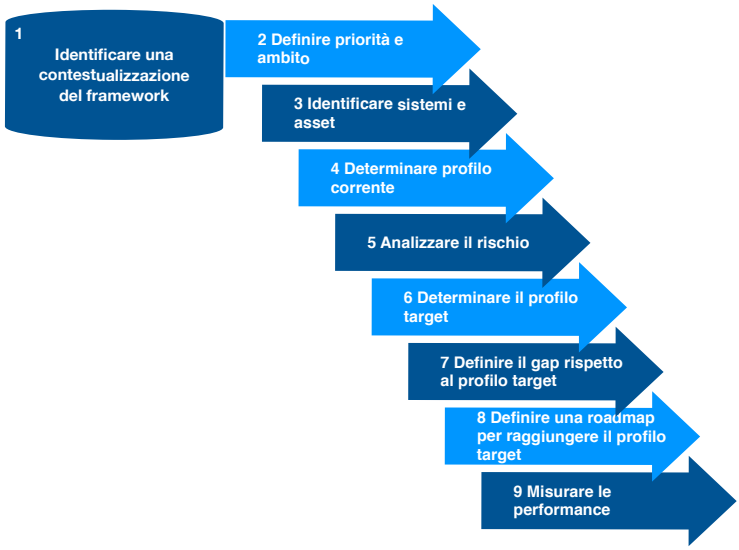

Figura 4.2: Processo di adozione del Framework Nazionale di cyber security da parte delle Grandi Imprese e infrastrutture critiche

Con riferimento alla Figura 4.2, l'applicazione del Framework dovrebbe avvenire in nove passaggi, di seguito illustrati:

1. *Identificare una contestualizzazione del Framework.* Nel caso in cui la grande impresa appartenga ad un settore regolato, questa dovrebbe utilizzare una delle contestualizzazioni fornite dal proprio regolatore di settore. Nel caso in cui la grande impresa non appartenga ad un settore regolato deve identificare tra le contestualizzazioni disponibili quella da utilizzare nel processo di implementazione del Framework. Da notare che la contestualizzazione selezionata non è un regolamento da seguire, ma una linea guida. Potrebbe quindi essere modificata in base ai propri obiettivi di business e alle proprie criticità. Si noti, inoltre, che la grande impresa, a differenza delle PMI, potrebbe avere le capacità per definire una propria contestualizzazione del Framework;

2. *Definire priorità e ambito*. Identificare periodicamente gli obiettivi strategici e le priorità di business dell'organizzazione in modo da selezionare aree e funzioni chiave che necessitino specifica focalizzazione;

3. *Identificare sistemi e asset*. Individuazione delle informazioni e dei sistemi informatici (sia dell' ambito IT che di quello industriale) che l'organizzazione ritiene vitali e critici per garantire l'operatività dell'organizzazione stessa. Tale passaggio è importante soprattutto per le fasi successive, in quanto consente di valutare propriamente gli impatti durante l'analisi dei rischi e di agevolare pertanto la comprensione delle effettive necessità di protezione;

4. *Determinare il profilo corrente*. È previsto che sia valutato lo stato di implementazione e il livello di maturità per ciascuna Subcategory del Framework. Questo permette di definire uno o più profili correnti in relazione alle aree/funzioni previste per l'implementazione del programma;

5. *Analizzare il rischio*. Determinare e valutare i rischi mediante l'adozione di una metodologia considerata appropriata, in relazione alle specifiche caratteristiche organizzative e di mercato nel quale opera l'organizzazione. Alcuni spunti in merito al processo di analisi e gestione dei rischi sono forniti nel paragrafo 7.2;

6. *Determinare il profilo target*. Attraverso il processo di trattamento del rischio, l'organizzazione deve poter definire un profilo target che, differentemente da quello corrente, rappresenta il livello di implementazione e di maturità che si ambisce a conseguire per ciascuna Subcategory del Framework. È auspicabile che la selezione di tali livelli possa essere effettuata avendo a priori integrato il cyber security risk management all'interno del programma di enterprise risk management, in modo che la gestione del rischio cyber possa beneficiare di decisioni prese al livello organizzativo più elevato (i.e., top management), avvalendosi di una visione sistemica complessiva a supporto del processo decisionale;

7. *Determinare il gap rispetto al profilo target*. Completare una comparazione tra il profilo target e quello corrente per identificare i gap esistenti nella gestione della cyber security;

8. *Definire e attuare una roadmap per raggiungere il profilo target*. La fase attuativa del processo di adozione del Framework consiste nel definire l'insieme di attività necessarie a raggiungere il profilo target determinato nella fase precedente. Ciò significa elaborare un piano specifico per realizzare i singoli controlli del Framework, secondo un piano temporale che varierà in relazione agli effettivi rischi individuati e in funzione delle condizioni specifiche in cui opera la singola organizzazione;

9. *Misurare le performance*. Affinché l'efficienza del profilo target sia oggetto di revisioni periodiche e miglioramento continuo, è necessario che siano definite delle metriche di monitoraggio in grado di evidenziarne anche i costi operativi. Le valutazioni sull'efficienza del profilo corrente devono essere utilizzate per definire il nuovo profilo target.

È previsto che il Framework possa essere impiegato per la valutazione del livello di maturità delle attività e processi di cyber security. Questa applicazione, complementare alla precedente, prevede un processo più snello che permetta di valutare rapidamente i gap esistenti e di definire un piano di azione per il loro miglioramento. Il processo operativamente prevede passaggi analoghi a quelli descritti in precedenza, fatto salvo per il passaggio relativo alla valutazione del rischio.
Un ampio impiego del Framework da parte delle Grandi Imprese potrà fornire nuovi criteri per l'analisi e la mitigazione del rischio che partiranno da riscontri scaturiti direttamente dagli insegnamenti appresi (lessons learned). Queste indicazioni potranno garantire attualità e rilevanza al Framework. Ogni organizzazione coinvolta è pertanto invitata a partecipare attivamente allo sviluppo, alla convalida e all'implementazione del Framework.

4.3 Infrastrutture Critiche

Le Infrastrutture Critiche, analogamente alle Grandi Imprese, potranno adottare il Framework per supportare il processo di gestione e trattamento del rischio cyber, oltre a implementare opportune attività di cyber intelligence da effettuarsi privatamente e/o in cooperazione con le autorità, secondo le modalità previste per il settore in cui operano. Inoltre, potranno adottare il Framework al fine di:

- monitorare la minaccia, che deve essere considerata un elemento dinamico, attraverso l'attivazione di opportuni canali di cyber intelligence e di cooperazione con le autorità;
- incrementare la sicurezza della catena di approvvigionamento dei servizi. Le infrastrutture critiche potrebbero richiedere, ai propri fornitori di servizi, di avere un particolare profilo minimo o associare un profilo minimo al singolo servizio;
- rappresentare alle autorità preposte un quadro sintetico e armonico del livello di esposizione delle Infrastrutture Critiche, al fine di agevolare interventi correttivi sia riguardanti il piano di protezione sia il quadro normativo vigente.

Le fasi dell'applicazione del Framework per le Infrastrutture Critiche sono le medesime di quelle per le Grandi Imprese, con alcuni importanti distinguo:

- per quanto riguarda la fase 3, "Identificare sistemi e asset", oltre a quanto previsto per le Grandi Imprese, l'infrastruttura critica deve identificare gli obiettivi sensibili per il proprio esercizio e le interconnessioni con altre infrastrutture critiche che di fatto costituiscono interdipendenze sistemiche. Grazie a tale passaggio, e all'adozione di strumenti specifici per l'analisi di scenario, per la valutazione degli impatti e per il supporto alle decisioni, potranno essere valutati propriamente gli impatti specifici (es. impatto sulla safety) in fase di analisi dei rischi, evidenziati gli scenari di potenziale effetto domino e quindi comprese le effettive necessità di protezione;
- per quanto riguarda la fase 6, "Determinare il profilo target", oltre a quanto previsto per le Grandi Imprese, l'infrastruttura critica e in particolare il suo management, in questa fase deve avvalersi di una visione sistemica complessiva a supporto del processo decisionale, che tenga conto del bilanciamento tra strategia organica di protezione delle infrastrutture critiche e gli obiettivi intrinseci di difesa civile.

4.4 Regolatori di settore

Un regolatore può avere due ruoli nel ciclo di vita del Framework. Il primo, descritto nel Capitolo precedente, è quello di tenere allineate le proprie contestualizzazioni del Framework con il Framework istituzionale. Il secondo è quello di aggiornare la regolamentazione di settore utilizzando come riferimento le Category e Subcategory del Framework. Questo vale a maggior ragione per gli enti in grado di legiferare a livello nazionale. Una volta aggiornata la regolamentazione in relazione al Framework, si deve creare una mappatura tra Subcategory e regolamentazione, si devono aggiornare livelli di priorità e livelli di maturità. A quel punto il Framework aggiornato viene notificato alle organizzazioni che fanno parte del settore regolato. Il Framework quindi rappresenta anche un modo di fare evolvere le regolamentazioni fatte da diversi enti regolatori in modo omogeneo e coerente.

PARTE II - Documenti di supporto al Framework

5. Framework Core

Questo Capitolo riporta l'elenco delle Function, Category e Subcategory del Framework NIST, opportunamente tradotte e adattate al contesto aziendale italiano. La numerazione, l'ordine e la tematica di ogni Subcategory è coerente al Framework NIST, di conseguenza c'è piena compatibilità tra il Framework qui presentato e il Framework NIST originale. Questa compatibilità implica che un profile fornito da una qualunque organizzazione a livello globale (in rete ci sono già diversi esempi) sia perfettamente confrontabile con il Framework Nazionale. Si ricorda però che il Framework Nazionale consente la creazione di profili più complessi grazie al concetto di livelli di maturità.
Si noti che nella colonna "Informative References", oltre a riportare gli stessi riferimenti del Framework NIST, sono stati aggiunti, in grassetto, a titolo meramente esemplificativo e non esaustivo, alcuni dei principali obblighi derivanti dalla normativa italiana in materia di privacy. Nel caso siano presenti questi obblighi, la colonna presenta, in corrispondenza della Subcategory, la norma relativa e quando considerarla (es. quando l'organizzazione tratta dati personali). In tali casi è superfluo ricordare che, indipendentemente dal Livello di Priorità previsto, il controllo è da considerarsi obbligatorio e il relativo livello di maturità dovrà corrispondere con quello previsto dalla normativa in questione. Vengono riportati in tale colonna anche gli obblighi per le Pubbliche Amministrazioni[1] dettati dal Codice dell'Amministrazione Digitale (CAD) con relativo articolo, in accordo a quanto descritto in Sezione 11.1. Maggiori dettagli sul contesto normativo italiano in relazione al Framework sono riportati nella Sezione 10.

[1] Si noti che, per quanto riguarda la Subcategory ID.AM-5, l'obbligatorietà può essere dedotta dalla necessità di predisporre il piano, che dovrà necessariamente prevedere il censimento delle risorse e una qualche forma di loro valorizzazione, con conseguente prioritizzazione.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi di business e con la strategia di rischio dell'organizzazione	**ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione**	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati.	· CCS CSC 1 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Le risorse (es: hardware, dispositivi, dati e software) sono prioritizzati in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	· COBIT 5 APO03.03, APO03.04, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 · **Obbligatorio per le PP.AA. ai sensi dell'art. 50-bis, comma 3, lett. a) del CAD**
		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
	Business Environment (ID.BE): La mission dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono compresi e valutate in termini di priorità. Tali informazioni influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.	**ID.BE-1:Il ruolo dell'organizzazione all'interno della filiera produttiva è identificato e reso noto**	· COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 · NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: Il ruolo dell'organizzazione come infrastruttura critica e nel settore industriale di riferimento è identificato e reso noto	· COBIT 5 APO02.06, APO03.01 · NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione.	· COBIT 5 APO02.01, APO02.06, APO03.01 · ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 · NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.BE-4: Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici	· ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 · NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici	· COBIT 5 DSS04.02 · ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14
	Governance (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1: E' indetificata e resa nota una policy di sicurezza delle informazioni**	· COBIT 5 APO01.03, EDM01.01, EDM01.02 · ISA 62443-2-1:2009 4.3.2.6 · ISO/IEC 27001:2013 A.5.1.1 · NIST SP 800-53 Rev. 4 -1 controls from all families · **Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 novembre 2015 e dei relativi decreti n. 4/2015 e n.5/2015**
		ID.GV-2: Ruoli e responsabilità inerenti la sicurezza delle informazioni sono coordinati ed allineati con i ruoli interni ed i partner esterni	· COBIT 5 APO13.12 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 · NIST SP 800-53 Rev. 4 PM-1, PS-7

Function	Category	Subcategory	Informative References
IDENTIFY (ID)		**ID.GV-3: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti**	· COBIT 5 MEA03.01, MEA03.04 · ISA 62443-2-1:2009 4.4.3.7 · NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1) · ISO/IEC 27001:2013 A.18.1 · **Obbligatoria ai sensi del D.Lgs. 196/2003** · **Obbligatorio ai sensi dei provvedimenti del Garante per la protezione dei dati personali** · **Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 novembre 2015 e dei relativi decreti n. 4/2015 e n.5/2015**
		ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · NIST SP 800-53 Rev. 4 PM-9, PM-11
	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente l' operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate**	· CCS CSC 4 · COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: L'organizzazione riceve informazioni su minacce e vulnerabilità da fonti esterne (e.g. CERT, fonti aperte, forum di information sharing)	· ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · ISO/IEC 27001:2013 A.6.1.4 · NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5
		ID.RA-3: Le minacce, sia interne che esterne, sono identificate e documentate	· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Sono identificati i potenziali impatti sul business e le relative probabilità di accadimento	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	· COBIT 5 APO12.02 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
		ID.RA-6: Sono identificate e prioritizzate le risposte al rischio	· COBIT 5 APO12.05, APO13.02 · NIST SP 800-53 Rev. 4 PM-4, PM-9
	Risk Management Strategy (ID.RM): Le priorità e i requisiti dell'organizzazione e la tolleranza al rischio sono definiti e utilizzati per supportare le decisioni sul rischio operazionale.	**ID.RM-1: I processi di risk management sono stabiliti, gestiti e concordati tra i responsabili dell'organizzazione (c.d. stakeholder)**	· COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · ISA 62443-2-1:2009 4.3.4.2 · NIST SP 800-53 Rev. 4 PM-9
		ID.RM-2: Il rischio tollerato dall'organizzazione è identificato ed espresso chiaramente	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.2.6.5 · NIST SP 800-53 Rev. 4 PM-9
		ID.RM-3: Il rischio tollerato è determinato tenendo conto del ruolo dell'organizzazione come infrastruttura critica e dei rischi specifici presenti nel settore industriale di appartenenza	· NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14
PROTECT (PR)	**Access Control (PR.AC): L'accesso agli asset ed alle relative risorse è limitato al personale, ai processi, ai dispositivi, alle attività ed alle transazioni effettivamente autorizzate**	**PR.AC-1:Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate**	· CCS CSC 16 · COBIT 5 DSS05.04, DSS06.03 · ISA 62443-2-1:2009 4.3.3.5.1 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · NIST SP 800-53 Rev. 4 AC-2, IA Family · **Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 novembre 2015 e dei relativi decreti n. 4/2015 e n.5/2015** · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regole 1-10)**

Function	Category	Subcategory	Informative References
PROTECT (PR)		**PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato**	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 · ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003)**
		PR.AC-3: L'accesso remoto alle risorse è amministrato	· COBIT 5 APO13.01, DSS01.04, DSS05.03 · ISA 62443-2-1:2009 4.3.3.6.6 · ISA 62443-3-3:2013 SR 1.13, SR 2.6 · ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regole 1-10)** · **Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 novembre 2015 e dei relativi decreti n. 4/2015 e n.5/2015**
		PR.AC-4: Gli accessi alle risorse sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	· CCS CSC 12, 15 · ISA 62443-2-1:2009 4.3.3.7.3 · ISA 62443-3-3:2013 SR 2.1 · ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 · NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regole 12,13,14)**
		PR.AC-5:L'integrità di rete è protetta, anche applicando la segregazione di rete dove appropriata	· ISA 62443-2-1:2009 4.3.3.4 · ISA 62443-3-3:2013 SR 3.1, SR 3.8 · ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, SC-7
	Awareness and Training (PR.AT): Il personale e le terze sono sensibilizzate e formate in materia di cybersecurity e ricevono adeguata preparazione, coerente con le politiche, le procedure e gli accordi esistenti, per svolgere correttamente i compiti e le responsabilità legate alla sicurezza delle informazioni	**PR.AT-1: Tutti gli utenti sono informati e addestrati**	· CCS CSC 9 · COBIT 5 APO07.03, BAI05.07 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.7.2.2 · NIST SP 800-53 Rev. 4 AT-2, PM-13 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regole 4, 9, 18, 21, 27, 28)**
		PR.AT-2: Gli utenti privilegiati (e.g. Amministratori di Sistema) comprendono ruoli e responsabilità	· CCS CSC 9 · COBIT 5 APO07.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 AT-2, PM-13 · **Provvedimento Garante Privacy del 27 novembre 2008** · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003)**
		PR.AT-3: Tutte le terze parti (es. fornitori, clienti, partner) comprendono ruoli e responsabilità	· CCS CSC 9 · COBIT 5 APO07.03, APO10.04, APO10.05 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 PS-7, SA-9
		PR.AT-4: I dirigenti ed i vertici aziendali comprendono ruoli e responsabilità	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.AT-5: Il personale addetto alla sicurezza fisica e delle informazioni comprende i ruoli e le responsabilità	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13

Function	Category	Subcategory	Informative References
PROTECT (PR)	Data Security (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1: I dati e le informazioni memorizzate sono protette**	· CCS CSC 17 · COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 · ISA 62443-3-3:2013 SR 3.4, SR 4.1 · ISO/IEC 27001:2013 A.8.2.3 · NIST SP 800-53 Rev. 4 SC-28 · **Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 novembre 2015 e dei relativi decreti n. 4/2015 e n.5/2015** · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regole 16,17, 20)**
		PR.DS-2: I dati sono protetti durante la trasmissione	· CCS CSC 17 · COBIT 5 APO01.06, DSS06.06 · ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SC-8 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003)**
		PR.DS-3:Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 · NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.DS-4: I sistemi hanno adeguate risorse a disposione per poter garantire la disponibilità	· COBIT 5 APO13.01 · ISA 62443-3-3:2013 SR 7.1, SR 7.2 · ISO/IEC 27001:2013 A.12.3.1 · NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
		PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	· CCS CSC 17 · COBIT 5 APO01.06 · ISA 62443-3-3:2013 SR 5.2 · ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003)**
		PR.DS-6: Vengono implementate tecniche di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni	· ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 · ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SI-7
		PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	· COBIT 5 BAI07.04 · ISO/IEC 27001:2013 A.12.1.4 · NIST SP 800-53 Rev. 4 CM-2
	Information Protection Processes and Procedures (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli assets.	**PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale**	· CCS CSC 3, 10 · COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.3 · ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni	· COBIT 5 BAI06.01, BAI01.06 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10

Function	Category	Subcategory	Informative References
PROTECT (PR)		**PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati periodicamente**	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.9 · ISA 62443-3-3:2013 SR 7.3, SR 7.4 · ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 · NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regola 18)**
		PR.IP-5: Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: I dati sono distrutti in conformità con le policy	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.4.4.4 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · NIST SP 800-53 Rev. 4 MP-6
		PR.IP-7: I processi di protezione sono migliorati in maniera continuativa	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: L'efficacia delle tecnologie di protezione è condivisa con i referenti appropriati	· ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
		PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	· COBIT 5 DSS04.03 · ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 · NIST SP 800-53 Rev. 4 CP-2, IR-8 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003)**
		PR.IP-10: I piani di risposta e recupero a seguito di incidenti/disastri sono verificati nel tempo	· ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.17.1.3 · NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14 · **Obbligatorio per le PP.AA. ai sensi dell'art. 50-bis, comma 3, lett. b) del CAD**
		PR.IP-11: Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, licenziamenti)	· COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 · NIST SP 800-53 Rev. 4 PS Family
		PR.IP-12:Viene sviluppato e implementato un piano di gestione delle vulnerabilità	· ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 · NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
	Maintenance (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti	**PR.MA-1:La manutenzione e la riparazione delle risorse e dei sistemi è svolta e registrata in modo tempestivo e portata a termine attraverso l'utilizzo di strumenti controllati ed autorizzati**	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.3.3.7 · ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 · NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5
		PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	· COBIT 5 DSS05.04 · ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 · ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 · NIST SP 800-53 Rev. 4 MA-4
	Protective Technology (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-1: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi**	· CCS CSC 14 · COBIT 5 APO11.04 · ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · NIST SP 800-53 Rev. 4 AU Family

Function	Category	Subcategory	Informative References
PROTECT (PR)		**PR.PT-2: I supporti di memorizzazione removibili sono protetti ed il loro uso è ristretto in accordo alle policy**	· COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 2.3 · ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003)**
		PR.PT-3: L'accesso alle risorse e ai sistemi è limitato secondo il principio di minima funzionalità	· COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · ISO/IEC 27001:2013 A.9.1.2 · NIST SP 800-53 Rev. 4 AC-3, CM-7 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regola 13)**
		PR.PT-4: Le reti di comunicazione e controllo sono protette	· CCS CSC 7 · COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7
DETECT (DE)	**Anomalies and Events (DE.AE): Le attività anomale sono rilevate tempestivamente e il loro impatto potenziale viene analizzato.**	**DE.AE-1: sono definite, rese note e gestite delle pratiche di riferimento (c.d. baseline) inerenti l'utilizzo della rete ed i flussi informativi attesi per utenti e sistemi**	· COBIT 5 DSS03.01 · ISA 62443-2-1:2009 4.4.3.3 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Gli eventi rilevati vengono analizzati per comprendere gli obiettivi e le metodologie dell'attacco	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Le informazioni relative agli eventi sono aggregate e correlate da sensori e sorgenti multiple	· ISA 62443-3-3:2013 SR 6.1 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Viene determinato l'impatto di un evento	· COBIT 5 APO12.06 · NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4
		DE.AE-5: Vengono definite delle soglie di allerta per gli incidenti	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.2.3.10 · NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati periodicamente per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity**	· CCS CSC 14, 16 · COBIT 5 DSS05.07 · ISA 62443-3-3:2013 SR 6.2 · NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: Viene svolto il monitoraggio degli spazi fisici per rilevare potenziali eventi di cybersecurity	· ISA 62443-2-1:2009 4.3.3.3.8 · NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Viene svolto il monitoraggio del personale per rilevare potenziali eventi di cybersecurity	· ISA 62443-3-3:2013 SR 6.2 · ISO/IEC 27001:2013 A.12.4.1 · NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 · **Da eseguirsi ai sensi dell'art. 23 del D. Lgs. n. 151/2015**
		DE.CM-4: Il codice malevolo viene rilevato	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.3.4.3.8 · ISA 62443-3-3:2013 SR 3.2 · ISO/IEC 27001:2013 A.12.2.1 · NIST SP 800-53 Rev. 4 SI-3

Function	Category	Subcategory	Informative References
		DE.CM-5: Il codice non autorizzato su dispositivi mobili viene rilevato	· ISA 62443-3-3:2013 SR 2.4 · ISO/IEC 27001:2013 A.12.5.1 · NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44
		DE.CM-6: Viene svolto il monitoraggio delle attività dei service provider esterni per rilevare potenziali eventi di cybersecurity	· COBIT 5 APO07.06 · ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 · NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati.	· NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vengono svolte scansioni per l'identificazione di vulnerabilità	· COBIT 5 BAI03.10 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-5
	Detection Processes (DE.DP): Sono adottati, mantenuti e verificati nel tempo i processi e le procedure di monitoraggio per assicurare una tempestiva e adeguata comprensione degli eventi di sicurezza	**DE.DP-1: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability**	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.4.3.1 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
		DE.DP-2: Le attività di monitoraggio soddisfano tutti i requisiti applicabili	· ISA 62443-2-1:2009 4.4.3.2 · ISO/IEC 27001:2013 A.18.1.4 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4
		DE.DP-3: I processi di monitoraggio vengono testati	· COBIT 5 APO13.02 · ISA 62443-2-1:2009 4.4.3.2 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.14.2.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: L'informazione relativa agli eventi rilevati è comunicata a tutte le parti interessate	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.4.5.9 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4 · **Obbligatoria in caso di trattamento di dati personali (ai sensi degli artt. 19-22, 25-27, 32-bis e 39 del D. Lgs. 196/2003)**
		DE.DP-5: I processi di monitoraggio sono oggetto di periodici miglioramenti e perfezionamenti	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RESPOND (RS)	**Response Planning (RS.RP): Procedure e processi di risposa sono eseguiti e mantenuti per assicurare la tempestiva risposta agli eventi di cybersecurity rilevati.**	**RC.RP-1: Esiste un piano di ripristino (recovery plan) e questo viene eseguito durante o dopo un incidente**	· COBIT 5 BAI01.10 · CCS CSC 18 · ISA 62443-2-1:2009 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Le attività di risposta sono coordinate con le parti interne ed esterne, per includere eventuale supporto da parte degli organi di legge o dalle forze dell'ordine.	**RS.CO-1: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente**	· ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 · NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Sono stabiliti dei criteri per documentare gli incidenti/eventi	· ISA 62443-2-1:2009 4.3.4.5.5 · ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 · **Obbligatoria in caso di trattamento di dati personali (ai sensi degli artt. 19-22, 25-27, 32-bis e 39 del D. Lgs. 196/2003)**
		RS.CO-3: Le informazioni sono condivise in maniera coerente con il piano di risposta	· ISA 62443-2-1:2009 4.3.4.5.2 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 · **Obbligatoria in caso di trattamento di dati personali (ai sensi degli artt. 19-22, 25-27, 32-bis e 39 del D. Lgs. 196/2003)**

Function	Category	Subcategory	Informative References
RESPOND (RS)		**RS.CO-4: Il coordinamento con le parti interessate dell'organizzazione avviene in coerenza con i piani di risposta**	· ISA 62443-2-1:2009 4.3.4.5.5 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 · **Obbligatoria in caso di trattamento di dati personali (ai sensi degli artt. 19-22, 25-27, 32-bis e 39 del D. Lgs. 196/2003)**
		RS.CO-5: E' attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)	· NIST SP 800-53 Rev. 4 PM-15, SI-5 · **Obbligatoria in caso di trattamento di dati personali (ai sensi degli artt. 19-22, 25-27, 32-bis e 39 del D. Lgs. 196/2003)**
	Analysis (RS.AN): Vengono condotte analisi per assicurare un'adeguata riposta e supporto alle attività di ripristino	**RS.AN-1: Le notifiche provenienti dai sistemi di monitoraggio vengono sempre visionate e analizzate**	· COBIT 5 DSS02.07 · ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: Viene compreso l'impatto di ogni incidente	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4
		RS.AN-3: A seguito di un incidente viene svolta un'analisi forense	· ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · ISO/IEC 27001:2013 A.16.1.7 · NIST SP 800-53 Rev. 4 AU-7, IR-4
		RS.AN-4: Gli incidenti sono categorizzate in maniera coerente con i piani di risposta	· ISA 62443-2-1:2009 4.3.4.5.6 · ISO/IEC 27001:2013 A.16.1.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
	Mitigation (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per rimuovere l'incidente.	**RS.MI-1: In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto**	· ISA 62443-2-1:2009 4.3.4.5.6 · ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 · ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4
		RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	· ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
	Improvements (RS.IM): Le attività di risposta sono migliorate incorporando le "lesson learned" da attività precedenti di monitoraggio e risposta.	**RS.IM-1: I piani di risposta agli incidenti tengono in considerazione le esperienze passate (lesson learned)**	· COBIT 5 BAI01.13 · ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.IM-2: Le strategie di risposta agli incidenti sono aggiornate	· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP): I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un tempestivo recupero dei sistemi o asset coinvolti da**	**RC.RP-1: Esiste un piano di risposta (response plan) e viene eseguito durante o dopo un evento**	· CCS CSC 8 · COBIT 5 DSS02.05, DSS03.04 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	Improvements (RC.IM): I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "lesson learned" per le attività future.	**RC.IM-1: I piani di riprisitino tengono in considerazione le esperienze passate (lesson learned)**	· COBIT 5 BAI05.07 · ISA 62443-2-1 4.4.3.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.IM-2: Le strategie di recupero sono aggiornate	· COBIT 5 BAI07.08 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 · **Obbligatorio per le PP.AA. ai sensi dell'art. 50-bis, comma 3, lett. b) del CAD**

Function	Category	Subcategory	Informative References
	Communications (RC.CO): Le attività di ripristino a seguito di un incidente sono coordinate con le parti interne ed esterne, come ad esempio, le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT.	**RC.CO-1: A seguito di un incidente vengono gestite le pubbliche relazioni**	· COBIT 5 EDM03.02 · **Obbligatoria in caso di trattamento di dati personali (ai sensi degli artt. 19-22, 25-27, 32-bis e 39 del D. Lgs. 196/2003)**
		RC.CO-2: A seguito di un incidente viene ripristinata la reputazione	· COBIT 5 MEA03.02
		RC.CO-3: Le attività di recupero condotte a seguito di un incidente vengono comunicate alle parti interessate interne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione	· NIST SP 800-53 Rev. 4 CP-2, IR-4

6. Una contestualizzazione del Framework per PMI

Questo Capitolo riporta una contestualizzazione del Framework per piccole e medie imprese italiane (da qui in avanti chiamata *CONTEXT-PMI*). Tale contestualizzazione è indipendente dal dominio di business e, ad esempio, dalla dimensione delle imprese. Vengono applicati i passi presentati nella Sezione 3.4: selezione delle Subcategory, associazione a queste di valori di priorità, definizione dei livelli di maturità (in questo caso per le sole Subcategory a priorità alta). Infine, questo Capitolo riporta una guida all'implementazione per le Subcategory a priorità alta.

CONTEXT-PMI è una possibile contestualizzazione del Framework. Altre contestualizzazioni potrebbero essere create da operatori diversi (alcuni riportati nella Sezione 3.4.1). A tal proposito, si fa notare che la scelta di 3 livelli di priorità (bassa, media, alta) e 3 livelli di maturità è propria della contestualizzazione e non del Framework: le varie contestualizzazioni possono avere più o meno livelli di priorità e di maturità. Si fa notare inoltre che gli Implementation Tiers per PMI non vengono trattati in questa contestualizzazione.

6.1 Selezione delle Subcategory

La selezione delle Subcategory prevede che vengano identificate le Subcategory che gli estensori della contestualizzazione non ritengono adatte per l'insieme di imprese target a cui si rivolge la contestualizzazione stessa. Ricordiamo che il Framework NIST è stato pensato per il miglioramento delle pratiche di cyber security nelle infrastrutture critiche. Quindi è ragionevole pensare che alcune Subcategory possono non essere rilevanti per l'insieme di aziende per cui viene fatta la contestualizzazione. Tuttavia, il processo di selezione potrebbe portare alla conclusione che tutte le Subcategory siano rilevanti per l'insieme di aziende in considerazione.

Questa fase di selezione deve esser fatta da parte degli estensori della contestualizzazione, tenendo conto che togliere una Subcategory potrebbe significare aumentare il rischio cyber. Quindi si devono eliminare quelle Subcategory che sono non rilevanti per le aziende target della contestualizzazione ad esempio per motivi di business, dimensione, struttura ecc. Si rammenta di valutare attentamente l'esclusione di Subcategory, e di reinserire le categorie escluse laddove, ad esempio, la PMI pur non essendo una Infrastruttura Critica di per sé, svolga però un ruolo determinante nella filiera di erogazione del servizio per una o più Infrastrutture Critiche. Ciononostante, una

PMI potrebbe poi reinseire nella contestualizzazione qualche sottocategoria rimossa in base ai suoi obiettivi di business e di cyber security.

In ultimo, come descritto nella Sezione 3.5, una contestualizzazione potrebbe anche definire Subcategory che non fanno parte del Framework Core, a questo punto gli estensori della contestualizzazione dovrebbero contattare l'organizzazione che gestisce il Framework per un possibile inserimento della Subcategory nella revisione del Framework.

In *CONTEXT-PMI* le seguenti Subcategory sono state contrassegnate come "non selezionate" in quanto ritenute non particolarmente adatte a gran parte delle piccole-medie imprese italiane. Tuttavia, ciascuna PMI dovrà valutare l'eventuale applicabilità nel proprio contesto, anche sulla base delle dimensioni e caratteristiche dell'organizzazione e in generale in relazione al proprio profilo di rischio.

- ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati
- ID.BE-1: Il ruolo dell'organizzazione all'interno della filiera produttiva è identificato e reso noto
- ID.BE-2: Il ruolo dell'organizzazione come infrastruttura critica e nel settore industriale di riferimento è identificato e reso noto
- PR.DS-3: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale
- DE.CM-6: Viene svolto il monitoraggio delle attività dei service provider esterni per rilevare potenziali eventi di cyber security

Nel seguito, riportiamo le motivazioni che hanno guidato tale selezione delle Subcategory. DE.CM-6 richiede uno sforzo non proporzionato all'utilizzo che le PMI fanno dei service provider. Di conseguenza il costo e la gestione di tale pratica potrebbero essere superiori ai benefici ottenuti da una PMI. PR.DS-3 richiede la definizione di un processo formale che, per una PMI, potrebbe rappresentare un overhead eccessivo rispetto alla propria attività di business. ID.BE-1 e ID.BE-2 sono dedicate chiaramente a infrastrutture critiche o a organizzazioni altamente regolate, che devono riportare ai propri regolatori il ruolo o le proprie dipendenze funzionali. ID.AM-4 richiede la creazione di un catalogo di sistemi informativi non di proprietà della PMI. Fatta eccezione per i servizi cloud, è difficile che, nel panorama italiano, PMI abbiano tali sistemi.

6.2 Livelli di priorità

In questa Sezione presentiamo le priorità associate alle Subcategory selezionate in accordo a quanto descritto nel Capitolo 3 per la contestualizzazione *CONTEXT-PMI*. Per completezza si riporta nuovamente la colonna informative references. È importante notare che qualora nella colonna informative references sia specificata un'obbligatorietà della Subcategory, tale Subcategory va considerata come a priorità massima, dai soggetti specificati, indipendentemente da quanto indicato nella colonna Priorità.

Function	Category	Subcategory	Priorità	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi di business e con la strategia di rischio dell'organizzazione	ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	ALTA	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	ALTA	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati.	BASSA	· CCS CSC 1 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati	NON SELEZIONATA	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Le risorse (es: hardware, dispositivi, dati e software) sono prioritizzati in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	MEDIA	· COBIT 5 APO03.03, APO03.04, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 · **Obbligatorio per le PP.AA. ai sensi dell'art. 50-bis, comma 3, lett. a) del CAD**
		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	ALTA	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
	Business Environment (ID.BE): La mission dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono compresi e valutate in termini di priorità. Tali informazioni influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.	ID.BE-1:Il ruolo dell'organizzazione all'interno della filiera produttiva è identificato e reso noto	NON SELEZIONATA	· COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 · NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: Il ruolo dell'organizzazione come infrastruttura critica e nel settore industriale di riferimento è identificato e reso noto	NON SELEZIONATA	· COBIT 5 APO02.06, APO03.01 · NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione.	MEDIA	· COBIT 5 APO02.01, APO02.06, APO03.01 · ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 · NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.BE-4: Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici	MEDIA	· ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 · NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici	MEDIA	· COBIT 5 DSS04.02 · ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

Function	Category	Subcategory	Priorità	Informative References
IDENTIFY (ID)	Governance (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1: E' indetificata e resa nota una policy di sicurezza delle informazioni**	MEDIA	· COBIT 5 APO01.03, EDM01.01, EDM01.02 · ISA 62443-2-1:2009 4.3.2.6 · ISO/IEC 27001:2013 A.5.1.1 · NIST SP 800-53 Rev. 4 -1 controls from all families · **Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 novembre 2015 e dei relativi decreti n. 4/2015 e n.5/2015**
		ID.GV-2: Ruoli e responsabilità inerenti la sicurezza delle informazioni sono coordinati ed allineati con i ruoli interni ed i partner esterni	MEDIA	· COBIT 5 APO13.12 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 · NIST SP 800-53 Rev. 4 PM-1, PS-7
		ID.GV-3: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti	ALTA	· COBIT 5 MEA03.01, MEA03.04 · ISA 62443-2-1:2009 4.4.3.7 · ISO/IEC 27001:2013 A.18.1 · NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1) · **Obbligatoria ai sensi del D.Lgs. 196/2003** · **Obbligatorio ai sensi dei provvedimenti del Garante per la protezione dei dati personali** · **Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 novembre 2015 e dei relativi decreti n. 4/2015 e n.5/2015**
		ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity	BASSA	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · NIST SP 800-53 Rev. 4 PM-9, PM-11
	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente l' operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate**	MEDIA	· CCS CSC 4 · COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: L'organizzazione riceve informazioni su minacce e vulnerabilità da fonti esterne (e.g. CERT, fonti aperte, forum di information sharing)	BASSA	· ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · ISO/IEC 27001:2013 A.6.1.4 · NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5
		ID.RA-3: Le minacce, sia interne che esterne, sono identificate e documentate	BASSA	· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Sono identificati i potenziali impatti sul business e le relative probabilità di accadimento	BASSA	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	BASSA	· COBIT 5 APO12.02 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
		ID.RA-6: Sono identificate e prioritizzate le risposte al rischio	BASSA	· COBIT 5 APO12.05, APO13.02 · NIST SP 800-53 Rev. 4 PM-4, PM-9
	Risk Management Strategy (ID.RM): Le priorità e i requisiti dell'organizzazione e la tolleranza al rischio sono definiti e utilizzati per supportare le decisioni sul rischio operazionale.	**ID.RM-1: I processi di risk management sono stabiliti, gestiti e concordati tra i responsabili dell'organizzazione (c.d. stakeholder)**	BASSA	· COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · ISA 62443-2-1:2009 4.3.4.2 · NIST SP 800-53 Rev. 4 PM-9
		ID.RM-2: Il rischio tollerato dall'organizzazione è identificato ed espresso chiaramente	BASSA	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.2.6.5 · NIST SP 800-53 Rev. 4 PM-9
		ID.RM-3: Il rischio tollerato è determinato tenendo conto del ruolo dell'organizzazione come infrastruttura critica e dei rischi specifici presenti nel settore industriale di appartenenza	BASSA	· NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14

Function	Category	Subcategory	Priorità	Informative References
PROTECT (PR)	Access Control (PR.AC): L'accesso agli asset ed alle relative risorse è limitato al personale, ai processi, ai dispositivi, alle attività ed alle transazioni effettivamente autorizzate	**PR.AC-1:Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate**	ALTA	· CCS CSC 16 · COBIT 5 DSS05.04, DSS06.03 · ISA 62443-2-1:2009 4.3.3.5.1 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · NIST SP 800-53 Rev. 4 AC-2, IA Family · **Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 novembre 2015 e dei relativi decreti n. 4/2015 e n.5/2015** · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regole 1-10)**
		PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato	MEDIA	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 · ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003)**
		PR.AC-3: L'accesso remoto alle risorse è amministrato	ALTA	· COBIT 5 APO13.01, DSS01.04, DSS05.03 · ISA 62443-2-1:2009 4.3.3.6.6 · ISA 62443-3-3:2013 SR 1.13, SR 2.6 · ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regole 1-10)** · **Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 novembre 2015 e dei relativi decreti n. 4/2015 e n.5/2015**
		PR.AC-4: Gli accessi alle risorse sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	ALTA	· CCS CSC 12, 15 · ISA 62443-2-1:2009 4.3.3.7.3 · ISA 62443-3-3:2013 SR 2.1 · ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 · NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regole 12,13,14)**
		PR.AC-5:L'integrità di rete è protetta, anche applicando la segregazione di rete dove appropriata	MEDIA	· ISA 62443-2-1:2009 4.3.3.4 · ISA 62443-3-3:2013 SR 3.1, SR 3.8 · ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, SC-7
	Awareness and Training (PR.AT): Il personale e le terze sono sensibilizzate e formate in materia di cybersecurity e ricevono adeguata preparazione, coerente con le politiche, le procedure e gli accordi esistenti, per svolgere correttamente i compiti e le responsabilità legate alla sicurezza delle informazioni	**PR.AT-1: Tutti gli utenti sono informati e addestrati**	ALTA	· CCS CSC 9 · COBIT 5 APO07.03, BAI05.07 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.7.2.2 · NIST SP 800-53 Rev. 4 AT-2, PM-13 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regole 4, 9, 18, 21, 27, 28)**
		PR.AT-2: Gli utenti privilegiati (e.g. Amministratori di Sistema) comprendono ruoli e responsabilità	ALTA	· CCS CSC 9 · COBIT 5 APO07.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 AT-2, PM-13 · **Provvedimento Garante Privacy del 27 novembre 2008** · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003)**
		PR.AT-3: Tutte le terze parti (es. fornitori, clienti, partner) comprendono ruoli e responsabilità	MEDIA	· CCS CSC 9 · COBIT 5 APO07.03, APO10.04, APO10.05 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 PS-7, SA-9

Function	Category	Subcategory	Priorità	Informative References
PROTECT (PR)		**PR.AT-4: I dirigenti ed i vertici aziendali comprendono ruoli e responsabilità**	**ALTA**	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.AT-5: Il personale addetto alla sicurezza fisica e delle informazioni comprende i ruoli e le responsabilità	**MEDIA**	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13
	Data Security (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1: I dati e le informazioni memorizzate sono protette**	**MEDIA**	· CCS CSC 17 · COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 · ISA 62443-3-3:2013 SR 3.4, SR 4.1 · ISO/IEC 27001:2013 A.8.2.3 · NIST SP 800-53 Rev. 4 SC-28 · **Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 novembre 2015 e dei relativi decreti n. 4/2015 e n.5/2015** · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regole 16,17, 20)**
		PR.DS-2: I dati sono protetti durante la trasmissione	**BASSA**	· CCS CSC 17 · COBIT 5 APO01.06, DSS06.06 · ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SC-8 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003)**
		PR.DS-3:Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	**NON SELEZIONATA**	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 · NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.DS-4: I sistemi hanno adeguate risorse a disposione per poter garantire la disponibilità	**MEDIA**	· COBIT 5 APO13.01 · ISA 62443-3-3:2013 SR 7.1, SR 7.2 · ISO/IEC 27001:2013 A.12.3.1 · NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
		PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	**BASSA**	· CCS CSC 17 · COBIT 5 APO01.06 · ISA 62443-3-3:2013 SR 5.2 · ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003)**
		PR.DS-6: Vengono implementate tecniche di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle	**BASSA**	· ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 · ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SI-7
		PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	**MEDIA**	· COBIT 5 BAI07.04 · ISO/IEC 27001:2013 A.12.1.4 · NIST SP 800-53 Rev. 4 CM-2

Function	Category	Subcategory	Priorità	Informative References
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli assets.	**PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale**	ALTA	· CCS CSC 3, 10 · COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).	MEDIA	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.3 · ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni	MEDIA	· COBIT 5 BAI06.01, BAI01.06 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
		PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati periodicamente	ALTA	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.9 · ISA 62443-3-3:2013 SR 7.3, SR 7.4 · ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 · NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regola 18)**
		PR.IP-5: Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione	MEDIA	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: I dati sono distrutti in conformità con le policy	MEDIA	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.4.4.4 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · NIST SP 800-53 Rev. 4 MP-6
		PR.IP-7: I processi di protezione sono migliorati in maniera continuativa	BASSA	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: L'efficacia delle tecnologie di protezione è condivisa con i referenti appropriati	BASSA	· ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
		PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	MEDIA	· COBIT 5 DSS04.03 · ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 · NIST SP 800-53 Rev. 4 CP-2, IR-8 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003)**
		PR.IP-10: I piani di risposta e recupero a seguito di incidenti/disastri sono verificati nel tempo	BASSA	· ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.17.1.3 · NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14 · **Obbligatorio per le PP.AA. ai sensi dell'art. 50-bis, comma 3, lett. b) del CAD**
		PR.IP-11: Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, licenziamenti)	BASSA	· COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 · NIST SP 800-53 Rev. 4 PS Family
		PR.IP-12:Viene sviluppato e implementato un piano di gestione delle vulnerabilità	MEDIA	· ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 · NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2

Function	Category	Subcategory	Priorità	Informative References
PROTECT (PR)	Maintenance (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti	PR.MA-1:La manutenzione e la riparazione delle risorse e dei sistemi è svolta e registrata in modo tempestivo e portata a termine attraverso l'utilizzo di strumenti controllati ed autorizzati	BASSA	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.3.3.7 · ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 · NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5
		PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	ALTA	· COBIT 5 DSS05.04 · ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 · ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 · NIST SP 800-53 Rev. 4 MA-4
	Protective Technology (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	PR.PT-1: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi	MEDIA	· CCS CSC 14 · COBIT 5 APO11.04 · ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · NIST SP 800-53 Rev. 4 AU Family
		PR.PT-2: I supporti di memorizzazione removibili sono protetti ed il loro uso è ristretto in accordo alle policy	MEDIA	· COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 2.3 · ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003)**
		PR.PT-3: L'accesso alle risorse e ai sistemi è limitato secondo il principio di minima funzionalità	MEDIA	· COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · ISO/IEC 27001:2013 A.9.1.2 · NIST SP 800-53 Rev. 4 AC-3, CM-7 · **Obbligatoria in caso di trattamento di dati personali mediante strumenti elettronici (ai sensi dell'All. B) D. Lgs. 196/2003 Regola 13)**
		PR.PT-4: Le reti di comunicazione e controllo sono protette	ALTA	· CCS CSC 7 · COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7
DETECT (DE)	Anomalies and Events (DE.AE): Le attività anomale sono rilevate tempestivamente e il loro impatto potenziale viene analizzato.	DE.AE-1: sono definite, rese note e gestite delle pratiche di riferimento (c.d. baseline) inerenti l'utilizzo della rete ed i flussi informativi attesi per	BASSA	· COBIT 5 DSS03.01 · ISA 62443-2-1:2009 4.4.3.3 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Gli eventi rilevati vengono analizzati per comprendere gli obiettivi e le metodologie dell'attacco	BASSA	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Le informazioni relative agli eventi sono aggregate e correlate da sensori e sorgenti multiple	MEDIA	· ISA 62443-3-3:2013 SR 6.1 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Viene determinato l'impatto di un evento	MEDIA	· COBIT 5 APO12.06 · NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4
		DE.AE-5: Vengono definite delle soglie di allerta per gli incidenti	MEDIA	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.2.3.10 · NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
		DE.CM-1: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	MEDIA	· CCS CSC 14, 16 · COBIT 5 DSS05.07 · ISA 62443-3-3:2013 SR 6.2 · NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: Viene svolto il monitoraggio degli spazi fisici per rilevare potenziali eventi di cybersecurity	BASSA	· ISA 62443-2-1:2009 4.3.3.3.8 · NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20

Function	Category	Subcategory	Priorità	Informative References
DETECT (DE)	Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati periodicamente per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-3: Viene svolto il monitoraggio del personale per rilevare potenziali eventi di cybersecurity**	BASSA	· ISA 62443-3-3:2013 SR 6.2 · ISO/IEC 27001:2013 A.12.4.1 · NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 · **Da eseguirsi ai sensi dell'art. 23 del D. Lgs. n. 151/2015**
		DE.CM-4: Il codice malevolo viene rilevato	ALTA	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.3.4.3.8 · ISA 62443-3-3:2013 SR 3.2 · ISO/IEC 27001:2013 A.12.2.1 · NIST SP 800-53 Rev. 4 SI-3
		DE.CM-5: Il codice non autorizzato su dispositivi mobili viene rilevato	BASSA	· ISA 62443-3-3:2013 SR 2.4 · ISO/IEC 27001:2013 A.12.5.1 · NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44
		DE.CM-6: Viene svolto il monitoraggio delle attività dei service provider esterni per rilevare potenziali eventi di cybersecurity	NON SELEZIONATA	· COBIT 5 APO07.06 · ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 · NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati.	MEDIA	· NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vengono svolte scansioni per l'identificazione di vulnerabilità	MEDIA	· COBIT 5 BAI03.10 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-5
	Detection Processes (DE.DP): Sono adottati, mantenuti e verificati nel tempo i processi e le procedure di monitoraggio per assicurare una tempestiva e adeguata comprensione degli eventi di sicurezza.	**DE.DP-1: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability**	BASSA	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.4.3.1 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
		DE.DP-2: Le attività di monitoraggio soddisfano tutti i requisiti applicabili	MEDIA	· ISA 62443-2-1:2009 4.4.3.2 · ISO/IEC 27001:2013 A.18.1.4 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4
		DE.DP-3: I processi di monitoraggio vengono testati	BASSA	· COBIT 5 APO13.02 · ISA 62443-2-1:2009 4.4.3.2 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.14.2.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: L'informazione relativa agli eventi rilevati è comunicata a tutte le parti interessate	MEDIA	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.4.5.9 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4 · **Obbligatoria in caso di trattamento di dati personali (ai sensi degli artt. 19-22, 25-27, 32-bis e 39 del D. Lgs. 196/2003)**
		DE.DP-5: I processi di monitoraggio sono oggetto di periodici miglioramenti e perfezionamenti	BASSA	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Function	Category	Subcategory	Priorità	Informative References
RESPOND (RS)	Response Planning (RS.RP): Procedure e processi di risposa sono eseguiti e mantenuti per assicurare la tempestiva risposta agli eventi di cybersecurity rilevati.	RS.RP-1: Esiste un piano di ripristino (recovery plan) e questo viene eseguito durante o dopo un incidente	BASSA	· COBIT 5 BAI01.10 · CCS CSC 18 · ISA 62443-2-1:2009 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Le attività di risposta sono coordinate con le parti interne ed esterne, per includere eventuale supporto da parte degli organi di legge o dalle forze dell'ordine.	RS.CO-1: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	BASSA	· ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 · NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Sono stabiliti dei criteri per documentare gli incidenti/eventi	BASSA	· ISA 62443-2-1:2009 4.3.4.5.5 · ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 · **Obbligatoria in caso di trattamento di dati personali (ai sensi degli artt. 19-22, 25-27, 32-bis e 39 del D. Lgs. 196/2003)**
		RS.CO-3: Le informazioni sono condivise in maniera coerente con il piano di risposta	BASSA	· ISA 62443-2-1:2009 4.3.4.5.2 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 · **Obbligatoria in caso di trattamento di dati personali (ai sensi degli artt. 19-22, 25-27, 32-bis e 39 del D. Lgs. 196/2003)**
		RS.CO-4: Il coordinamento con le parti interessate dell'organizzazione avviene in coerenza con i piani di risposta	BASSA	· ISA 62443-2-1:2009 4.3.4.5.5 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 · **Obbligatoria in caso di trattamento di dati personali (ai sensi degli artt. 19-22, 25-27, 32-bis e 39 del D. Lgs. 196/2003)**
		RS.CO-5: E' attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)	BASSA	· NIST SP 800-53 Rev. 4 PM-15, SI-5 · **Obbligatoria in caso di trattamento di dati personali (ai sensi degli artt. 19-22, 25-27, 32-bis e 39 del D. Lgs. 196/2003)**
	Analysis (RS.AN): Vengono condotte analisi per assicurare un'adeguata riposta e supporto alle attività di ripristino	RS.AN-1: Le notifiche provenienti dai sistemi di monitoraggio vengono sempre visionate e analizzate	BASSA	· COBIT 5 DSS02.07 · ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: Viene compreso l'impatto di ogni incidente	MEDIA	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4
		RS.AN-3: A seguito di un incidente viene svolta un'analisi forense	BASSA	· ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · ISO/IEC 27001:2013 A.16.1.7 · NIST SP 800-53 Rev. 4 AU-7, IR-4
		RS.AN-4: Gli incidenti sono categorizzate in maniera coerente con i piani di risposta	BASSA	· ISA 62443-2-1:2009 4.3.4.5.6 · ISO/IEC 27001:2013 A.16.1.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
	Mitigation (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per rimuovere l'incidente.	RS.MI-1: In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto	ALTA	· ISA 62443-2-1:2009 4.3.4.5.6 · ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti	ALTA	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 · ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4
		RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	ALTA	· ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
	Improvements (RS.IM): Le attività di risposta sono migliorate incorporando le "lesson learned" da attività precedenti di monitoraggio e risposta.	RS.IM-1: I piani di risposta agli incidenti tengono in considerazione le esperienze passate (lesson learned)	BASSA	· COBIT 5 BAI01.13 · ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

Function	Category	Subcategory	Priorità	Informative References
		RS.IM-2: Le strategie di risposta agli incidenti sono aggiornate	**BASSA**	· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP): I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un tempestivo recupero dei sistemi o asset coinvolti da**	**RC.RP-1: Esiste un piano di risposta (response plan) e viene eseguito durante o dopo un evento**	**MEDIA**	· CCS CSC 8 · COBIT 5 DSS02.05, DSS03.04 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	Improvements (RC.IM): I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "lesson learned" per le attività future.	**RC.IM-1: I piani di riprisitino tengono in considerazione le esperienze passate (lesson learned)**	**BASSA**	· COBIT 5 BAI05.07 · ISA 62443-2-1 4.4.3.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.IM-2: Le strategie di recupero sono aggiornate	**BASSA**	· COBIT 5 BAI07.08 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 · **Obbligatorio per le PP.AA. ai sensi dell'art. 50-bis, comma 3, lett. b) del CAD**
	Communications (RC.CO): Le attività di ripristino a seguito di un incidente sono coordinate con le parti interne ed esterne, come ad esempio, le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT.	**RC.CO-1: A seguito di un incidente vengono gestite le pubbliche relazioni**	**BASSA**	· COBIT 5 EDM03.02 · **Obbligatoria in caso di trattamento di dati personali (ai sensi degli artt. 19-22, 25-27, 32-bis e 39 del D. Lgs. 196/2003)**
		RC.CO-2: A seguito di un incidente viene ripristinata la reputazione	**BASSA**	· COBIT 5 MEA03.02
		RC.CO-3: Le attività di recupero condotte a seguito di un incidente vengono comunicate alle parti interessate interne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione	**MEDIA**	· NIST SP 800-53 Rev. 4 CP-2, IR-4

6.3 Livelli di maturità

Questa Sezione riporta i livelli di maturità per le Subcategory contrassegnate come a "priorità alta" nella contestualizzazione *CONTEXT-PMI*. Per ognuna di queste Subcategory viene anche fornito un riferimento alla guida all'implementazione delle Subcategory a priorità alta, riportata in Sezione 6.4. Si noti che non sempre ha senso definire tre livelli di maturità crescenti, pertanto, alcune Subcategory riportano solo uno o due livelli di maturità. Si ricorda, inoltre, che le Subcategory a priorità alta sono quelle che dovrebbero essere implementate per prime e almeno al livello di maturità minimo. In base al proprio contesto di business, risk assessment e altri fattori, si devono implementare poi le Subcategory a priorità minore nella contestualizzazione e i livelli di maturità desiderati.

Function	Subcategory	Rif.Guida	Livello 1	Livello 2	Livello 3
IDENTIFY (ID)	ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	Tabella 6.1: Identificazione degli Asset (IA)	Il censimento, la classificazione e l'aggiornamento degli asset (intesi come informazioni, applicazioni, sistemi ed apparati presenti) avviene in modalità per lo più manuale secondo un processo definito e controllato	Il censimento, la classificazione e l'aggiornamento degli asset avviene attraverso un sistema parzialmente automatico, che consenta di automatizzare almeno la fase di "discovery" dei sistemi connessi in rete, rilevando le principali caratteristiche degli stessi (caratteristiche hardware, software installati, configurazioni adottate, ecc.) e registrando l'inventario ottenuto in un repository centralizzato	Il censimento, la classificazione e l'aggiornamento degli asset avviene attraverso un sistema completamente automatico, che consenta di gestire l'intero ciclo di vita di un asset (identificazione, assegnazione, cambiamenti di stato, dismissioni)
	ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	Tabella 6.1: Identificazione degli Asset (IA)	Vedi ID.AM-1	Vedi ID.AM-1	Vedi ID.AM-1
	ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	Tabella 6.2: Assegnazione Responsabilità (AR)	La Proprietà e/o il Vertice Aziendale nomina il referente per la Cyber Security, definendo formalmente le attività in carico. Formalizza inoltre il disciplinare tecnico per l'utilizzo consono delle informazioni e degli strumenti informatici da parte di tutte le parti interessate (e.g. dipendenti, consulenti, terze parti)	Deve essere predisposto un documento di Politica Aziendale per la Cyber Security che definisca e formalizzi chiaramente i ruoli, le responsabilità e le attività richieste a ciascuna parte coinvolta a vario titolo nella gestione della Cyber Security (dipendenti, consulenti, terze parti), comunicando chiaramente l'impegno della Proprietà o dei Vertici Aziendali rispetto a tali necessità	N/A
	ID.GV-3: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti	Tabella 6.3: Conformità a leggi e regolamenti (CLR)	La conformità a leggi e regolamenti è raggiunta e verificata, anche ricorrendo a specialisti e fornitori esterni, ove ritenuto necessario, in grado di agevolare l'individuazione e la gestione degli aspetti normativi e di conformità, soprattutto quando direttamente o indirettamente connessi con gli aspetti di Cyber Security	N/A	N/A

Function	Subcategory	Rif.Guida	Livello 1	Livello 2	Livello 3
PROTECT (PR)	PR.AC-1:Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate	Tabella 6.6: Controllo Accessi (CA)	Il ciclo di vita delle identità e delle credenziali di autenticazione è gestito ed amministrato localmente su ciascun dispositivo o sistema IT secondo un processo definito e controllato	Le identità e le credenziali sono amministrate attraverso una directory aziendale che consente l'applicazione omogenea di regole e livelli minimi di sicurezza	Specifiche soluzioni tecnologiche sono adottate per gestire in maniera specifica ed appropriata anche le utenze privilegiate (e.g. Amministratori di Sistema).
	PR.AC-3: L'accesso remoto alle risorse è amministrato	Tabella 6.6: Controllo Accessi (CA)	L'accesso remoto alle risorse avviene attraverso l'uso di canali di comunicazioni sicuri (e.g. VPN con crittografia delle comunicazioni) e in linea con i criteri specificati nella guida all'implementazione dei controlli	L'accesso remoto alle risorse avviene attraverso l'uso di canali di comunicazioni sicuri e sistemi di autenticazione a due fattori	L'accesso remoto alle risorse avviene solo se vengono rispettati specifici criteri di configurazione dei sistemi (i.e. presenza antivirus, aggiornamento stato patch,…)
	PR.AC-4: Gli accessi alle risorse sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	Tabella 6.6: Controllo Accessi (CA)	Gli accessi ai sistemi informatici vengono concessi previo censimento dei principali ruoli esistenti, finalizzato ad individuare il perimentro di intervento di ciascun ruolo ed evidenziando eventuali incompatibilità esistenti tra gli stessi. Successivamente i profili di abilitazione e le credenziali di accesso devono essere assegnate in coerenza con un iter autorizzativi definito, nel rispetto dei criteri di separazione dei ruoli stabiliti e dell'attribuzione del privilegio minimo necessario all'espletamento delle sole funzioni previste da ciascun ruolo	Devono essere definite regole di segregazione dei ruoli atte a prevenire l'assegnazione di ruoli incompatibili tra di loro ed implementati strumenti automatici di controllo delle stesse e del rispetto dell'iter autorizzativo definito al fine di prevenire o identificare la possibilità di compimento di frodi, abusi, errori da parte degli utenti	Deve essere definito ed attuato un processo di certificazione periodica dei privilegi assegnati ed effettuate attività di verifica degli stessi al fine di accertarsi che i privilegi assegnati siano validi (i.e. persistenza delle condizioni che ne hanno determinato la loro assegnazione)

Function	Subcategory	Rif.Guida	Livello 1	Livello 2	Livello 3
PROTECT (PR)	PR.AT-1: Tutti gli utenti sono informati e addestrati	Tabella 6.9: Formazione di base del personale (FBP)	La formazione di base del personale sui rischi di cybersecurity avviene secondo una pianificazione ed una periodicità definite ed attraverso l'ausilio di tecniche e strumenti di formazione appropriati (e.g. e- learning, formazione in aula, materiale didattico) in linea con le caratteristiche specifiche di ciascuna organizzazione (e.g. distribuzione territoriale del personale, utilizzo prevalente di fornitori esterni).	Le iniziative di formazione sulla cybersecurity vengono differenziate nei loro obiettivi e nei contenuti in base allo specifico ruolo svolto dalle risorse coinvolte	Le iniziative di formazione sulla cybersecurity vengono svolte, per particolari categorie di utenti, prevedendo un addestramento sulla identificazione e risposta ai rischi di cybersecurity
	PR.AT-2: Gli utenti privilegiati (e.g. Amministratori di Sistema) comprendono ruoli e responsabilità	Tabella 6.9: Formazione di base del personale (FBP)	La formazione del personale specialistico sulla cybersecurity avviene anche ricorrendo a percorsi formativi esterni, tali da garantire un'adeguata preparazione tecnico-professionale in linea con la criticità dei ruoli svolti (e.g. amministratori di sistema)	La formazione del personale specialistico sulla cybersecurity, viene svolta, per particolari categorie di utenti, mediante il supporto di organizzazioni esterne specializzate prevedendo eventuali percorsi di Certificazione Professionale	N/A
	PR.AT-4: I dirigenti ed i vertici aziendali comprendono ruoli e responsabilità	Tabella 6.9: Formazione di base del personale (FBP)	La Proprietà ed i vertici aziendali sostengono la sensibilizzazione del personale sulla cybersecurity mediante l'allocazione di risorse specifiche e provvedono a comunicare l'importanza della stessa mediante richiami formali (e.g. Politica di sicurezza generale, comunicati interni, bacheca aziendale)	La Proprietà e i Vertici Aziendali partecipano attivamente ai programmi di sensibilizzazione, mediante la partecipazione diretta a workshop ed interventi formativi mirati volti ad accrescere la percezione dei rischi Cyber e delle pratiche da attuare per indirizzare al meglio gli stessi	N/A

Function	Subcategory	Rif.Guida	Livello 1	Livello 2	Livello 3
PROTECT (PR)	PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale	Tabella 6.7: Configurazione sicura sistemi (CSS)	La configurazione sicura dei sistemi viene attuata dai referenti IT (ove presenti) e/o da ditte esterne incaricate (ove presenti) nel rispetto dei criteri specificati nella guida all'implementazione dei controlli	La configurazione sicura dei sistemi avviene attraverso il ricorso a linee guida e procedure operative che ne formalizzano i criteri e le modalità secondo gli standard di mercato	La configurazione sicura dei sistemi avviene anche attraverso l'utilizzo di strumenti e soluzioni automatiche finalizzate ad agevolare la configurazione ed il controllo delle configurazioni dei sistemi IT connessi alla rete aziendale. Gli standard di sicurezza deveno essere aggiornati in maniera periodica
	PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati periodicamente	Tabella 6.10: Backup & Restore (BR)	Il Backup ed il Restore dei dati avviene mediante il ricorso a soluzioni tecnologiche specifiche in grado di automatizzare le principali attività richieste (pianificazione dei salvataggi, monitoraggio degli esiti, ecc.) ed in linea con gli altri criteri specificati nella guida all'implementazione dei controlli. I backup vengono testati regolarmente secondo un processo definito.	Soluzioni finalizzate al mantenimento della continuità operativa devono essere valutate in base agli obiettivi di ripristino e salvaguardia delle informazioni indetificati. Piani di continuità devono essere definiti per il ripristino della continuità operativa	Gli obiettivi di ripristino e salvaguardia devono essere rivisti con periodicità. Piani di continuità devono essere testati e aggiornati periodicamente
	PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	Tabella 6.6: Controllo Accessi (CA)	Inserire un processo di autorizzazione preventiva e di documentazione dell'intervento effettuato	Vedi PR.AC-3	Vedi PR.AC-3
	PR.PT-4: Le reti di comunicazione e controllo sono protette	Tabella 6.5: Protezione perimetrale (PP)	La protezione perimetrale delle reti è ottenuta mediante soluzioni hardware e software appropriate, in linea con i criteri specificati nella guida all'implementazione dei controlli	Le reti di comunicazione interne all'azienda (comprese quelle ove sono attestati sistemi virtuali) che rivestono particolare rilevanza per le business operations devono essere opportunamente protette attraverso impiego di dispositivi firewall che segreghino le reti e limitino il traffico a solo quello autorizzato. Le reti wireless aziendali devono essere configurate in modo da prevenire accessi non autorizzati	Le reti di comunicazione perimetrali ed interne all'azienda devono essere protetti con soluzioni avanzate di protezione del traffico di rete che estendano le funzionalità di base delle soluzioni Firewall. L'accesso alle reti aziendali deve essere concesso solo dopo verifica del rispetto di standard aziendali

Function	Subcategory	Rif.Guida	Livello 1	Livello 2	Livello 3
DETECT (DE)	DE.CM-4: Il codice malevolo viene rilevato	Tabella 6.4: Protezione da Virus (PV)	La protezione da Malware avviene mediante l'adozione di soluzioni tecnologiche dedicate	Le soluzioni di protezione da malware (e.g. software antivirus e/o soluzioni per protezione endpoint) sono gestiste e monitorare a livello centrale	La protezione da malware è ottenuta combinando più soluzioni tecnologiche a copertura dei sistemi e delle reti (host based e network based)
RESPOND (RS)	RS.MI-1: In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto	Tabella 6.11: Risposta agli incidenti di sicurezza (RI)	La risposta agli incidenti di Cyber Security avviene almeno attraverso la formalizzazione di una procedura aziendale, redatta in coerenza con i criteri definiti nella guida all'implementazione dei controlli e comunicata a tutte le parti interessate (e.g. dipendenti, consulenti, terze parti)	Il processo di gestione degli incidenti deve prevedere criteri per la definizione delle priorità degli incidenti, modalità di contenimento degli incidenti e ripristino dell'operatività. Deve essere possibile identificare incidenti attraverso analisi degli eventi generati da soluzioni di sicurezza o registrati dai sistemi	Il processo di gestione degli incidenti deve prevedere la registrazione degli incidenti e la registrazione delle attività completate per la loro gestione. Deve essere completata l'analisi sugli incidenti occorsi per determinare cause e ridurre la probabilità di accadimento. Deve essere previsto un piano per la comunicazione esterna degli incidenti
	RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti	Tabella 6.11: Risposta agli incidenti di sicurezza (RI)	Vedi RS.MI-1	Vedi RS.MI-1	Vedi RS.MI-1
	RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	Tabella 6.8: Aggiornamento sistemi (AS)	L'aggiornamento dei sistemi avviene automaticamente per le postazioni ed i dispositivi degli utenti finali, attraverso l'utilizzo di soluzioni tecnologiche specifiche ed in linea con i criteri definiti nella guida all'implementazione dei controlli. I server vengono aggiornati periodicamente	Attività di Vulnerability Assessment devono essere effettuate sui sistemi e le reti più rilevanti in termini di operatività aziendale. Le Vulnerabilità identificate devono essere risolte	Attività di Vulnerability Assessment devono essere effettuate su tutti i sistemi e le reti aziendali, in maniera periodica. Le Vulnerabilità identificate devono essere risolte secondo priorità basate sulla rilevanza degli Asset interessati. Attività di Penetration Test devono essere effettuate

6.4 Guida all'implementazione delle Subcategory a priorità alta

L'adozione del Framework da parte delle PMI è stata semplificata – come anticipato nel Capitolo 4 – rispetto all'approccio proposto per grandi aziende e organizzazioni. Questa prevede, in prima istanza, che siano verificate e attuate tutte quelle Subcategory del Framework classificate come a priorità alta. Queste rappresentano, difatti, le azioni essenziali da completare per contrastare le principali e più comuni minacce cyber e proteggere i sistemi delle PMI comunemente esposti. Questo Capitolo nasce nell'ottica di supportare le PMI nel completamento di questo primo fondamentale passo.

La presente guida è strutturata in 4 aree di indirizzo, a loro volta organizzate in undici sotto aree, come di seguito riportato:

1. Identificazione degli asset e governo della sicurezza

   1.1 Identificazione degli asset (IA)

   2.2 Assegnazione Responsabilità (AR)

   3.3 Conformità a Leggi e Regolamenti (CLR)

2. Identificazione delle minacce

   2.1 Protezione da Malware (PM)

3. Protezione dei sistemi e delle infrastrutture

   3.1 Protezione perimetrale (PP)

   3.2 Controllo Accessi (CA)

   3.3 Configurazione Sicura Sistemi (CCS)

   3.4 Aggiornamento Sistemi (AS)

   3.5 Formazione di Base del Personale (FBP)

   3.6 Backup e Restore (BR)

4. Gestione degli incidenti di sicurezza

   4.1 Risposta agli Incidenti di Sicurezza (RI)

Per ciascuna sotto area sono indicati i controlli di carattere procedurale, organizzativo e tecnico da attuare e i riferimenti alle Subcategory a priorità alta del Framework che risultano soddisfatte. Tutte le Subcategory a priorità alta sono indirizzate dalla guida.

Identificazione degli asset e governo della sicurezza

Tabella 6.1: **Identificazione degli asset (IA)**

Descrizione:	L'applicazione di contromisure di sicurezza finalizzate a ridurre il rischio cyber deve avvenire su tutti sistemi e i computer aziendali e in particolare su quelli valutati come critici per il business stesso. È indispensabile pertanto disporre di un inventario di tutti gli asset rappresentati dalle informazioni, applicazioni, sistemi e apparati informatici presenti all'interno dell'azienda. Registrare attributi importanti, come ad esempio la posizione fisica, il proprietario, la funzione di riferimento, le dipendenze, ecc. risulta funzionale alle attività di governo e gestione della cyber security. Ad esempio, un inventario delle risorse è in grado di abilitare l'identificazione dei sistemi che necessitano dell'applicazione di uno specifico aggiornamento software.
Subcategory:	▪ ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione ▪ ID.AM-2: Sono censiti le piattaforme e le applicazioni software in uso nell'organizzazione
Controlli applicabili:	IA.1 Deve essere predisposto un inventario delle informazioni, applicazioni, sistemi e apparati presenti in azienda, sia a livello IT, sia riferito ai sistemi di controllo industriale (Industrial Control Systems), qualora presenti IA.2 L'inventario deve rispondere ai seguenti criteri: (a) Sono riportate per gli asset censiti come minimo le tipologie di informazioni trattate, la posizione, la direzione/funzione di riferimento, il responsabile, i referenti coinvolti a diverso titolo nelle attività di gestione e manutenzione, dipendenze e ulteriori dettagli utili per l'attuazione dei controlli menzionati nelle successive sotto aree (e.g. tipologia hardware, versioni software, informazioni trattate, contratti di servizio ecc.) (b) Sono identificati i sistemi con maggiore rilevanza in termini di conseguimento degli obiettivi di business aziendale e quelli coinvolti a diverso titolo nel rispetto di vincoli normativi cogenti (c) Sono registrati tutti i cambiamenti di stato legati agli asset, come acquisizione, installazione, operatività e ritiro. IA.3 L'inventario deve essere costantemente aggiornato, in particolare ogni qualvolta si dovesse verificare un cambiamento e deve essere mantenuto uno storico dei cambiamenti avvenuti

Tabella 6.2: **Assegnazione Responsabilità (AR)**

Descrizione:	L'assegnazione dei ruoli e delle responsabilità è un elemento indispensabile per assicurare un corretto governo dei rischi e permettere un'efficace operatività, intesa come attuazione dei controlli di prevenzione e/o contrasto delle minacce di cyber security a cui le aziende sono esposte. E' fondamentale che tutto il personale sia consapevole dei ruoli e delle responsabilità di sicurezza, correlate allo svolgimento della attività lavorative. Ai vertici aziendali, nelle figure dell'amministratore delegato, del consiglio di amministrazione, della dirigenza e più in generale alla "proprietà", è assegnato il ruolo chiave di definizione delle priorità e di assegnazione delle risorse associate alle iniziative di cyber security. Questi difatti sono i responsabili ultimi per i rischi cyber all'interno dell'azienda.
Subcategory:	▪ ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cyber security per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner) ▪ PR.AT-4: I dirigenti e i vertici aziendali comprendono ruoli e responsabilità
Controlli applicabili:	AR.1 I vertici aziendali (i.e., amministratore delegato, consiglio di amministrazione e dirigenti) devono essere consapevoli e comprendere le responsabilità associate a rischi di cyber security. Questo deve essere evidente almeno in sede di consiglio di amministrazione (ove presente/applicabile) AR.2 Devono essere stabiliti e formalizzati i ruoli e le responsabilità legati alla cyber security, come ad esempio quelli previsti per la protezione dei sistemi e delle infrastrutture o quelli legati all'uso corretto degli strumenti informatici, per tutto il personale e le terzi parti interessate (es. i fornitori, i clienti, i partner) AR.3 All'interno dell'organizzazione deve essere identificata una figura che rappresenti il punto di riferimento per la cyber security (i.e. responsabile per la cyber security), con il compito di coordinare le diverse iniziative di cyber security e contattare le autorità e il CERT Nazionale in caso di eventi di ampia portata AR.4 Tutte le assegnazioni di responsabilità devono essere opportunamente formalizzate

Tabella 6.3: **Conformità a leggi e regolamenti (CLR)**

Descrizione:	La crescita esponenziale delle tecnologie dell'informazione e del processo di digitalizzazione in atto ha comportato e comporterà anche in futuro, la necessità per le aziende di adeguarsi costantemente a leggi e regolamenti specifici, volti a tutelare utenti e organizzazioni nello spazio cyber. L'organizzazione ha l'obbligo di conoscere e ottemperare alle leggi e ai regolamenti applicabili al proprio contesto, soprattutto in relazione ai mercati in cui essa opera e alla tipologia di servizi informatici fruiti e/o erogati.
Subcategory:	▪ ID.GV-3: I requisiti legali in materia di cyber security, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti
Controlli applicabili:	CLR.1 Individuare le leggi e i regolamenti che hanno un impatto diretto o indiretto sulla cyber security (es. Computer Crime, Data Breach Notification, proprietà intellettuale), aggiornando periodicamente il censimento CLR.2 Identificare, attraverso un'attività di monitoraggio periodico, ogni potenziale non conformità rispetto a quanto richiesto da leggi e regolamenti e preparare un piano specifico di adeguamento in cui indirizzare tali non conformità, condividendo gli impatti e le implicazioni specifiche con i vertici aziendali CLR.3 Applicare le misure definite nel piano di adeguamento, approvato dai vertici aziendali CLR.4 Verificare nel tempo l'effettiva applicazione delle misure necessarie a garantire la conformità con leggi e regolamenti, condividendo con i referenti aziendali preposti, i gap e/o le criticità che possono comportare non conformità e ripercussioni legali di carattere civile e/o penale

Identificazione delle minacce

Tabella 6.4: **Protezione da Virus (PV)**

Descrizione:	I sistemi informativi sono comunemente esposti a software malevoli, denominati malware, soprattutto se connessi a internet. La compromissione attraverso malware può avvenire mediante diverse modalità, quali l'apertura di una e-mail infetta, la navigazione su siti compromessi, l'apertura di file su dispositivi locali o contenuti su memorie di massa esterne (come Storage USB). Soluzioni di protezione specifiche devono essere adottate per monitorare, individuare e rimuovere il software malevolo.
Subcategory:	▪ DE.CM-4 Il codice malevolo viene rilevato
Controlli applicabili:	PV.1 Soluzioni di protezione da malware (es. software antivirus e/o soluzioni per protezione endpoint) devono essere adottate su tutti i sistemi aziendali come computer, server e dispositivi mobili aziendali, inclusi quelli afferenti ai sistemi di controllo industriale (es. sistemi SCADA) PV.2 La protezione malware deve essere efficace nel contrasto a tutte le forme di malware: Virus, Worm, Trojan, Spyware, Rootkit, Botnet, Keystroke Loggers, Adware. PV.3 La protezione da malware deve essere mantenuta costantemente aggiornata nel tempo, ricorrendo il più possibile a meccanismi automatici di aggiornamento che prevedano controlli come minimo giornalieri; PV.4 La soluzione di protezione da malware deve essere sempre attiva e non disattivabile dagli utenti. Deve essere inoltre configurata per: (a) Rimuovere o isolare (porre in quarantena) i file infetti da malware (b) Eseguire scansioni a intervalli regolari di tutti i file (c) Fornire notifiche nel caso di identificazione di sospetto malware PV.5 La soluzione deve assicurare la protezione nei seguenti casi: (a) Accesso a file e dati memorizzati localmente, su dispositivi esterni o su server centralizzati (es. file server) (b) Accesso a e-mail e relativi allegati (c) Accesso a pagine web durante navigazione internet, prevenendo la connessione a siti malevoli (d) Accesso Instant Messanger e qualsiasi altra forma di comunicazione che consenta lo scambio di file o di informazioni

Protezione dei sistemi e delle infrastrutture

Tabella 6.5: **Protezione perimetrale (PP)**

Descrizione:	Le reti di computer di un organizzazione, collegate a Internet o interconnesse con altre reti, devono essere protette da attaccanti volti ad avere accesso ai sistemi, computer e alle informazioni ivi contenute. Un dispositivo di sicurezza di rete come il firewall, posizionato sul perimetro della rete, è in grado di proteggere la stessa contro le minacce cyber basilari - attacchi che richiedono capacità e tecniche limitate, e che conseguentemente risultano largamente diffusi - limitando il traffico di rete in entrata e in uscita alle sole connessioni autorizzate. Tali restrizioni si ottengono applicando delle impostazioni di configurazione note come regole (o policy) del firewall. Questa soluzione deve essere opportunamente installata, configurata e gestita nel tempo, al fine di non vanificare il conseguimento delle specifiche finalità.
Subcategory:	▪ PR.PT-4: Le reti di comunicazione e controllo sono protette
Controlli applicabili:	PP.1 Uno o più firewall (o dispositivi di protezione equivalenti) devono essere installati sul perimetro di rete più esterno dell'organizzazione (ed esempio tra la rete Internet e la rete interna) PP.2 Ogni regola che consenta il passaggio di traffico attraverso il firewall, legato a comunicazioni informatiche, deve essere soggetta ad approvazione da parte di un referente aziendale PP.3 Servizi non approvati o servizi tipicamente vulnerabili devono essere disattivati o bloccati, attraverso specifiche regole del firewall PP.4 Le regole firewall che non sono più necessarie (ad esempio perché il servizio non è più necessario) devono essere rimosse o disabilitate in modo tempestivo PP.5 Le password associate alle credenziali di amministrazione dei firewall devono essere modificate, in alternativa a quelle fornite di base dal produttore e attribuite ad account uninominali PP.6 L'interfaccia amministrativa utilizzata per gestire il sistema deve essere protetta da accesi non autorizzati, attraverso tecniche di Strong Authentication (es. basata su due fattori indipendenti di autenticazione) o password forti se acceduta solamente dalla rete interna. Le utenze devono essere bloccate dopo un numero massimo di tentativi di accesso non andati a buon fine

Tabella 6.6: **Controllo Accessi (CA)**

Descrizione:	Modalità di controllo accessi devono essere stabilite per limitare l'accesso alle informazioni, applicazioni, sistemi, reti e in generale dispositivi informatici aziendali da parte di tutti le tipologie di utenti. L'obiettivo è garantire che solo gli utenti effettivamente autorizzati possano accedere a tali sistemi o dati, assicurando il livello di privilegio minimo necessario a esercitare le proprie funzioni.
Subcategory:	■ PR.AC-1: Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate ■ PR.AC-3: L'accesso remoto alle risorse è amministrato ■ PR.AC-4: Gli accessi alle risorse sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni ■ PR.AT-2: Gli utenti privilegiati (es. Amministratori di Sistema) comprendono ruoli e responsabilità ■ PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati
Controlli applicabili:	CA.1 Le misure di controllo degli accessi devono interessare: (a) Tutte le tipologie di individui (dipendenti, fornitori, partner, ecc.) (b) Tutti i tipi di informazione, servizi o sistemi con cui gli individui devono interagire CA.2 Tutto il personale (interno ed esterno) deve essere univocamente identificato e autenticato per accedere a servizi, sistemi e informazioni aziendali attraverso l'impiego di identificativi nominali (account) CA.3 Nel caso di impiego di strumenti di autenticazione come username e password, questi devono rispondere ai seguenti criteri: (a) Impiego di password robuste (almeno 8 caratteri alfanumerici e utilizzo di caratteri speciali, es. $, #, !,?,"), possibilmente attuato attraverso meccanismi di impostazione e controllo automatici (b) Aggiornamento periodico delle password con cadenza non superiore ai 60 giorni CA.4 L'assegnazione delle credenziali di accesso e dei relativi privilegi devono essere soggetti a un processo di approvazione e deve avvenire nel rispetto dei seguenti principi: (a) Minimo privilegio, ovvero con assegnazione dei privilegi minimi necessari a esercitare le proprie mansioni (i.e., Least Privilege) (b) Accesso alle sole informazioni strettamente necessarie allo svolgimento delle proprie mansioni (i.e., Need-to-Know) (c) Segregazione dei ruoli, al fine di separare attività incompatibili tra soggetti diversi CA.5 Le credenziali impiegate per attività specifiche, come quelle di amministrazione dei sistemi e delle applicazioni informatiche, devono essere gestite nel rispetto dei seguenti criteri: (a) Limitate a un numero ristretto di individui, preventivamente autorizzati e gestite in conformità con la normativa vigente (b) Differenziate da quelli impiegate per altri scopi CA.6 Gli account e i privilegi di accesso devono essere disabilitati quando non più necessari (es. cambiamento di struttura, abbandono dell'organizzazione) o dopo un periodo di inattività

Tabella 6.7: **Configurazione sicura dei sistemi (CSS)**

Descrizione:	I computer e i dispositivi di rete non possono essere considerati sicuri quando configurati con le impostazioni standard fornite in origine dai produttori. Spesso infatti le credenziali amministrative, o in generale le configurazioni impostate dal produttore, sono pubbliche o insicure e potrebbero essere usate per ottenere l'accesso non autorizzato ai sistemi di un'azienda e alle informazioni in questi contenute. Applicando alcuni semplici accorgimenti di sicurezza durante la configurazione di nuovi computer o sistemi informatici è possibile ridurre considerevolmente i rischi e le probabilità che un attacco informatico vada a buon fine.
Subcategory:	▪ PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale
Controlli applicabili:	CSS.1 Disabilitare le utenze non strettamente necessarie, soprattutto quelle caratterizzate da privilegi elevati (es. utenze amministrative e di sistema e di sistema) CSS.2 Cambiare immediatamente le utenze non nominali e qualsiasi password standard pre-impostata dai produttori, adottando utenze uninominali e password robuste CSS.3 Rimuovere o disabilitare il software e i servizi non necessari (incluse applicazioni e strumenti di amministrazione) CSS.4 Disabilitare le funzioni di "auto avvio" al fine di prevenire ad esempio la possibilità che un software venga automaticamente eseguito quando un dispositivo esterno (es. Storage USB) è connesso a un computer CSS.5 Adottare un personal firewall (o equivalente) su PC, laptop e altri dispositivi informatici di produttività personale o aziendale, bloccando le connessioni di rete non autorizzate CSS.6 Utilizzare protocolli di rete cifrati per la gestione remota dei server e dei dispositivi di rete (es. SSH, SSL) CSS.7 Impostare le utenze tecniche (application to application o machine to machine) in maniera tale che non ne sia possibile l'utilizzo interattivo da parte di utenti CSS.8 Attivare le funzionalità logging sui sistemi. In caso di trattamento di dati personali, occorre conformarsi a quanto previsto dalla normativa in materia. CSS.9 Configurare i sistemi in maniera tale che l'utente finale non possa modificare in autonomia le configurazioni impostate

Tabella 6.8: **Aggiornamento dei sistemi (AS)**

Descrizione:	I software presenti su tutti i computer e più in generale sui sistemi informatici possono contenere difetti ed errori, genericamente conosciuti come "vulnerabilità". Queste rappresentano degli elementi di debolezza intrinseci, sfruttabili da individui o gruppi di attaccanti, come anche da malware o altri programmi malevoli. Le vulnerabilità, dal momento della loro scoperta, fino al momento in cui sono eventualmente sfruttate, devono essere individuate e gestite attraverso opportune contromisure, come ad esempio l'installazione degli aggiornamenti rilasciati dai produttori software, proprio per risolvere una o più vulnerabilità. I produttori di software sono difatti responsabili per la fornitura di correzioni per le vulnerabilità identificate, nel più breve tempo possibile, in forma di aggiornamenti software, conosciuti anche come "Patch di sicurezza" e rilasciati ai clienti nell'ambito dei contratti di licenza. Per ridurre i rischi di compromissione di informazioni e sistemi informatici attraverso lo sfruttamento delle vulnerabilità del software, le aziende e organizzazioni devono gestire efficacemente tali processi di aggiornamento del software.
Subcategory:	▪ RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato
Controlli applicabili:	AS.1 I software installati sui sistemi aziendali come computer, server, apparati di rete,dispositivi mobili, ecc. devono disporre della licenza del fornitore in modo da garantire la disponibilità di aggiornamenti di sicurezza o di aggiornamenti che comunque possano avere un impatto su di essa AS.2 Le aziende devono individuare e ottenere Patch (inclusi aggiornamenti critici, service pack), quando resi disponibili per porre rimedio alle vulnerabilità scoperte, interagendo con i produttori di software o completando il recupero delle stesse dai siti web ufficiali o autorizzati da questi ultimi AS.3 Gli aggiornamenti devono essere installati in modo tempestivo e,ove possibile, previa valutazione degli impatti, attraverso meccanismi che prevedano l'aggiornamento automatico degli stessi AS.4 Il software non più supportato (i.e., Out-of-Date) deve essere rimosso dai sistemi aziendali o sostituito con versioni più recenti (e per le quali il produttore rilascia gli aggiornamenti)

Tabella 6.9: **Formazione di base del personale (FBP)**

Descrizione:	Gli utenti delle aziende che interagiscono con i sistemi informatici rappresentano la principale fonte di rischio cyber. I comportamenti non consoni o errati possono vanificare le più sofisticate misure di sicurezza adottate da un'azienda. Per migliorare la consapevolezza degli utenti nell'utilizzo consono degli strumenti informatici e delle informazioni, l'organizzazione deve prevedere specifici programmi di sensibilizzazione e formazione, volti a migliore la percezione dei rischi cyber e a promuovere l'utilizzo di comportamenti appropriati. Specifici programmi di sensibilizzazione e formazione devono essere rivolti a tutto il personale interno o esterno che accede, direttamente o indirettamente, ai sistemi informatici e alle informazioni dell'organizzazione. Tali programmi devono essere orientati a creare una cultura della sicurezza cyber, tale da prevenire comportamenti non consoni e ridurre di conseguenza l'esposizione ai rischi.
Subcategory:	▪ PR.AT-1: Tutti gli utenti sono informati e addestrati
Controlli applicabili:	FPB.1 Pieno coinvolgimento e approvazione dei piani di formazione e sensibilizzazione del personale da parte dei vertici aziendali che ne comunicano l'importanza e ne monitorano il completamento FPB.2 Svolgimento di sessioni con cadenza almeno annuale mediante formazione in aula e/o ricorrendo all'utilizzo di piattaforme di e-learning FPB.3 Richiami alla cyber security integrati nelle attività quotidiane, mediante il ricorso a diverse tecniche e modalità di comunicazione (es. poster esplicativi negli uffici, e-mail di sensibilizzazione sui rischi e i comportamenti corretti, distribuzione di opuscoli specifici, sezioni dedicate su siti e portali interni). FPB.4 I temi trattati devono includere come minimo: (a) Principi di sicurezza (b) Utilizzo appropriato degli strumenti aziendali (PC, dispositivi mobili, ecc.) e rischi correlati al loro utilizzo improprio o non corretto (c) Comportamenti da tenere in caso di eventi sospetti (es. ricezione di mail sospette, comportamenti non usuali degli strumenti aziendali) o nel caso di incidenti di sicurezza (es. compromissioni di sistemi o supporti esterni) (d) Ruoli e responsabilità specifiche in tema di cyber security (e) Leggi o regolamenti applicabili e conseguenze in caso di violazione FPB.5 Formazione dedicata e specialistica per gli utenti dotati di privilegi di accesso elevati (es. amministratori di sistemi informatici), volti ad accrescere e mantenere nel tempo aggiornate le competenze specifiche sui rischi cyber e sulle relative tecniche di protezione

Tabella 6.10: **Backup & Restore (BR)**

Descrizione:	La disponibilità delle informazioni e dei sistemi è essenziale per garantire l'operatività stessa di un'azienda nel mercato. Il controllo primario da attuare è rappresentato dal salvataggio delle informazioni di business e delle configurazioni dei sistemi, su supporti dedicati, da impiegare in caso di disastri, guasti o errori umani, favorendo il ripristino della normale operatività.
Subcategory:	▪ PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati periodicamente
Controlli applicabili:	BR.1 Devono essere adottati adeguati meccanismi e strumenti finalizzati al salvataggio e ripristino di informazioni e dati BR.2 Deve essere definita la tipologia (parziale o totale) e la frequenza di completamento dei salvataggi. Questa deve essere stabilita in base alle esigenze di business dell'organizzazione, i requisiti di sicurezza delle informazioni, gli obblighi di legge e la criticità delle informazioni, trattate rispetto al mantenimento delle attività operative BR.3 Deve essere verificato periodicamente (es. attraverso attività di test) il buon esito delle attività di salvataggio e di ripristino di informazioni e dati BR.4 I backup devono essere conservati in una sede remota, a una distanza sufficiente dalla sede principale, o avvalendosi di servizi cloud aventi analoga finalità, per evitare compromissioni in caso di eventi di disastro. Questi devono essere protetti con analoghe misure di carattere fisico e logico, rispetto a quelle adottate nelle sedi principali.

Risposta agli incidenti di sicurezza

Tabella 6.11: **Risposta agli incidenti di sicurezza (RI)**

Descrizione:	Nei casi in cui le misure di sicurezza non siano in grado o risultino limitatamente efficaci nella prevenzione di eventi avversi di sicurezza (es. compromissione di un sistema, accesso non autorizzato alle informazioni), l'organizzazione deve avere la capacità di rispondere rapidamente ed efficacemente a un potenziale incidente di sicurezza, riducendo gli impatti e limitando la possibilità di occorrenze future.
Subcategory:	▪ RS.MI-1: In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto ▪ RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti
Controlli applicabili:	RI.1 Descrivere e rendere note a tutto il personale interessato le prassi da adottare in caso di sospetta violazione o incidente di sicurezza (i.e., processo di gestione degli incidenti) RI.2 Il processo di gestione degli incidenti deve definire come minimo: (a) Criteri generali da adottare per riconoscere un incidente (b) Tipologie di incidenti con relativa scala della severità, necessarie a effettuare una prima classificazione (c) Elenco dei referenti interni (es. responsabile Sistemi Informativi, responsabile Comunicazione, Responsabile legale, Direzione Aziendale) ed esterni (es. organi di Polizia Giudiziaria, fornitori esterni) da contattare in caso di incidente (d) Criteri di notifica degli incidenti ai diversi referenti e criteri di risposta, relativi ruoli e responsabilità, finalizzati a contenere gli impatti e/o mitigarne gli effetti in funzione di ciascuna tipologia e severità (e) Criteri, ruoli e responsabilità, procedure per il ripristino della situazione precedente al verificarsi dell'incidente

7. Raccomandazioni per le Grandi Imprese

Negli ultimi decenni il valore patrimoniale degli asset aziendali si è progressivamente espanso con uno spostamento dal fisico al virtuale. In molti settori gli asset virtuali, come la proprietà intellettuale, la reputazione e la fiducia online, la base clienti online e altri asset immateriali, hanno superato per valore economico e, talvolta per criticità, quelli fisici. Inoltre, l'uso delle tecnologie di Information Communication & Technologies (ICT) nei processi produttivi ha interessato numerosi settori chiave per l'economia nazionale, da quello finanziario all'energetico, dai trasporti alle telecomunicazioni, dal chimico alla grande distribuzione organizzata e così via. Inoltre, con l'avvento dell'"Industry 4.0", anche i processi produttivi tradizionali si sono evoluti in modo tale che l'ICT ne sia divenuto una componente strategica e indispensabile.

Questo nuovo scenario espone tutte le aziende e le istituzioni a rischi nuovi, quali furto di proprietà intellettuale, manomissione di dati, discontinuità operativa o addirittura effetti sulla qualità e safety degli impianti produttivi. Tutto ciò può avere impatti, non trascurabili, sul posizionamento competitivo e sul valore dell'azienda, ivi inclusi il prezzo delle azioni o il valore per l'azionista.

L'evoluzione verso le tecnologie dell'informazione è stata accompagnata anche da una diversificazione e proliferazione delle minacce di tipo informatico: nell'arco di pochi anni gli attacchi cyber perpetrati da una molteplicità di attori – ad esempio attivisti, criminali e gruppi sostenuti da governi - si sono aggiunti a quelli noti del mondo fisico. La conseguenza di siffatto scenario, tra i vari motivi, è stata l'apparizione della cosiddetta "guerra ibrida", in cui elementi tipici della sicurezza fisica e i nuovi di quella cibernetica si sono uniti coinvolgendo direttamente in primis le infrastrutture critiche nazionali.

Le aziende e le organizzazioni possono avviare un processo di evoluzione della propria sicurezza attraverso iniziative e attività progettuali specifiche. A titolo di supporto all'individuazione e all'avviamento di iniziative strategiche, riportiamo alcuni suggerimenti per il top management e alcune proposte di progetto che aiutano le aziende a indirizzare in modo ampio l'evoluzione della propria capacità di protezione e difesa, sia estendendo l'ampiezza dei propri controlli, sia il livello di maturità degli stessi.

7.1 Il ruolo del top management nella gestione del rischio cyber

Le aziende sono sempre più bersaglio di minacce sofisticate e per tali ragioni hanno cominciato a dotarsi di ingenti risorse tecnologiche e finanziarie per difendersi. Le minacce riguardano tutte le aziende: non solo le grandi, ma anche le medie e le piccole sono diventate bersagli abituali, vista la ricchezza di asset immateriali e il basso livello di protezione. I danni non sono esclusivamente legati al furto di proprietà intellettuale, ma anche alla reputazione dell'azienda. è sempre più frequente che a causa di attacchi, alcuni dirigenti perdano la propria posizione. Le sempre più diffuse regole di Corporate Governance impongono che i dirigenti siano responsabili della conduzione e protezione delle proprie attività. Per i motivi su esposti, è necessario che i consigli di amministrazione e il top management di aziende/istituzioni/organizzazioni comprendano e valutino i nuovi rischi, bilanciando la crescita e la profittabilità di mercato con la tutela dell'azienda e la mitigazione dei rischi. Tale compito è già previsto nel mandato del Consiglio di Amministrazione che, anche attraverso il Comitato Controllo e Rischi ove presente, è chiamato a definire la natura e il livello di rischio compatibile con gli obiettivi strategici dell'azienda, includendo nelle valutazioni tutti i rischi che possono assumere rilievo nell'ottica della sostenibilità nel medio-lungo periodo dell'attività dell'azienda. Inoltre, il Consiglio è anche chiamato a valutare l'adeguatezza dell'assetto organizzativo, amministrativo e contabile dell'azienda. Tali principi sono ad esempio già contenuti nel codice di autodisciplina di Borsa Italiana [8]. Non vi è dubbio che il rischio cyber debba essere valutato come potenziale "rischio principale" per le aziende e le organizzazioni pubbliche, come evidenziato nella Relazione Annuale 2014 della Presidenza del Consiglio dei Ministri sulla politica per la Sicurezza della Repubblica [22].

Non vi è dubbio che, vista la portata e gli effetti della minaccia cyber, questa debba rientrare tra i rischi di alto rilievo che oramai ogni azienda e organizzazione deve valutare e gestire. Nell'ambito dell'attuazione di questi principi di Corporate Governance e in linea con le indicazione contenute nel Quadro Strategico e nel Piano Nazionale, le aziende dovrebbero avviare le seguenti iniziative/pratiche a livello di Consiglio d'Amministrazione e top management:

1. **Il rischio cyber** – Il Consiglio di Amministrazione e i vertici aziendali (di seguito indicati "top management") inseriscono i rischi cyber (o informatici) tra i rischi di alto livello. I rischi devono essere valutati in maniera precisa e analitica, identificando i possibili impatti sull'azienda, la clientela e le entità esterne (altri operatori del settore, cittadini/società civile, governo). Le valutazioni di questi rischi sono supportate dal Comitato Controllo e Rischi (CCR) ove presente, attraverso una adeguata attività istruttoria sia di natura consultiva sia propulsiva. Il top management deve affrontare il tema della cyber security come un problema di gestione generale del rischio (Enterprise risk management) e non esclusivamente come un problema dell'"Information Technology".

2. **La cyber security come elemento strategico nelle politiche di governance aziendale** – La Governance aziendale si riferisce all'insieme di regole, di ogni livello (leggi, regolamenti etc.) che disciplinano la gestione e la direzione di un'azienda (o più in generale di un'organizzazione, sia essa pubblica o privata) e include le relazioni tra i vari attori coinvolti (gli stakeholder) e gli obiettivi dell'organizzazione stessa. Gli attori principali sono gli azionisti (shareholders), il consiglio di amministrazione (board of directors) e il management. Più in generale, il governo di un'organizzazione abbraccia una serie di regole, relazioni, processi e sistemi aziendali, tramite i quali l'autorità fiduciaria è esercitata e controllata. La struttura della governance aziendale esprime quindi le regole e i processi con cui si prendono le decisioni in un'azienda, le modalità con cui vengono decisi gli obiettivi aziendali nonché i mezzi per il raggiungimento e la misurazione dei risultati raggiunti.

Tutte le aree di un'azienda contribuiscono a stilare le linee guida che consentono di definire la governance dell'organizzazione e in tal senso, anche la cyber security deve essere considerata in un'ottica di visione sistemica condivisa per cui la cyber non sia vista come elemento posticcio o di disturbo, bensì sia integrata come uno degli aspetti fondamentali nella definizione dei rischi, ergo sia considerata uno degli elementi strategici intorno ai quali si estrinseca la visione aziendale.

Il top management predispone dunque un piano di governo integrato della cyber security che coinvolga tutte le funzioni aziendali e che includa tutte le aree di rischio operativo, definendo chiaramente i ruoli e le responsabilità e la loro opportuna separazione (principio della segregazione dei compiti) che individui tre livelli di controllo: controllo di primo livello, sotto la responsabilità diretta di chi opera la funzione (produzione, IT, vendite, ecc.); controlli di secondo livello, sotto la responsabilità di una funzione di sicurezza, esterna alle funzioni di produzione/business; controlli di terzo livello, sotto la responsabilità delle funzioni di controllo interno (audit). La funzione responsabile dei controlli di secondo livello dovrà occuparsi di definire le politiche di sicurezza aziendale e verificarne la loro corretta applicazione (compliance). Inoltre, il top management si assicura che il piano di governo integrato risponda alle seguenti esigenze:

(a) fornisca un allineamento tra la gestione del rischio e gli obiettivi strategici dell'azienda;

(b) definisca un modello organizzativo che fornisca una copertura dei processi e domini di sicurezza di tutta l'azienda;

(c) definisca, nel modello organizzativo, un processo di gestione integrata del rischio al fine di inquadrare e contestualizzare, valutare, rispondere e monitorare i rischi relativi all'organizzazione e ai suoi asset, servizi, individui, altre organizzazioni e allo Stato;

(d) allochi in modo efficiente ed efficace le risorse richieste da una gestione sistemica aziendale, inclusa la gestione dei rischi;

(e) definisca un processo di monitoraggio e reportistica dell'efficacia ed efficienza organizzativa (secondo le metriche desiderate e condivise con il top management) nonché un processo di gestione del cambiamento nel caso di esigenza di modificare la propria struttura aziendale, avvalendosi di opportuni approcci di analisi (es.: System Dynamics) che tengano in considerazione la dinamicità e la "sistemicità" intrinseche dell'organizzazione;

(f) fornisca, in tale processo, una misurazione, monitoraggio e presentazione del processo di gestione dei rischi.

Il top management si assicura che il modello di governo e il piano di cyber security siano integrati con il piano aziendale per la gestione dei rischi (Enterprise risk management) e il piano di gestione crisi o "crisis management". Sempre più frequentemente gli impatti derivati dalla minaccia cyber sono classificabili come crisi e pertanto è indispensabile una gestione coerente e integrata, eventualmente avvalendosi di strumenti e metodologie di supporto alle decisioni che forniscano un'ottica integrata del modello di sistema e considerino tutte le dinamiche aziendali (es. Model-based Governance). Tra gli aspetti che vengono portati all'attenzione del top management vi sono anche quelli relativi alla gestione del rischio nel caso di contratti di outsourcing e cloud. Spesso si crede erroneamente che vi sia cessione del rischio, ma non è così: vi è solo una modalità diversa di gestione operativa della sicurezza, che richiede attente valutazioni sia da parte del top management, sia del CISO e delle strutture coinvolte nella gestione del servizio.

3. **Ruoli e e responsabilità** – Una corretta Governance aziendale che sia integrata, ossia che abbia una visione olistica, e condivisa dal proprio management, delle interdipendenze tra le varie funzioni aziendali, e degli impatti che alcune problematiche in una di tali funzioni potrebbero provocare a cascata su altre, deve prevedere la definizione di un corretto assetto organizzativo, che includa da un lato un processo di miglioramento continuo sia nei propri processi che nelle proprie policy e dunque l'abbattimento di modelli mentali errati da pate dei responsabili di funzione, tendendo così a quella che viene virtuosamente definita una Learning Organization. Ad esempio, è ormai noto che alcune strategie di aggressione di tipo sociale (attraverso il multiforme fenomeno noto come Insider Threat) si sono dimostrate particolarmente efficaci per aggirare controlli marcatamente tecnologici a discapito di procedure di sicurezza relative all'introduzione di materiali informatici esterni all'azienda, oppure attraverso la dissimulazione di personale di servizio esterno (come nel noto caso del Mall Target, negli USA). La cyber security è una tematica che tocca dunque tutta l'azienda, dal top management alle strutture operative, e deve essere pertanto soggetta ad una valutazione sistemica e ad un monitoraggio continuo. L'errore che spesso le aziende commettono è di assegnare la gestione della cyber security in maniera esclusiva alla struttura ICT. Sebbene l'ICT ricopra un ruolo rilevante nella gestione della sicurezza, questa impostazione presenta alcuni possibili problemi; ne elenchiamo alcuni:

   (a) il rischio cyber viene visto principalmente da un punto di vista dei sistemi informativi, fornendo spesso contromisure inadeguate;

   (b) si assume implicitamente che vi sia una limitata coniugazione tra le esigenze del business e la riduzione dei rischi di tutta l'organizzazione;

   (c) si introducono difficoltà organizzative intrinseche nell'implementare processi e contromisure di sicurezza all'interno delle varie funzioni aziendali (di business, di produzione, amministrative, ecc.);

   (d) vi è una parzialità dei piani di gestione della sicurezza;

   (e) possibile tensione tra investimenti ICT e investimenti di sicurezza (non di rado, tagli ai budget ICT ricadono direttamente sui budget di cyber security).

   Al fine di garantire una copertura completa dell'azienda, sarebbe opportuno affiancare le funzioni di sicurezza che si trovano all'interno della divisione ICT, con funzioni di sicurezza "logica" collocate al di fuori dell'ICT (solitamente a riporto del Chief Security Officer o del Chief Risk Officer, oppure in alcuni casi a riporto diretto del Direttore Generale, del Chief Operating Officer o dell'Amministratore Delegato). Questa funzione di sicurezza logica è guidata dal CISO - Chief Information Security Officer. Questa impostazione garantisce i principi di segregazione delle responsabilità, nonché consente di poter differenziare i controlli di sicurezza di primo livello (a carico dell'ICT o delle funzioni di business/produzione) dai controlli di secondo livello (a carico del CISO e/o della funzione di sicurezza logica).

4. **Il ruolo del CISO** – La figura del Chief Information Security Officer o CISO è individuata dal top management, che si accerta che il ruolo sia assegnato a persona con adeguate competenze ed esperienza in materia. Tra le responsabilità del CISO vi dovrà essere: a) Avviamento/evoluzione di un piano di gestione dei rischi informatici aziendali, in linea con il processo generale di gestione dei rischi (Enterprise risk management) b) Monitoraggio dell'evoluzione dei rischi e conseguente adeguamento del piano c) Analisi dei maggiori incidenti, delle loro conseguenze e delle azioni intraprese per la mitigazione di future occorrenze d) Relazione periodica al top management e) Funzione di raccordo tra il top management, le funzioni aziendali e le istituzioni nazionali ed estere. Nelle aziende di

medie/grandi dimensioni, tale ruolo dovrebbe essere assegnato a figura dedicata a questo scopo.

5. **Monitoraggio integrato** – Il top management valuta periodicamente i rischi individuati, di concerto con l'ERM complessivo, e il piano previsto per la loro mitigazione. Il top management è chiamato a esprimersi e decidere sulle scelte relative alle strategie di mitigazione/accettazione/cessione del rischio cyber, così come già avviene per tutti gli altri rischi a cui è esposta l'azienda.

6. **Risorse** – Il top management dovrà valutare se il piano di sicurezza sia correttamente supportato da adeguate risorse in termini economici e di personale chiamato a svolgere le attività inerenti. Le risorse allocate dovranno essere coerenti e in linea con il piano di gestione dei rischi aziendali (Enterprise risk management). L'eventuale rischio residuo dovrà essere correttamente valutato e se non in linea con le linee generali, si dovrà definire dei piani di trattamento dei rischio, valutando l'opportunità di ridurre il rischio tramite applicazioni di contromisure, evitare il rischio, eliminando le sorgenti di questo rischio, oppure trasferire il rischio.

7. **Consapevolezza e cultura della cyber security** – Il top management dovrà condurre attività per promuovere la consapevolezza e la cultura della cyber security a tutti i livelli aziendali. Il CISO predisporrà un programma per aumentare la consapevolezza del personale interno ed esterno al fine di ridurre i rischi derivati da uso improprio o errato degli strumenti e dei processi informativi dell'organizzazione. Inoltre, potranno essere previste esercitazioni interne e/o di settore e nazionali per testare e migliorare la capacità del top management e delle strutture operative di gestire eventi cyber.

8. **Scambio di informazioni e cooperazione** – Il top management dovrà promuovere e supportare iniziative finalizzate a stabilire e rafforzare rapporti di cooperazione con altre organizzazioni dello stesso settore e con gli organi istituzionali deputati al contrasto della Minaccia cyber. L'adesione a CERT di Settore o CERT a carattere istituzionale (come il CERT Nazionale) e la cooperazione con altre organizzazioni permette di migliorare la comprensione della minaccia, la condivisione di pratiche e strumenti di contrasto e, in alcuni casi, di poter sviluppare capacità comuni.

7.2 Il processo di cyber security risk management

Con l'evoluzione delle minacce cyber è necessario adeguare anche l'approccio alla protezione del patrimonio informativo, delle infrastrutture informatiche e dei processi di business, passando da un paradigma statico a una visione dinamica del rischio. Nella Figura 7.1 è illustrato un processo tradizionale di gestione dei rischi relativi alla sicurezza delle informazioni, con una limitata integrazione del rischio a livello enterprise, spesso demandata al personale tecnico IT. Il processo si esaurisce inoltre all'interno dell'ambito aziendale, senza interazioni, se non sporadiche e non strutturate, con il mondo esterno. Diversamente, il cyber security risk management è un processo continuo e dinamico, da cui desumere le azioni da implementare per la gestione del rischio in modo consapevole, adeguato agli asset da proteggere e in linea, sul piano temporale, con i mutamenti organizzativi, ambientali e tecnologici che coinvolgono l'azienda internamente ed esternamente. In assenza di questo processo, l'azienda rischia di investire e sostenere costi su aree non prioritarie e/o di non investire opportunamente su aree ad alto rischio.

Focalizzandosi sugli scenari di attacco in continua evoluzione, uno dei possibili processi evoluti di gestione del rischio cyber viene illustrato di seguito. Esso si basa sull'introduzione di nuove importanti componenti:

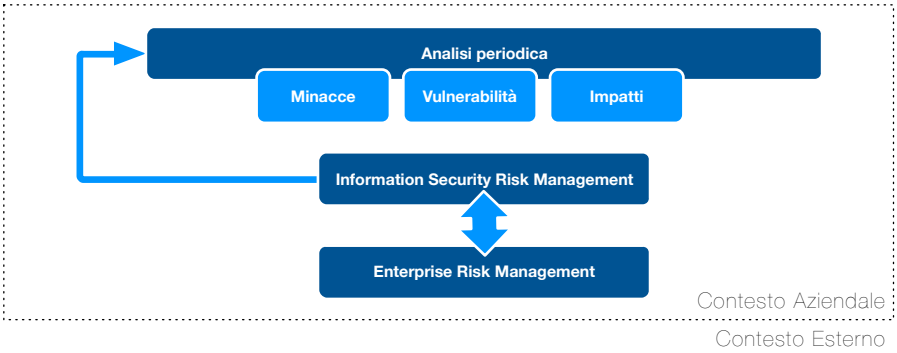

Figura 7.1: Un approccio tradizionale alla gestione del rischio IT.

- Cyber intelligence – analisi delle minacce nel "mondo reale" attraverso un costante presidio e analisi predittiva di informazioni provenienti da fonti prevalentemente esterne al contesto aziendale; Questa componente di cyber intelligence può essere alimentata attraverso un processo di information gathering, da fonti istituzionali (CERT, Intelligence, Polizia Postale ecc.) e da fonti private (business information agencies) che di fatto fungono anche da certificatori della qualità delle informazioni.

- Monitoraggio Continuo – analisi continua delle informazioni provenienti dalle fonti interne al contesto aziendale (ad esempio CERT e SOC), al fine di raffinare e contestualizzare le probabilità di accadimento degli eventi di minaccia, agendo come fattore abilitante per il calcolo dinamico del rischio;

- Threat modelling – identificazione e selezione dei fattori (minacce, vulnerabilità ed impatti) in grado di rappresentare i potenziali scenari di minaccia, con valutazione dettagliata dei rischi in base alla comprensione delle capacità e delle intenzioni dei potenziali attaccanti;

- Information Sharing – scambio di informazioni rilevanti e tempestive per la prevenzione e/o il contrasto della minaccia Cyber verso soggetti governativi (come ad esempio il CERT Nazionale o gli ISAC in USA), pubblici e privati, a valle della definizione di accordi di condivisione.

La Figura 7.2 illustra tale processo evoluto di gestione del rischio cyber, coerente con i principi sopra espressi. In particolare, il processo prevede che l'organizzazione utilizzi politiche di information gathering e information sharing per alimentare una componente di cyber intelligence e che condivida parte di questa informazione mediante i medesimi canali di information sharing. In questo modo l'organizzazione non si limita soltanto a considerare i potenziali rischi inerenti al contesto interno all'azienda, ma valuta anche i potenziali rischi riferiti al contesto esterno, soprattutto in relazione al livello di interconnessione che il proprio sistema informativo ha rispetto al mondo esterno. La Figura mette anche in risalto il nuovo ruolo giocato dal processo di cyber security risk management che è ora parte integrante e fondamentale di una gestione del rischio globale e in cui gioca un ruolo fondamentale il top management. Con questo approccio, il processo di cyber security risk management riceve informazioni e dati dai componenti di cyber intelligence e dal monitoraggio continuativo dell'infrastruttura IT per definire, in un processo ciclico e continuo, le strategie migliori per il trattamento del rischio cyber.

La finalità di fondo è quella di spostare il governo delle minacce cyber da un approccio reattivo a un approccio proattivo, mediante un modello dinamico che consenta di leggere l'organizzazione

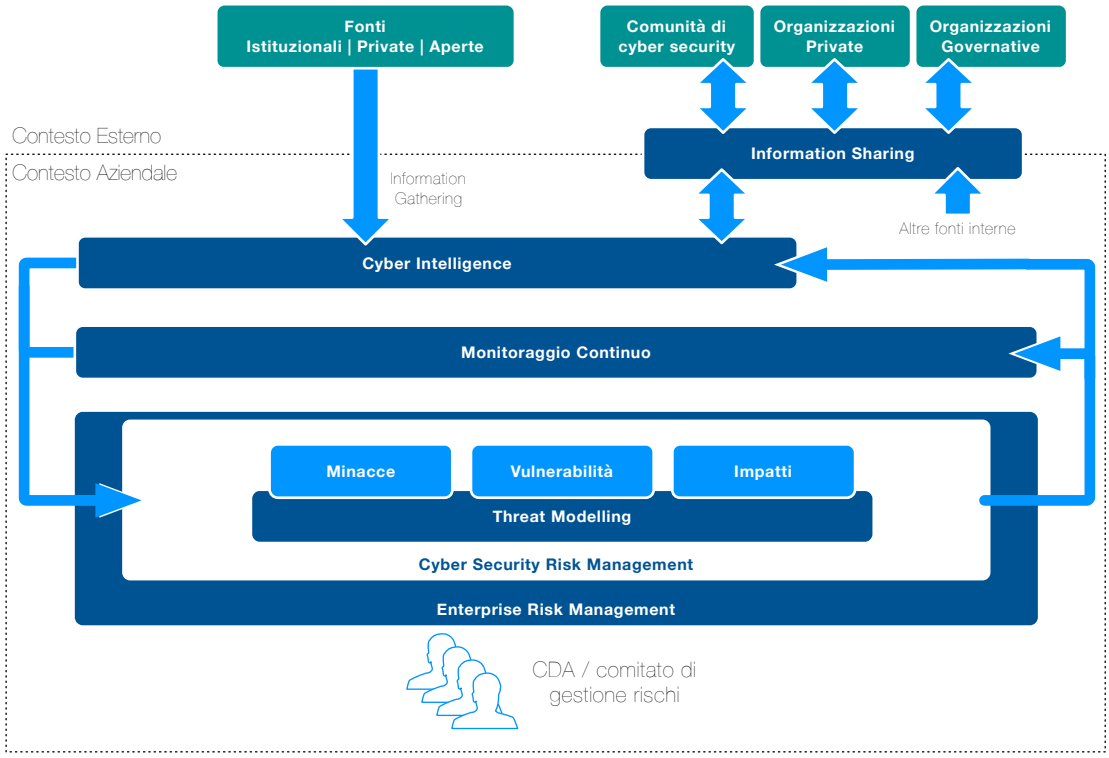

Figura 7.2: Un approccio evoluto alla gestione del rischio cyber.

come un sistema interdipendente di attività, processi, tecnologie, dati, persone, relazioni, ecc. dimensionabile e implementabile progressivamente rispetto alle specificità dell'organizzazione. In questa nuova visione risulta imprescindibile effettuare un'analisi dei rischi cyber all'interno di una più generale analisi sistemica delle dinamiche organizzative, per poter dunque avviare il percorso evolutivo dall' Information Security Risk Management al cyber security risk management, in modo che siano correttamente ponderate le scelte delle strategie e/o delle policy da adottare.

In termini generali, un adeguato processo di cyber security risk management deve essere strettamente correlato con i principali processi di business dell'organizzazione e necessita, in primis, del coinvolgimento sia del Board dell'organizzazione, sia di personale con esperienze e competenze verticali su tematiche di rischio e di sicurezza, nonché del supporto di adeguati strumenti tecnologici abilitanti. Per quest'ultimo aspetto è fondamentale ricorrere a un processo di analisi e selezione delle soluzioni tecnologiche e operative più adeguate, anche mediante il ricorso a servizi di consulenza esterni altamente specializzati, che a partire dalla situazioni *AS IS* individuino le soluzioni più confacenti al contesto dell'organizzazione sulla base dei requisiti del modello *TO BE*.

Nella definizione del processo di cyber security risk management l'organizzazione dovrebbe perseguire i seguenti obiettivi:

- formulare criteri univoci per la valutazione e determinazione dei rischi cyber;
- standardizzare e uniformare un metodo di analisi al fine di ottenere risultati comparabili e confrontabili nel tempo;
- acquisire consapevolezza del livello di rischio cui è esposto ciascun componente del sistema informativo aziendale;

- valutare se il rischio individuato è accettabile o se, invece, è necessario prevedere opportuni trattamenti a mitigazione del rischio stesso.
- mettere a disposizione un metodo adeguato e flessibile per individuare le necessità di protezione tecnologico-organizzative tese a bilanciare in maniera ottimale le possibili contromisure di sicurezza di carattere preventivo o di rilevazione;
- consentire di monitorare e analizzare gli incidenti di sicurezza al fine di mettere in campo interventi migliorativi;
- valutare tutti i potenziali rischi nella definizione e implementazione di nuovi servizi informatici;
- individuare una funzione aziendale che coordini tutte le attività;
- integrare il processo di cyber security risk management all'interno del processo di Enterprise Risk Management (se già presente nell'organizzazione), secondo un Framework comune che consenta un'aggregazione di informazioni finalizzata a ottenere sia una visione sistemica dei rischi aziendali sia una selezione di interventi specifici nell'ambito IT in termini di priorità di mitigazione.
- realizzare un reporting unico verso i vertici aziendali.

L'attivazione del processo di cyber security risk management consentirebbe all'organizzazione di ottenere una serie di benefici tra i quali:

- ottemperare alle normative e regolamenti nazionali e internazionali che richiedono espressamente che l'organizzazione sia dotata di un processo e di una metodologia per l'Analisi dei rischi IT;
- garantire l'aderenza della governance IT agli obiettivi di business aziendali, in termini di evoluzione sostenibile, eccellenza operativa e competitività dei costi, attraverso la riduzione dell'esposizione al rischio;
- pianificare adeguate azioni di risposta a potenziali cyber-attacchi, al fine di minimizzare gli eventuali impatti e quindi di garantire la continuità dei servizi erogati;
- consentire all'organizzazione di ridurre al minimo i costi di sicurezza, garantendo una adeguata riduzione dei rischi a livelli accettabili da parte dell'organizzazione stessa. In altre parole, evitare di sostenere costi per implementare un livello di sicurezza che vada oltre l'ottimale o che si applichi a componenti del sistema informativo a basso impatto per l'organizzazione.

Il disegno e l'attivazione del processo di cyber security risk management richiede un insieme di iniziative che, pur essendo fortemente dipendenti dalla situazione iniziale, comporta un significativo effort (risorse umane, tempo, ecc.). Pertanto l'implementazione dello stesso dovrebbe essere attuata in fasi progettuali distinte.

7.3 Computer Emergency Readiness Team (CERT)

Coerentemente con gli orientamenti nazionali e internazionali, la costituzione di un centro per la gestione degli incidenti critici di cyber security, comunemente conosciuto come CERT, è divenuta una pratica essenziale e diffusa per prevenire e rispondere efficacemente a tale tipologia di incidenti. Il CERT rappresenta il punto di contatto principale dell'organizzazione in materia di cyber security,

sia in termini preventivi per evitare o ridurre gli effetti di una compromissione, sia in termini reattivi e di risposta tempestiva in seguito a uno specifico evento critico; in questo senso opera attivamente per favorire lo scambio informativo con altri CERT e community di sicurezza, sia appartenenti allo stesso settore, sia riferiti a centri di eccellenza specifici in questo ambito. Tra le capacità principali che un CERT deve possedere si segnalano:

- identificazione e analisi proattiva delle principali minacce, funzionali a valutare tempestivamente scenari di compromissione noti o emergenti e che possono avere un impatto diretto sulla Constituency;
- definizione di processi e metodologie strutturate per la gestione degli incidenti, in grado di favorire una risposta rapida e appropriata a eventuali compromissioni, cooperando, ove necessario, con altre organizzazioni (es. altre aziende dello stesso settore) o istituzioni e community di riferimento (es. Forze dell'Ordine, CERT Nazionale);
- sviluppo delle capacità di individuazione tempestiva degli eventi significativi per la sicurezza, anche ricorrendo all'integrazione con altri presidi di cyber security eventualmente presenti nell'organizzazione, come ad esempio il Security Operations Center (SOC)[1];
- disponibilità di strumenti centrali (es. Portale Web, Blog, e-mail sicura, piattaforme di Information Sharing, ecc.) per favorire il colloquio e lo scambio informativo con la Constituency e con gli altri soggetti di interesse (es. Enti, Istituzioni, community di cyber security, ecc.);
- sviluppo e partecipazione a simulazioni interne ed esterne per verificare il grado di robustezza dei processi e delle procedure di risposta agli incidenti;
- supporto alla definizione e somministrazione di programmi di security awareness finalizzati ad aumentare la consapevolezza sui rischi Cyber e favorire i comportamenti corretti in termini di prevenzione degli stessi.

Lo sviluppo e la nascita di un CERT dovrebbe avvenire attraverso il completamento delle seguenti attività principali:

- Definizione degli obiettivi e della Constituency di riferimento, attraverso l'identificazione formale delle finalità che il CERT si prefigge di raggiungere e l'individuazione puntuale della comunità di utente (interni ed esterni) a cui i servizi CERT sono rivolti;
- Scelta accurata dei servizi da erogare, valutando i benefici e le aspettative correlate a ciascun servizio. Tale valutazione dovrebbe essere fondata su criteri e modalità che rendano i servizi effettivamente appropriati e in grado di produrre i massimi benefici per la Constituency;
- Individuazione del modello organizzativo di riferimento, considerando le eventuali sinergie e integrazioni interne, funzionali al raggiungimento degli obiettivi prefissati e al mantenimento degli indicatori di qualità per i servizi erogati (es. tempi di risposta in caso di incidente, frequenza dei bollettini di sicurezza);

[1] Rispetto al CERT, il ruolo del SOC è quello di monitorare costantemente le minacce cyber che possono interessare direttamente le infrastrutture ICT dell'organizzazione, nonché gestire operativamente i dispositivi di sicurezza posti a protezione delle medesime infrastrutture. Il CERT opera in ogni caso in stretto coordinamento con il SOC, fornendo prevalentemente servizi informativi (es. Security Intelligence) e di coordinamento complessivo nella gestione degli incidenti critici (o non noti). L'interazione tra SOC e CERT è normalmente assicurata da un processo condiviso di prevenzione e gestione degli incidenti, basato su criteri specifici di reciproco "ingaggio", volti ad assicurare la stretta cooperazione tra le due funzioni.

- Sviluppo delle capacità tecniche e operative necessarie all'erogazione dei servizi, secondo un modello di riferimento che consideri, da un lato, le best practice del settore, dall'altro le necessità di maturazione graduale nel tempo dei servizi e delle capacità stesse del CERT;
- Definizione dei modelli di condivisione, cooperazione e coordinamento, necessari a massimizzare i benefici derivanti dallo scambio informativo e in generale da una capacità distribuita di contrasto e riduzione degli impatti in seguito a un eventuale attacco cyber;
- Definizione del Piano degli investimenti con relativa roadmap degli interventi, con l'obiettivo di prioritizzare il rilascio dei servizi e delle capacità correlate in un'ottica costi/benefici e tenendo conto delle complessità intrinseche legate alla tematiche (es. necessità di competenze professionali specialistiche, integrazione e utilizzo delle piattaforme tecnologiche, relazioni con la Constituency e con le altre entità di riferimento, scelta e gestione delle terze parti)

PARTE III - Aspetti legati al contesto di applicazione

8. L'Enterprise Risk Management: il contesto di riferimento

L'attività d'impresa è caratterizzata da un indissolubile legame con il rischio. Il rischio è una caratteristica intrinseca del business aziendale e le capacità di identificazione, valutazione e gestione dei rischi sono alla base del successo aziendale. L'interesse per il tema del risk management ha assunto valore cruciale a partire dagli anni '90: gradualmente accresciutosi nell'ultimo decennio, è letteralmente esploso negli anni più recenti. Tuttavia inizialmente la visone del rischio assumeva, tanto nella prassi quanto nella letteratura, uno spessore meramente marginale nella conduzione dell'impresa dove la gestione del rischio era solitamente circoscritta a semplici azioni disgiunte volte a contenere l'incertezza derivante da specifiche attività. I limiti di un simile orientamento sono divenuti evidenti a partire dalla fine degli anni novanta, quando la maggiore incertezza che il contesto economico e i mercati finanziari hanno iniziato a manifestare ha profondamente modificato il contesto nel quale l'impresa opera. La crescente competitività, i nuovi modelli organizzativi adottati, gli impatti esercitati dalle evoluzioni tecnologiche sulle dinamiche competitive dei business, i collassi finanziari che recentemente hanno travolto alcune Grandi Imprese quotate, la crescente instabilità dei contesti economico-politico e sociali hanno aumentato il livello di instabilità, incertezza e il numero di variabili che incidono sul raggiungimento o mantenimento degli obiettivi aziendali. Mercati mobiliari, istituti di credito, agenzie di rating e investitori hanno acquisito coscienza dell'aumentata rilevanza assunta dal rischio nell'attività aziendale e iniziato a richiedere alle imprese una maggiore considerazione di tale fenomeno oltreché l'adozione di misure idonee alla sua gestione, evidenziando l'esigenza di migliorare i sistemi di controllo interni delle medesime imprese al fine di anticipare e gestire il cambiamento, e, dunque, di rafforzare e accrescere la propria capacità di creare valore per gli stakeholder. Il tradizionale approccio rischio-assicurazione viene abbandonato a favore di un processo di gestione integrato basato su soluzioni organizzative riconosciute e condivise dall'intera organizzazione. La crisi del 2008 ha inoltre contribuito a diffondere nelle imprese la consapevolezza di come anche rischi apparentemente insignificanti possano causare gravi danni, qualora non vengano gestiti adeguatamente, circostanza ancor più probabile nel caso le diverse tipologie di eventi rischiosi interagiscano tra loro. Ne deriva che un buon modello di risk management deve permettere la comprensione dei potenziali aspetti positivi e negativi di tutti i fattori che possono influenzare l'organizzazione, incrementando la

probabilità di successo della strategia e riducendo l'incertezza sul raggiungimento degli obiettivi generali dell'azienda. Il rischio, dunque, diviene un ulteriore fattore produttivo in ambito aziendale da gestire secondo i principi imprenditorialità e managerialità comuni [12]. L'evoluzione del contesto economico così come la mutata considerazione del rischio hanno portato alla creazione di innovativi modelli di gestione dello stesso nell'ambito aziendale. Ne è esempio l'Enterprise Risk Management – Integrated Framework definito e sviluppato dal Committee of Sponsoring Organisations of Treadway Commission (COSO) [14]. Tale Framework, pubblicato nel settembre del 2004, definisce l'Enterprise Risk Management (ERM) come un processo posto in essere dal consiglio di amministrazione, dal management direzionale e da altro personale aziendale; applicato nello sviluppo della strategia aziendale dell'intera organizzazione; progettato per l'identificazione e gestione di eventi che potrebbero avere un impatto, sia positivo che negativo, sull'azienda; focalizzato nel mantenere il livello di rischio aziendale all'interno della soglia accettabile di risk appetite (propensione al rischio); concepito per dare una ragionevole garanzia all'azienda in relazione al raggiungimento dei propri obiettivi aziendali. In questo modello, la gestione dei rischi si affianca alla regolare attività operativa e diventa parte integrante della struttura organizzativa aziendale. Inoltre, l'ERM adotta una visione olistica del rischio che risulta essenziale alla rilevazione delle eventuali interconnessioni presenti tra le diverse tipologie di rischio. Di fatto, solo considerando l'impresa come un'unica entità nella quale si articolano diverse aree e attività interconnesse tra loro è possibile sfruttare appieno le potenzialità della gestione del rischio aziendale. Dunque, il modello di Enterprise Risk Management (ERM) proposto dal COSO promuove il paradigma di una gestione organica e integrata di tutte le tipologie di rischio aziendale dove l'ERM si affianca a qualsiasi attività e processo aziendale per meglio valutare la rischiosità assunta dall'impresa sia nel dettaglio che a livello d'insieme. Una valutazione del profilo di rischio globale dell'impresa consente al management da una parte di verificare e analizzare la coerenza delle scelte effettuate, e dall'altra di allineare il livello di rischiosità aziendale con il livello di rischio accettabile. Una completa e dettagliata valutazione del rischio aziendale è fondamentale ed essenziale per una corretta valutazione e selezione delle strategie aziendali e dei relativi obiettivi. Dunque, la gestione integrata dei rischi assume una natura strategica, tattica e competitiva capace di influenzare positivamente l'intero processo di creazione di valore per l'impresa. Un altro approccio significativo e di nicchia, in quanto specificamente rivolto agli aspetti di cyber security delle piccole e medie imprese, è rappresentato da "A simplifie approach to Risk Management for SMEs", un'iniziativa del 2007 promossa dall'Agenzia Europea per la Sicurezza delle Reti e delle Informazioni (ENISA). Così come indicato dal titolo, l'organo dell'Unione Europea ha deciso di fornire, soprattutto al personale direzionale non esperto di questioni di sicurezza, un tool semplice attraverso il quale eseguire una autovalutazione guidata e modulare del rischio. In questo senso sono stati semplificati gli aspetti di sicurezza e suggeriti i livelli accettabili di sicurezza da raggiungere individuando, così come previsto dal Framework Nazionale, un profilo target di rischio a cui tendere[27].

8.1 L'analisi del rischio

Risk Appetite e Risk Tolerance

Nel processo di analisi del rischio, primaria rilevanza ha la definizione dell'ambiente interno e degli obiettivi strategici dell'azienda. L'ambiente interno costituisce l'identità essenziale di un'organizzazione, determina i modi in cui il rischio è considerato e affrontato dalle persone che operano in azienda, i valori etici e l'ambiente di lavoro in generale. In questo ambito risulta fondamentale la definizione della filosofia aziendale della gestione del rischio. Questa rappresenta le attitudini comuni che caratterizzano l'approccio dell'azienda al rischio, come viene considerato in tutte le attività, come viene individuato e gestito. Ne deriva l'identificazione della Risk Appetite aziendale, ovvero la propensione al rischio, che riflette il modo in cui vengono percepiti e identificati gli

eventi, quali tipi di rischi vengono accettati o meno e come verranno gestiti. La Risk Appetite individuata deve essere il risultato di un confronto tra il management e il consiglio di amministrazione, in quanto influirà sia sulle scelte strategiche, indirizzate dal board, sia su quelle operative, di attinenza dei dirigenti delle varie unità. La Risk Appetite scelta costituirà la base sulla quale vengono prese le decisioni relative alla strategia da perseguire, nonché l'allocazione delle risorse tra le diverse divisioni operative. Tuttavia, come detto in precedenza, lo scopo dell'ERM è di dare una ragionevole certezza nel raggiungimento degli obiettivi strategici prefissati. Risulta dunque necessario quantificare tale ragionevolezza. La soglia di rischio tollerabile deve essere stabilita sulla base dell'attività svolta, dell'organizzazione che l'adotta e di un vasto insieme di altre variabili. Tale soglia di confidenza determina i livelli di scostamento accettabili rispetto al raggiungimento dell'obiettivo, viene definita Risk Tolerance (tolleranza al rischio) ed è misurabile con la stessa unità di misura scelta per gli obiettivi.

La valutazione del rischio

Il processo di analisi del rischio prende le mosse dall'identificazione degli eventi di rischio che potrebbero inficiare il raggiungimento degli obiettivi aziendali. Ognuno dei rischi identificati diviene oggetto di due valutazioni: prima e dopo le azioni di mitigazione messe in essere dal management. Dalla prima valutazione si determina il rischio inerente (o intrinseco), ovvero il massimo livello di rischio possibile senza alcuna azione di mitigazione applicata. La seconda valutazione determina invece il rischio residuo, ovvero la porzione di rischio che rimane in capo all'azienda dopo aver messo in atto le attività di controllo esistenti sul rischio inerente. Per azioni di mitigazioni si intendono tutte quelle attività poste in essere per ridurre la probabilità del manifestarsi del rischio e/o l'impatto collegato. La valutazione del rischio avviene su due dimensioni:

- impatto;
- probabilità.

L'identificazione dell'impatto di un rischio consiste nel definire la tipologia di perdita potenziale e misurare la grandezza associata al verificarsi del rischio. Considerando che ciascun rischio è relativo a un determinato obiettivo e che questi sono misurabili sia qualitativamente che quantitativamente, i rischi stessi possono essere quantificati adottando le medesime metriche degli obiettivi di riferimento. Tipicamente, i criteri per la valutazione dell'impatto dei rischi sono:

- Economico: valuta l'effetto di un rischio in termini di minori ricavi o maggiori costi. Tale criterio può essere utilizzato per tutti quei rischi che hanno un effetto quantificabile sul conto economico della Società e necessita che vengano definite specifiche soglie sulla base di un parametro di riferimento (Costi, Ricavi, Margine);
- Mercato: possibile perdita di quote di mercato in seguito a rischi concernenti l'incapacità di soddisfare le esigenze dei clienti in termini di qualità del prodotto/servizio;
- Reputazionale: basato sul verificarsi di possibili eventi che potrebbero ledere l'immagine della Società;
- Vantaggio competitivo: misura l'eventuale perdita di vantaggio competitivo acquisito dalla Società a fronte del verificarsi dei rischi valutati.

La probabilità di accadimento di un rischio è la possibilità che l'evento/rischio identificato si manifesti in un dato orizzonte temporale. Questo aspetto rimane uno dei più complessi e controversi del processo di analisi del rischio. In assenza di informazioni quantitative precise, che possono provenire dall'analisi dello storico di esperienze simili pregresse o da studi e analisi specifiche dei

fenomeni d'interesse, è possibile stabilire la probabilità di accadimento sulla base della sensibilità ed esperienza del personale riguardo a funzioni di loro competenza. Sarà poi possibile determinare e costruire una matrice dei rischi, simile a quella mostrata in Figura 8.1, ovvero una rappresentazione sintetica del posizionamento relativo dei singoli rischi rispetto alla risk appetite e alla risk tolerance aziendale, consentendo alla direzione e al management di identificare le priorità di azione e le possibili strategie di risposta al rischio.

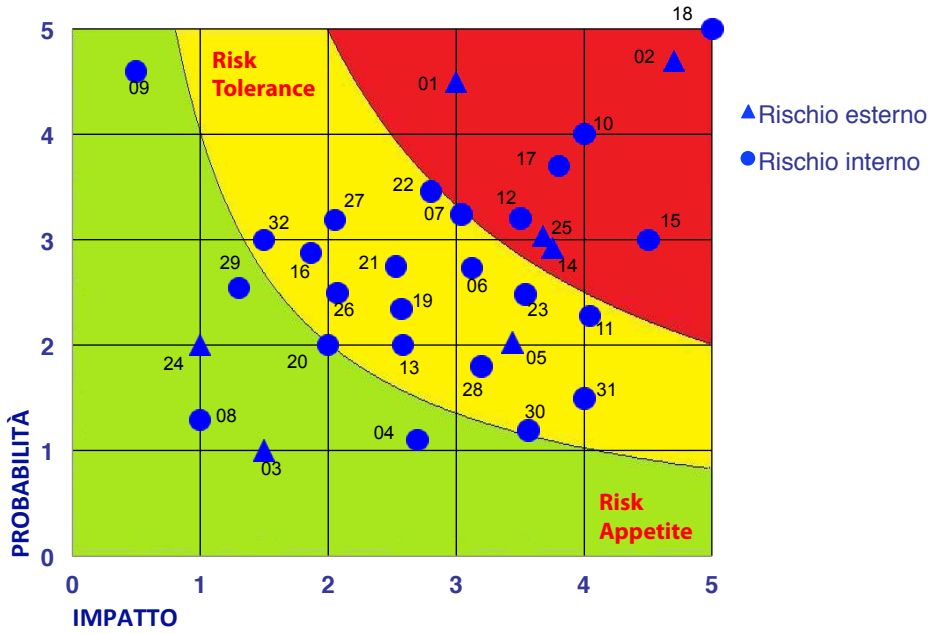

Figura 8.1: Un esempio di matrice dei rischi aziendali.

La valutazione del rischio, data dal prodotto di probabilità di accadimento e impatto, genera tre livelli di rischio:

- Rischio Basso – Non rilevante: il rischio rientra all'interno della risk appetite aziendale e di conseguenza non sono necessarie misure di controllo o strategie di mitigazione ulteriori;
- Rischio Medio – Monitorare: il rischio supera la risk appetite ma rientra nella risk tolerance. Questa tipologia di rischio solitamente viene sottoposta a costante monitoraggio/gestione da parte dell'organizzazione;
- Rischio Alto – Evitare/Ridurre: Il rischio supera i livelli sia di risk appetite che di risk tolerance. Necessita un'elevata attenzione da parte della direzione che deve quali strategie di trattamento applicare: riduzione/mitigazione del rischio, trasferimento del rischio o eliminazione della fonte di rischio.

Risposta al rischio

La direzione aziendale, dopo aver preso visione dei rischi residui, determina come allinearli con il livello di risk appetite desiderato attraverso un piano di trattamento dei rischi. Le possibili risposte al rischio rientrano nelle seguenti categorie:

- Evitare il rischio: non si è riusciti a trovare un'opzione valida che riduca l'impatto e la probabilità del rischio ad un livello accettabile di conseguenza viene eliminata la fonte di rischio;
- Ridurre il rischio: sono intraprese azioni per ridurre la probabilità o l'impatto del rischio, oppure entrambi, a un livello che è in linea con la tolleranza al rischio desiderata. In altre parole vengono implementate ulteriori azioni di mitigazione del rischio;
- Condividere/Assicurare il rischio: è ridotta la probabilità e l'impatto del rischio trasferendo oppure compartecipando una parte del rischio (e.g. acquisto di una polizza assicurativa, operazioni di copertura contro i rischi di oscillazione dei prezzi o delle valute, attività di esternalizzazione o outsourcing);
- Accettare il rischio: non sono intraprese azioni per incidere sulla probabilità e sull'impatto del rischio, in quanto il rischio è già posizionato nell'area di tolleranza.

Monitoraggio nel tempo e prevenzione del rischio: i Key Risk Indicator

Definiti i valori di impatto e probabilità e considerato che un rischio è composto da molteplici fattori in continua evoluzione, un efficace processo di ERM necessita un monitoraggio continuo di questi fattori al fine di assicurarsi che i relativi rischi vengano tenuti sotto controllo. In questo contesto è fondamentale identificare le metriche, o indicatori, più appropriate nella descrizione dei fattori concorrenti a un dato rischio e definire come questi influiscono sui valori di impatto e probabilità. In questo caso, questi indicatori sono generalmente definiti Key Risk Indicator (indicatori chiave di rischio). L'identificazione e l'utilizzo di accurati Key Risk Indicator (KRI) assume un ruolo fondamentale dal punto di vista strategico in quanto migliorano il processo di risk management, facilitano l'identificazione di vulnerabilità e migliorano il processo di monitoraggio dei rischi. Affinché le gli indicatori di rischio si possano considerare efficaci essi devono poter essere ripetibili e significativi a tal punto da poter costituire un database dell'andamento del rischio utile a comparare l'efficienza delle contromisure adottate e del ritorno di investimento (in termini di mancate perdite). I KRI sono statistiche o misurazioni in grado di offrire una prospettiva riguardo il posizionamento della compagnia rispetto al rischio, tendono ad essere rivisti periodicamente per assicurare la corretta ed eterogenea valutazione del rischio e segnalano alla compagnia quei cambiamenti che possono indicare l'aumentare o l'emergere di un rischio.

8.2 I vantaggi dell'applicazione di un processo di ERM

L'inadeguatezza delle tradizionali forme di gestione del rischio è stata compresa anche dalle autorità regolamentari che, nell'ultima decade, hanno gradualmente implementato vincoli sempre più stringenti in materia di gestione e consapevolezza del rischio aziendale. La stessa concezione del rischio ha subito una significativa modifica: dapprima fenomeno unicamente ricondotto a situazioni negative, viene oggi considerato un artefice del successo dell'azienda, qualora questa riesca ad estrarne il valore intrinseco. Il rischio non è, dunque, unicamente un onere da sopportare, bensì, se ben gestito, può diventare un fattore critico di successo e dare un vantaggio competitivo in grado di garantire lo sviluppo e la protezione dell'attività aziendale. L'implementazione di un sistema aziendale di ERM possiede inoltre una serie di vantaggi indiretti non trascurabili. Considerato infatti che l'equilibrio tra rischi assunti e consistenza del capitale aziendale è un requisito essenziale alla continuità operativa e che la dotazione di capitale proprio e del livello di indebitamento influisce direttamente su tale equilibrio, una migliore gestione dei rischi aziendali consente di ridurre la possibilità di incorrere in situazioni di dissesto finanziario influendo positivamente sul valore dell'impresa. Inoltre, gli istituti di credito valutano positivamente la presenza di un sistema di ERM

nel contesto aziendale in quanto questo offre una ragionevole sicurezza che l'azienda manterrà inalterato il proprio livello di assetto economico. Tale apprezzamento da parte dei finanziatori può ridurre notevolmente il costo di reperimento di capitale da parte dell'azienda e dunque influire positivamente sul conto economico della stessa. Nel contesto economico attuale, la definizione e implementazione di un sistema aziendale di gestione del rischio diviene un elemento propulsivo del miglioramento e della crescita aziendale nonché un fattore determinante di competitività.

9. Le polizze cyber risk

Come precedentemente anticipato, il tema del cyber risk rappresenta oggi un punto critico nel processo di analisi e mitigazione dei rischi cui un'azienda può andare incontro nella conduzione della propria attività. Infatti, la diffusione di tecnologie e modelli di business sempre più basati sulla rete, sullo scambio/possesso di informazioni sensibili e sulla condivisione di spazi virtuali (social media, cloud computing, ...) racchiude certamente nuove possibilità, ma deve comportare anche una maggiore attenzione da parte delle imprese sui pericoli che derivano da questi cambiamenti.

Dai cyber risk possono derivare infatti danni economici di grande entità, dovuti principalmente a:

- Furto/corruzione di dati sensibili e/o di terzi;
- Danni patrimoniali derivanti da interruzione dell'attività (es. blocco dell'operatività e/o transazioni on line);
- Danni patrimoniali derivanti da frodi finanziarie;
- Danni materiali agli asset dell'impresa;
- Danni materiali ai clienti (con particolare riferimento all'ambito sanitario);
- Danni di immagine.

La necessità di un processo integrato di risk management e il ruolo dell'assicurazione.
Per far fronte a queste minacce, le Aziende devono strutturare un processo integrato di Risk Management che includa l'ambito Cyber. Tale approccio garantisce infatti il più efficace metodo per prevenire/mitigare l'impatto di un rischio informatico, grazie allo sviluppo di una adeguata consapevolezza unitamente all'ottimizzazione del processo di trasferimento del rischio al mercato assicurativo. La copertura assicurativa di tali rischi è infatti l'ultimo tassello di un processo strutturato, che parte con l'analisi della realtà specifica dell'azienda: dal tipo di business che conduce, al tipo di attività che implementa, fino alle caratteristiche dell'infrastruttura IT. A titolo esemplificativo si riportano alcuni aspetti critici di cui occorre tenere considerazione:

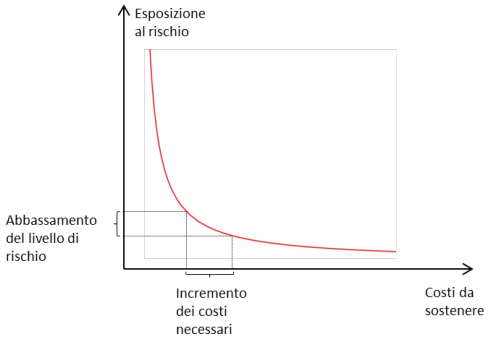

Figura 9.1: Ogni nuovo abbassamento dell'esposizione al rischio cyber richiede costi crescenti.

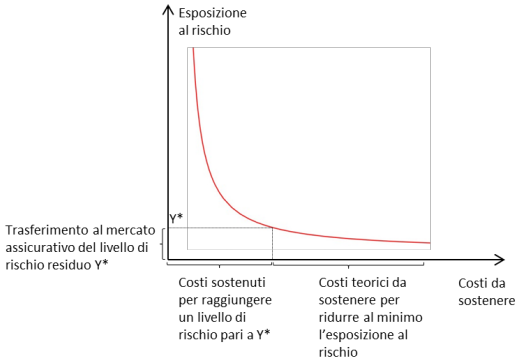

Figura 9.2: La società stabilisce una soglia oltre la quale trasferire al mercato assicurativo il rischio residuo.

- Il mercato di riferimento;
- Il contesto geografico nel quale si opera;
- Le peculiarità dell'infrastruttura IT (localizzazione sale server, valore risorse IT, reti intra/extra net,...);
- Il tipo di dati/informazioni trattate;
- I servizi e i canali on line based;
- Le possibilità di accesso (fisico/virtuale), anche da remoto, ai sistemi/reti aziendali;
- Le policy di cyber security e le misure di prevenzione/protezione poste in atto.

Occorre infatti ricordare che la Cyber Insurance deve operare quale strumento a tutela del bilancio aziendale, intervenendo a copertura dei cosiddetti "rischi catastrofali", anche in funzione del risk appetite e risk tolerance dell'Impresa. Occorre inoltre considerare che i benefici incrementali derivanti da ulteriori azioni di prevenzione/protezione si riducono progressivamente al di là di una certa soglia, per cui il costo da sostenere per accrescere ulteriormente i livelli di sicurezza diverrebbe insostenibile se comparato ai benefici connessi. La società dovrà pertanto stabilire oltre quale soglia sia maggiormente conveniente un trasferimento al mercato assicurativo del rischio residuo e, nel contempo, valutare il trade-off ottimale tra il prezzo della copertura assicurativa e il livello di esposizione residua al rischio (si vedano Figure 9.1 e 9.2).

Il mercato degli assicuratori e metodologie di indennizzo.
Il mercato assicurativo delle polizze cyber risks oggi è in rapida evoluzione e offre la possibilità di creare tutele ad hoc per il cliente. Tale personalizzazione offre un ottimo livello di aderenza al rischio cyber reale cui è esposta l'azienda, ma presuppone ovviamente un precedente processo di analisi e valutazione, così come descritto precedentemente. Tuttavia va tenuto presente che, ancorché in rapida evoluzione, il mercato assicurativo italiano si trova ancora in una fase embrionale. Ciò perché, come sempre in questo tipo di mercato, la risposta a un rischio si attua nel momento in cui tale rischio diviene conosciuto e valutabile. La situazione di novità riguarda però il solo mercato italiano in quanto, nei paesi dell'America settentrionale e anglosassoni, le problematiche afferenti i rischi cibernetici vengono affrontate da circa una decina d'anni. Da ciò però deriva il fatto che l'impianto contrattuale della maggior parte delle coperture ricalchi l'approccio risarcitorio per la violazione dei dati sulla privacy, tanto caro al mondo anglofono. Delle 50 compagnie di assicurazioni operanti in Europa che specificamente si dichiarano pronte a sottoscrivere rischi cibernetici, soltanto un terzo opera direttamente in Italia, la restante parte opera fondamentalmente dal Regno Unito (a copertura di rischi italiani).

Il mercato degli assicuratori presenta due approcci:

1. First Party Damages: ovvero i danni sofferti dall'azienda colpita da un evento cibernetico;
2. Third Party Damages: ossia la responsabilità dell'azienda assicurata per la violazione dei dati di terzi di cui l'azienda assicurata sia in possesso.

Questi due approcci danno origine a due metodologie di indennizzo differenti. Nel primo caso, infatti, l'assicuratore indennizzerà le spese per fronteggiare la crisi di emergenza, intese quindi come le spese di società informatiche specializzate nella messa in sicurezza informatica, nel ripristino dei dati persi, criptati o distrutti, i costi legali per far fronte ad una indagine dell'autorità preposta al controllo, la perdita di profitto legata al blocco dell'attività della società assicurata e inoltre, eventualmente, la frode informatica patita dall'azienda e i danni cagionati a terzi.

Il secondo approccio invece sarà speculare e indennizzerà fondamentalmente la richiesta danni avanzata da terzi per violazione dei dati di terzi, in possesso della società, con l'aggiunta però delle spese addizionali per il recupero dei dati, dei danni all'immagine della società assicurata, e delle spese legali per fronteggiare una richiesta di risarcimento od una indagine, nel caso in cui vi sia effettivamente una perdita di flusso di dati di terzi verso l'esterno. In questo caso però non verrà indennizzata, salva la specifica pattuizione la riduzione di profitto patita dall'azienda assicurata.

La differenza tra i due approcci risarcitori trova riscontro in due momenti diversi di attivazione della copertura; nel caso della metodologia first party, l'elemento che fa scattare la copertura è la scoperta del danno all'azienda assicurata, sia esso danno materiale, immateriale o patrimoniale. Nel secondo caso invece, ciò che fa scattare la copertura è la richiesta di risarcimento danni avanzata da terzi in conseguenza della violazione di dati di terzi detenuti dall'assicurato, o di cui l'assicurato sia responsabile.

9.1 Percezione del rischio e diffusione delle polizze cyber

Il rapporto Ponemon 2015 sul rischio cibernetico ha evidenziato come, benché il livello di consapevolezza sui danni materiali ai beni e sui danni immateriali ai beni non tangibili (dati) sia identico, il trasferimento al mercato assicurativo sia estremamente sperequato. L'indagine rivela che il valore percepito sia di beni tangibili sia di beni intangibili è relativamente simile con una differenza di un mero 3%. In media, il valore totale dei beni tangibili riportato nello studio ammonta a 872 milioni di USD, confrontato con gli 845 milioni di USD per quanto attiene i beni immateriali. Quando è stato chiesto di stimare il valore medio di perdita o distruzione di tutti i beni immateriali (o la massima perdita probabile, PML) anche la stima è stata simile (638 milioni di dollari per i

beni immateriali, contro 615 milioni di dollari per i beni materiali). Al contrario, sia l'impatto dell'interruzione di attività legata ai beni immateriali, sia la probabilità di una violazione di dati o di beni immateriali sono viste come significativamente maggiori rispetto alle medesime situazioni occorse sui beni materiali. L'impatto stimato di una business interruption legata ai beni immateriali è pari a 168 milioni di dollari, maggiore del 63% rispetto ai 103 milioni di dollari previsti in caso di beni materiali; mentre la probabilità di fronteggiare una perdita è pari al 4.7%, rispetto al 1.5% per i beni materiali (per i danni che totalizzino non più del 50% del PML nell'arco dei prossimi 12 mesi).

Nonostante questa crescente consapevolezza sul cyber risk, esiste un vasto gap assicurativo. Se confrontiamo beni materiali e beni immateriali, i Business Leaders EMEA indicano che i beni immateriali sono più esposti del 38% rispetto ai beni materiali circa la protezione assicurativa. Circa la metà delle perdite potenziali (49%) sui beni materiali è coperta dall'assicurazione, mentre tale percentuale si attesta solo all'11% per quanto concerne i beni immateriali. Al contrario, per ciò che concerne i beni immateriali è più diffusa l'autoassicurazione – intesa come la ritenzione del rischio all'interno del Bilancio d'esercizio rispetto all'acquisto di polizze assicurative. In generale si osserva come un danno ai dati sia considerato più pericoloso in termini reputazionali rispetto a un danno materiale ai beni. Questo implica che, in assenza di un obbligo legale di notifica, le aziende siano meno propense a dichiarare di avere subito delle perdite di dati rispetto alla propensione a dichiarare di avere subito un danno a beni materiali. Parlando di obbligatorietà dal punto di vista legale, a oggi soltanto tre tipologie di aziende sono obbligate a notificare le violazioni dei dati: società di telecomunicazioni e internet providers, banche, aziende sanitarie. Inoltre secondo quanto prescritto dal Provvedimento del 2 luglio 2015, le amministrazioni pubbliche sono tenute a comunicare al Garante le violazioni dei dati personali (data breach) che si verificano Per ciò che riguarda le società di telecomunicazioni, il Garante per la Protezione dei Dati Personali ha predisposto anche una procedura per la notifica al Garante e a clienti della violazione dei dati. Per quanto concerne le altre due categorie a oggi non esiste una procedura normalizzata di notifica ai clienti per ciò che riguarda le banche, mentre non esiste un obbligo di notifica ai pazienti, ma solo al Garante, per quanto riguarda le aziende sanitarie.

Capacità del mercato assicurativo e la necessità di un assessment del rischio

Dobbiamo aggiungere che, mentre la capacità teorica del mercato per ogni singola azienda si attesta su circa 200.000.000 di euro, quando si vuole circoscrivere la copertura alle fattispecie first party, il limite si riduce drasticamente in un intervallo compreso tra 25 e 80 milioni di euro. Questo limite indiscutibilmente favorisce la selezione del rischio da parte dell'assicuratore. Inoltre, la già segnalata carenza normativa fa sì che non esista uno standard a cui gli assicuratori debbano comunque fare fronte, cosicché il fenomeno di anti-selezione del rischio viene esasperato. La capacità complessiva, apparentemente limitata può, sembrare un limite per le Aziende, e in particolar modo per quelle di maggiori dimensioni. In realtà tutti gli assicuratori stanno tentando di sviluppare coperture per la protezione dai rischi cibernetici. Proprio il fatto che gli operatori assicurativi stiano ancora valutando la portata di questo comparto, può rappresentare un'opportunità per le Aziende che vogliano tutelarsi. Quasi tutte le Compagnie si stanno strutturando per poter offrire, nell'ambito delle garanzie accessorie al programma assicurativo, anche coperture per la proprietà intellettuale (violazione di marchi ecc.) e per i danni reputazionali, pur in presenza di sottolimiti del massimale principale di polizza e soltanto in conseguenza di una violazione informatica esterna, oppure interna, ma fraudolenta. Fatti quindi i necessari distinguo tra i vari settori di operatività e quindi tra i principali fattori di rischio, è importante - ai fini della progettazione di una copertura assicurativa - effettuare un processo di assessment che sia in grado di valutare e apprezzare i rischi maggiormente significativi in termini finanziari. Il beneficio finale che le aziende possono trarre da questo tipo di copertura - progettata alla luce di una valutazione accurata del rischio - risiede fondamentalmente nella tutela finanziaria del bilancio d'Impresa, a fronte di un rischio residuo non

ulteriormente contenibile, se non a fronte di investimenti eccessivamente significativi, come sopra illustrato.

9.2 Guida all'implementazione di una copertura assicurativa cyber risk

Ai fini dell'implementazione di una copertura assicurativa cyber risk, sarebbe opportuno che l'azienda seguisse i 4 passaggi:

1. Coinvolgimento di un Consulente Assicurativo: Come anticipato, il settore dei rischi cyber non è ancora maturo né ha standard di riferimento (in ambito assicurativo). La peculiarità del rischio e l'immaturità del settore rendono indispensabile la conoscenza del mercato e delle leve tecnico-commerciali degli operatori del settore assicurativo. Il coinvolgimento di uno o più consulenti specializzati nel trasferimento dei rischi al mercato assicurativo diventa fondamentale per il trasferimento delle specifiche necessarie agli assicuratori. Interpellare direttamente le compagnie assicurative potrebbe portare le stesse a fornire prodotti non rispondenti alle esigenze dell'assicurando;

2. Risk Assessment: Ai fini di isolare correttamente il massimo danno probabile e di stimare correttamente l'esposizione al rischio, sarebbe opportuno, prima di stipulare la Polizza, effettuare un'analisi e quantificazione del rischio stesso. Molto spesso le Aziende – anche di medio grandi dimensioni – faticano a quantificare la propria esposizione, soprattutto lato danni indiretti, in quanto di difficile valutazione l'impatto economico che un evento informatico avverso può causare. Anche in questo caso, il supporto di un consulente riconosciuto anche presso il mercato assicurativo diviene molto importante. L'assessment del rischio dovrà inoltre consentire di reperire le informazioni utili alla compilazione di un questionario assicurativo. Un Risk Assessment strutturato è fortemente consigliato per le Grandi Imprese e Infrastrutture Critiche, oltre che per tutte le PMI che risultano molto dipendenti dai Sistemi o che operano in ambiti definiti (es commercio on-line, retail, sanità, media-editoria, broker, società di servizi IT, ecc.);

3. Compilazione del questionario assicurativo: il questionario in ambito assicurativo ha lo scopo di raccogliere le informazioni base necessarie per una prima valutazione del rischio da parte degli assicuratori. La compilazione del questionario ha come risultato il fatto che possano essere apprezzate le varie ipotesi di limite di indennizzo che stanno alla base del contratto assicurativo e, parallelamente, fa prendere coscienza all'assicurando di quelli che sono i suoi punti di forza e di debolezza. Va detto per inciso che il questionario raccoglie informazioni di tipo standardizzato (esistenza di certificazioni, esistenza di protezioni standard, soggetti che hanno accesso ai sistemi aziendali, contrattualistica tra assicurando e terzi soggetti) e pertanto il livello di approfondimento non è elevato. Tuttavia la compilazione del questionario ha il pregio per l'assicurato di permettere all'assicuratore di fornire un intervallo di premio che potrà poi essere raffinato con il prosieguo della trattativa; per quanto riguarda l'assicuratore, il questionario (anche in assenza di assessment) dà certezza di alcuni dati fondamentali, essendo tra l'altro sottoscritto dall'azienda che richiede la copertura assicurativa;

4. Implementazione della Copertura Assicurativa: Una volta esaurito il processo di valutazione tramite questionario e/o tramite risk Assessment strutturato, sarà possibile richiedere una quotazione formale al mercato assicurativo. Anche in questo caso l'apporto negoziale di un Consulente specializzato è perlomeno consigliabile, in quanto la conoscenza del settore e la capacità negoziale di chi opera continuativamente nel settore permettono risultati più performanti rispetto a quelli ottenibili dal singolo Cliente direttamente con gli assicuratori, oppure da un Consulente non specializzato con gli assicuratori.

10. Aspetti di privacy legati al Framework

Questo Capitolo presenta alcuni aspetti di privacy, relativi ai documenti classificati e al segreto di Stato, da tenere in giusta considerazione nel momento in cui si implementa o contestualizza il Framework. Si basa principalmente sulle disposizioni del Codice della Privacy e in minor misura sul Decreto del Presidente del Consiglio dei Ministri 6 novembre 2015, comprendente la "Disciplina della firma digitale dei documenti classificati" (Decreto n. 4/2015) e le "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva" (Decreto n. 5/2015). Tuttavia, tale Capitolo dovrà tenere conto, in successive revisioni del Framework, di alcune disposizioni europee in corso di approvazione: il Regolamento generale sulla protezione dei dati[1] e la Direttiva sulla protezione dei dati nel settore delle attività di contrasto[2], i quali implicheranno modifiche al Codice della Privacy e la cui entrata in vigore è prevista per la primavera del 2018, nonché la direttiva NIS (Network and Information Security), la cui entrata in vigore è prevista per la primavera del 2016[3].

10.1 Il Codice della Privacy

Il Framework Nazionale è implementato in maniera conforme al panorama normativo italiano e, in particolar modo, alle disposizioni del Codice della Privacy (in seguito "Codice"). In tal senso, la Subcategory "ID.GV-3: I requisiti legali in materia di cyber security, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti" prevede che tutta la normativa in vigore in termini di cyber security e protezione dei dati personali sia identificata e analizzata in accordo al tipo di attività svolto dall'organizzazione e al tipo di dati trattati. In linea generale, il Codice individua quali titolari del trattamento: "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e

[1] http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52012PC0011&from=EN
[2] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205833%202012%20INIT
[3] http://data.consilium.europa.eu/doc/document/ST-15229-2015-REV-2/en/pdf

agli strumenti utilizzati, ivi compreso il profilo della sicurezza" (art. 4). Tali soggetti hanno degli obblighi:

- di sicurezza (artt. 31-34);
- di comunicazione (artt. 19-22, 25-27, 32, 32-bis e 39).

Di seguito saranno descritti tali obblighi e la relazione con le Subcategory del Framework che questi implicano per i soggetti individuati.

Obblighi di sicurezza e comunicazione

Gli obblighi di sicurezza, relativi ai dati personali oggetto del trattamento, sono declinati all'articolo 31 del Codice, il quale impone che questi siano "custoditi e controllati [...] in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta". Alcuni di questi obblighi sono esplicitati nell'articolo 34 e nell'allegato tecnico di riferimento B sotto forma di misure minime di sicurezza (intese come "il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta"). Tali misure comprendono:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico (almeno annuale) dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici (strumenti elettronici da aggiornare almeno ogni 6 mesi; gli aggiornamenti dei programmi volti a prevenire la vulnerabilità dei sistemi elettronici almeno annualmente);

f) adozione di procedure per la custodia di copie di sicurezza (salvataggio dei dati almeno settimanale), il ripristino della disponibilità dei dati e dei sistemi (entro 7 giorni);

g) adozione di procedure per la gestione e l'uso di supporti rimovibili;

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Tali disposizioni fanno si che cinque Subcategory del Framework proposto siano da considerarsi obbligatorie per quelle organizzazioni che trattano dati personali mediante strumenti elettronici. Tali Subcategory sono:

- PR.DS-1: I dati e le informazioni memorizzate sono protette;
- PR.IP-9: Sono attivi e amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro;

- PR.PT-2: I supporti di memorizzazione removibili sono protetti e il loro uso è ristretto in accordo alle policy;
- PR.PT-3: L'accesso alle risorse e ai sistemi è limitato secondo il principio di minima funzionalità;
- PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato.

L'esplicitazione delle misure minime di cui sopra non riduce, a ogni modo, l'importanza degli obblighi più generali di sicurezza a cui devono attenersi i titolari del trattamento di dati personali, ai sensi dell'articolo 31 del Codice. Questi ultimi sono, infatti, responsabili in sede giudiziaria (a norma dell'articolo 2050 del Codice Civile, in materia di responsabilità per l'esercizio di attività pericolose) di eventuali danni causati da violazioni del predetto articolo 31 e per sottrarsi alla pena del risarcimento, sono tenuti a dimostrare il rispetto degli obblighi di sicurezza, in virtù del principio dell'inversione dell'onere della prova.
Gli obblighi di comunicazione variano a seconda del titolare del trattamento e della tipologia del dato personale oggetto del trattamento stesso. Nello specifico:

- per soggetti pubblici (esclusi gli enti pubblici economici) e per dati non sensibili e giudiziari (artt. 19 e 39):
  - la comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa in qualunque forma quando è comunque necessaria per lo svolgimento di funzioni istituzionali, previa comunicazione al Garante. Il conseguente trattamento dei dati può iniziare se è decorso il termine di 45 giorni dall'invio della comunicazione al Garante (salvo sua diversa determinazione anche successiva);
  - la comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.
- per soggetti pubblici (esclusi gli enti pubblici economici) e per dati sensibili e giudiziari (artt. 20-22):
  - il trattamento dei dati sensibili e giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante;
  - i dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità;
  - i dati idonei a rivelare lo stato di salute non possono essere diffusi. In ogni caso, la diffusione dei dati sensibili e giudiziari è ammessa solo se prevista da espressa disposizione di legge.
- per privati ed enti pubblici economici (artt. 25-27):
  - è fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati;

  - i dati sensibili possono essere oggetto di trattamento con o senza il consenso scritto dell'interessato e previa autorizzazione del Garante. I dati idonei a rivelare lo stato di salute non possono essere diffusi;
  - il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

- per fornitori di servizi di comunicazione elettronica, a seguito di una violazione subita (art. 32-bis):

  - in caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza indebiti ritardi la violazione al Garante. Quando la violazione di dati personali rischia di arrecare pregiudizio ai dati personali o alla riservatezza del contraente o di altra persona, il fornitore comunica anche agli stessi senza ritardo l'avvenuta violazione;
  - la comunicazione non é dovuta se il fornitore ha dimostrato al Garante di aver utilizzato misure tecnologiche di protezione che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate ai dati oggetto della violazione.

Ciò implica che nel Framework proposto, le Subcategory relative alla comunicazione siano da considerarsi ad alta priorità per le categorie di soggetti e le tipologie di dati trattati di cui sopra, indipendentemente da quanto indicato nella contestualizzazione che tali soggetti hanno preso come riferimento. Le pratiche in oggetto sono:

- DE.DP-4: L'informazione relativa agli eventi rilevati è comunicata a tutte le parti interessate;
- RC.CO-1: A seguito di un incidente vengono gestite le pubbliche relazioni;
- RS.CO-2: Sono stabiliti dei criteri per documentare gli incidenti/eventi;
- RS.CO-3: Le informazioni sono condivise in maniera coerente con il piano di risposta;
- RS.CO-4: Il coordinamento con le parti interessate dell'organizzazione avviene in coerenza con i piani di risposta;
- RS.CO-5: È attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness).

Il monitoraggio dell'attività del personale

Prima della riforma introdotta dal "Jobs Act", l'articolo 4, comma 1 dello Statuto dei lavoratori sanciva il divieto di utilizzo di "impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori". Il decreto legislativo di riforma n. 151/2015 ha modificato tale disposizione, in linea con le pronunce del Garante in merito, sancendo che "gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali". Tali disposizioni vanno tenute in debito conto nell'implementazione della Subcategory

- DE.CM-3: Viene svolto il monitoraggio del personale per rilevare potenziali eventi di cyber security.

10.2 Informazioni classificate e segreto di Stato

Il Decreto del Presidente del Consiglio dei Ministri 6 novembre 2015, comprendente la "Disciplina della firma digitale dei documenti classificati" (Decreto n. 4/2015) e le "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva" (Decreto n. 5/2015), introduce nuovi elementi per la tutela di tali documenti, alla luce dei rischi cibernetici e in relazione alle necessità di protezione dei dati personali. Ne consegue che le disposizioni contenute in questi atti vadano tenute in debito conto, da parte di tutti i soggetti pubblici e privati che gestiscono in via informatizzata questioni coperte da segreto di Stato e informazioni classificate, nell'implementazione delle seguenti Subcategory:

- ID.GV-1: È identificata e resa nota una policy di sicurezza delle informazioni;
- ID.GV-3: I requisiti legali in materia di cyber security, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti;
- PR.AC-1: Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate;
- PR.AC-3: L'accesso remoto alle risorse è amministrato;
- PR.DS-1: I dati e le informazioni memorizzate sono protette.

11. Regolatori di settore

In questo Capitolo discutiamo il posizionamento rispetto al Framework di alcuni settori regolati, ovvero Pubblica Amministrazione, settore bancario e aziende quotate borsa e come questi settori potrebbero usare il Framework a loro vantaggio. Le sezioni che proponiamo sono esempi: ogni settore regolato ha la propria specificità regolamentare, più o meno matura nel settore cyber, e quindi dovrà posizionarsi e utilizzare il Framework nel modo che riterrà più appropriato.

11.1 Pubbliche Amministrazioni

Le pubbliche amministrazioni possono essere riguardate come organizzazioni fortemente regolate, stante il fatto che la loro attività si svolge nell'ambito e nei limiti di norme che hanno valore di legge; tuttavia il corpus normativo ha fino a oggi dedicato poco spazio alla cyber security. Le norme più importanti al riguardo sono quelle contenute nel Codice dell'Amministrazione Digitale (CAD - DLgs. 7 marzo 2005 s.m.i.), che all'art. 17, comma 1, evidenzia la necessità di concentrare in un unico ufficio il coordinamento strategico dello sviluppo dei sistemi informatici di telecomunicazione e fonia (lettera a) e l'indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture (lettera C). Nei successivi articoli 50, 50 bis e 51 vengono affrontati i problemi dell'integrità e disponibilità dei dati, attribuendo all'AgID un ruolo di primo piano nell'emanazione delle regole tecniche nel campo della sicurezza informatica, nonché nella prevenzione e gestione degli incidenti di sicurezza informatici. Tale ruolo è rafforzato dal Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico, che tra i compiti dell'Agenzia cita esplicitamente:

- detta indirizzi, regole tecniche e linee guida in materia di sicurezza informatica;
- assicura la qualità tecnica e la sicurezza dei sistemi informativi pubblici e della loro rete di interconnessione per salvaguardare il patrimonio informativo della PA e garantire integrità, disponibilità e riservatezza dei servizi erogati ai cittadini;
- opera il CERT-PA, CERT della Pubblica Amministrazione, che garantisce la sicurezza cibernetica dei sistemi informativi della P.A., oltre che della loro rete di interconnessione,

provvedendo al coordinamento delle strutture di gestione della sicurezza ICT – ULS, SOC e CERT, operanti negli ambiti di competenza.

È perciò compito dell'Agenzia contestualizzare il Framework in modo da specializzarlo per le PP.AA. italiane, tenendo presente che queste hanno caratteristiche, struttura e obiettivi sostanzialmente diversi da quelli di un'azienda, nella quale il danno, e di conseguenza il rischio, può essere più facilmente quantificato. Spesso il loro status e la natura dei servizi offerti ai cittadini le accomuna alle Infrastrutture Critiche, se non altro, per la dipendenza dei servizi offerti dai privati da quelli autoritativi pubblici. In ogni caso, il Framework rappresenta un'opportunità di estrema utilità anche per le pubbliche amministrazioni, le quali possono utilizzarlo a fini diversi:

- Awareness: incrementare la propria awareness in termini di cyber security, autovalutandosi attraverso la creazione del proprio profilo. Il Framework infatti permette, indipendentemente dalla tipologia o dimensione dell'organizzazione, di evidenziare quelle pratiche di sicurezza che risultano a priorità alta e che attualmente non vengono considerate in maniera immediata. Questo contribuirebbe a colmare parte delle lacune che le PA hanno dimostrato di avere (vedi Cyber Security Report 2013[5] e 2014[6]) e consentirebbe di individuare le azione a alto impatto sulla gestione del rischio cyber della PA;

- Profilo target: a seconda di diversi fattori, la definizione del processo per incrementare la propria cyber security difficilmente è un problema di facile soluzione. Identificare quelle pratiche da svolgere che porterebbero alla condizione voluta, senza una guida, potrebbe portare a un dispendio di energia e risorse economiche. La definizione di un profilo target, il quale individui tutte le pratiche di sicurezza che la PA vorrebbe raggiungere, comparato con il profilo corrente, rappresenta uno strumento utile per la definizione di una roadmap che porti verso la messa in sicurezza della PA;

- Supply chain: incrementare la sicurezza dell'intera catena di approvvigionamento dei servizi per pubbliche amministrazioni. Le PP.AA. potrebbero richiedere ai propri fornitori di servizi di avere un particolare profilo minimo: una serie di pratiche di sicurezza necessarie per trattare dati particolarmente critici, oppure per poter interagire con i sistemi della PA e così via. La PA potrebbe definire profili specifici per i singoli servizi e allegare tali profili ai bandi per la selezione dei fornitori.

Il Framework viene a inserirsi nel percorso intrapreso dall'Agenzia per adeguare il livello di organizzazione, consapevolezza e robustezza delle PP.AA. nei confronti del rischio cyber. Le "Regole tecniche in materia di sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni", da essa redatte e in corso di emanazione, danno corpo e consistenza alle prescrizioni del CAD, ponendo in capo alle PP.AA. l'obbligo di implementare un adeguato Sistema di Gestione della Sicurezza delle Informazioni (SGSI, equivalente italiano di ISMS), basato su una precisa attribuzione di ruoli e responsabilità. Se il focus delle Regole Tecniche è principalmente organizzativo, operativamente la loro implementazione è fondata sulle Linee Guida per la Sicurezza ICT nelle PP.AA. In tale ambito è già stato reso disponibile un sistema di controlli di sicurezza, derivato dal SANS 20, nel quale questi sono qualificati per priorità, impatto e costo. Viene così individuato l'insieme minimo da implementare necessariamente, che può essere equiparato a quello a "Priorità alta" del § 5.1 e rappresenta le misure minime di sicurezza per tutte le amministrazioni. L'adozione di ulteriori controlli viene in tale sede presentata come strumento atto a perseguire livelli di sicurezza più elevati, ma corrisponde, nell'ottica del Framework, a livelli di maturità crescenti. All'adozione del Framework dovrà seguire un allineamento terminologico, con l'unificazione del sistema di identificazione dei controlli e una maggiore articolazione della guida all'applicazione, che tenga conto delle caratteristiche dimensionali dell'amministrazione, della sua complessità

organizzativa, della tipologia di dati trattati, anche in considerazione della normativa sulla privacy, senza trascurare, infine, il livello di esposizione al rischio cyber, che dipende anche da fattori ambientali e politici.

11.2 Settore bancario e finanziario

I principali istituti bancari italiani e intermediari finanziari hanno nel corso degli ultimi anni definito e avviato programmi di cyber security per la predisposizione di misure di governo, gestione e controllo della sicurezza con l'obiettivo di prevenire, contenere e reagire alle minacce di sicurezza IT cui sono esposti gli asset informativi aziendali. Tra i diversi fattori che determinato una situazione complessiva di più elevata maturità nell'approccio al rischio cyber si citano:

- Il cambiamento sostanziale che si è registrato nelle modalità di proposizione ed erogazione dei servizi bancari. L'adozione di un approccio multicanale per l'interazione con la clientela, attuale o potenziale, oltre alla crescente digitalizzazione dei processi operativi, ha imposto l'implementazione di controlli di sicurezza informatica e di protezione dei dati e delle operazioni trattate dagli intermediari finanziari e creditizi, unitamente alla protezione della privacy;
- Una sviluppata cultura e sensibilità sul tema rischio all'interno degli istituti. Questi, difatti, hanno predisposto da tempo approcci, sistemi e strumenti volti alla valutazione di tutti i rischi, tra i quali anche quelli operativi e reputazionali, che hanno facilitato l'introduzione di sistemi per la gestione del rischio cyber;
- L'obbligo di rispettare regolamenti e provvedimenti specifici per il settore emanati a livello nazionale e internazionale in materia di sicurezza delle informazioni, sistemi informativi e continuità operativa. I programmi di compliance avviati dagli istituti, infatti, oltre a includere l'implementazione delle misure richieste, hanno costituito occasione, in generale, per una complessiva revisione delle proprie strutture di governo e gestione dell'IT e per l'attuazione di migliori prassi su pratiche e controlli di sicurezza nei processi aziendali;
- La resilienza dei servizi finanziari è un aspetto strategico che incide direttamente sul core business delle banche, che hanno sempre dedicato grande attenzione alla continuità operativa e alla sicurezza ICT.

Iniziative nazionali

Un ruolo centrale è stato ricoperto dalla Banca d'Italia, responsabile dell'emanazione di regolamenti trasversali applicabili a tutto il comparto finanziario. È recente, difatti, l'entrata in vigore di disposizioni di vigilanza prudenziale con rilevanza sulla gestione del rischio informatico, sul governo della sicurezza informatica e sulla continuità operativa per le banche (cfr Circ. 285 del 17 dicembre 2013, 11° agg., Tit. IV). Nello specifico è stato introdotto un nuovo capitolo dedicato al Sistema Informativo (Cap. 4), mentre sono stati aggiornati i capitoli che disciplinano i controlli interni e le misure a presidio della continuità operativa (rispettivamente Cap. 3 e 5).

L'aspetto di particolare novità è stata proprio la rilevanza attribuita alla valutazione del rischio informatico, integrato nel processo di gestione complessiva dei rischi aziendali (RAF Risk Assessment Framework), per consentire agli organi con funzione di supervisione e gestione di beneficiare di una visione complessiva del profilo di rischio aziendale. La normativa è entrata in vigore a febbraio 2015 per consentire agli intermediari di adeguare i sistemi informativi alla prescrizione regolamentare. A tal fine, nel luglio del 2013 l'emanazione della circolare è stata accompagnata dalla richiesta alle aziende di effettuare una autovalutazione per identificare eventuali carenze (gap Analysis) e definire un piano di interventi per il raggiungimento della piena conformità alla

regolamentazione nei 18 mesi successivi. La stessa Circolare induce gli intermediari a considerare, tra l'altro: "la policy di sicurezza informatica; le misure adottate per assicurare la sicurezza dei dati e il controllo degli accessi, incluse quelle dedicate alla sicurezza dei servizi telematici per la clientela; la gestione dei cambiamenti e degli incidenti di sicurezza; la disponibilità delle informazioni e dei servizi ICT". Inoltre, a partire da febbraio 2015 gli intermediari sono anche tenuti a segnalare tempestivamente gli incidenti di sicurezza rilevanti alla Banca d'Italia. La Banca d'Italia nel 2003 ha istituito il CODISE, struttura deputata al coordinamento delle crisi operative della piazza finanziaria italiana. Esso è presieduto dalla Banca d'Italia e vi partecipano la CONSOB e gli operatori del settore finanziario rilevanti sul piano sistemico. Il CODISE, che opera in raccordo con le analoghe strutture a livello internazionale, organizza e partecipa a test e simulazioni nazionali ed europee. Quale sede di confronto periodico fra i partecipanti favorisce l'analisi dell'evoluzione delle minacce alla continuità operativa del sistema e lo studio dei metodi di prevenzione e di controllo dei rischi, inclusa la cyber security.

Iniziative europee

Nel corso del 2015, la Banca Centrale Europea (ECB - European Central Bank, che nel novembre del 2014 ha assunto la responsabilità della supervisione diretta sugli intermediari bancari più significativi dell'Unione Europea) ha avviato un programma per la verifica della cyber security presso gli istituti europei vigilati, compresi quelli italiani[1]. Sono inoltre in corso di recepimento nella normativa nazionale gli "Orientamenti in materia di sicurezza dei pagamenti via internet" adottati dall'Autorità Bancaria Europea (ABE) il 18 dicembre 2014, che dettagliano le misure di sicurezza richieste a tutti i Prestatori di servizi di pagamento, con specifico riguardo ai servizi elettronici di pagamento offerti attraverso internet.

Iniziative globali

Il Committee on Payments and Market Infrastructures (CPMI) e la International Organisation of Securities Commissions (IOSCO) hanno posto in consultazione pubblica una guida [2] per migliorare la resilienza delle Financial Market Infrastructures (FMI)[2] a fronte di minacce cyber. La guida, indirizzata alle FMI e ai loro overseer:

- non impone requisiti aggiuntivi rispetto ai Principles for financial market infrastructures (PFMI) del 2012 ed è redatta per supportare alcuni obiettivi critici per la stabilità finanziaria, in particolare la rapida ripartenza delle FMI;
- definisce principi e non regole, anche per evitare la rapida obsolescenza delle raccomandazioni in essa contenute e non impone rigidità riguardo alla attuazione dei principi stessi;
- sottolinea l'importanza di robusti controlli ICT, ma non entra nel loro dettaglio per lasciare flessibilità agli operatori, anche in considerazione dei numerosi standard presenti sul mercato;
- ha un linguaggio leggibile e comprensibile per il vertice delle FMI, in considerazione del ruolo fondamentale che il vertice aziendale ha nel rafforzare la resilienza cyber;
- è suddivisa in capitoli che individuano cinque categorie fondamentali per la gestione dei rischi (1.Governance; 2.Identification; 3.Protection; 4.Detection; 5 Response and Recovery) e tre componenti trasversali (1.Testing; 2.Situational Awareness; 3.Learning and Evolving);

[1] La Banca d'Italia ha esteso tale esercizio a 12 banche italiane di media grandezza ("High priority banks").

[2] Le FMI sono i sistemi di pagamento a rilevanza sistemica, i sistemi per il regolamento titoli, le controparti centrali, i depositari centrali, i trade repositories. Per una definizione più estesa si veda `http://www.bis.org/cpmi/publ/d101a.pdf`

- definisce il concetto di "cyber governance" e lo pone al centro degli sforzi per migliorare la resilienza cyber delle FMI. I meccanismi di cyber governance devono assicurare che i rischi cyber siano adeguatamente considerati a tutti i livelli all'interno della FMI e che le risorse e le competenze appropriate siano impiegate per gestire tali rischi. La guida incoraggia il coinvolgimento dei vertici aziendali per creare una cultura aziendale in cui il personale, a tutti i livelli, sia consapevole del proprio ruolo e responsabilità in materia di resilienza cyber;

- punta l'accento sul fatto che una efficace mitigazione dei rischi cyber richiede una identificazione e prioritizzazione dei processi critici, nonché una comprensione delle minacce, non generica ma specifica per la singola FMI. La guida incoraggia le FMI a possedere una chiara e corretta percezione – in tempo reale – di quanto è accaduto, di quanto sta accadendo e di quanto potrà accadere nell'immediato futuro (situational awareness), anche attraverso la partecipazione a iniziative di information sharing;

- invita le FMI ad attuare processi - non solo di tipo tecnologico - in linea con le migliori pratiche internazionali. In particolare le FMI devono disporre di capacità avanzate per monitorare, rilevare tempestivamente e contenere gli impatti di attacchi cyber;

- invita le FMI a prepararsi per minacce cyber estreme ma plausibili e indirizza le FMI verso le azioni necessarie per costruire una capacità di ripartenza entro due ore da un evento distruttivo (in coerenza con il principio 17 dei PFMI). La guida, pur riconoscendo le difficoltà di raggiungere tale obiettivo, osserva che sono disponibili opzioni tecniche e organizzative che possono supportare il raggiungimento di tale obiettivo;

- ricorda che la resilienza del mercato dipende dall'intero ecosistema della FMI e quindi è necessario uno sforzo collettivo per assicurare la stabilità finanziaria, che includa la realizzazione di esercitazioni;

- sottolinea che la resilienza cyber richiede un continuo adattamento e miglioramento.

11.3 Aziende quotate in mercati regolamentati

Il Codice di Autodisciplina, in linea con l'esperienza dei principali mercati internazionali, indica le best practice in materia di governo societario raccomandate al Comitato per la Corporate Governance delle Società Quotate. Tra gli articoli che compongono il Codice di Autodisciplina, l'art. 7 fornisce i Principi, Criteri Applicativi e Commenti sul Sistema di controllo interno e di gestione dei rischi (SCIGR). Il Codice assegna un ruolo centrale alla "identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi" per contribuire alla conduzione dell'impresa coerente con gli obiettivi e all'assunzione di decisioni consapevoli in un contesto in cui anche i cyber risk stanno acquisendo una sempre maggiore rilevanza. La stessa ridenominazione del "sistema di controllo interno" in "sistema di controllo interno e di gestione dei rischi" ("SCIGR") e del "comitato per il controllo interno" in "comitato controllo e rischi" confermano la specifica attenzione rivolta dagli estensori del Codice proprio a tale temi. Le scelte ora richiamate paiono essere il frutto dalla presa d'atto, da parte dei redattori del Codice di Autodisciplina, che "la moderna concezione dei controlli ruota attorno alla nozione di rischi aziendali, alla loro identificazione, valutazione e monitoraggio". È anche per tale motivo che "la normativa e il Codice si riferiscono al sistema di controllo interno e di gestione dei rischi come a un sistema unitario di cui il rischio rappresenta il filo conduttore". L'art. 7 del Codice di Autodisciplina fornisce poi una chiara definizione di SCIGR, in linea con quanto previsto dal CoSO ERM Integrated Framework, vale a dire "l'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi". Se si fa riferimento all'esperienza

in altri paesi, la SEC (Security Exchange Commission USA) ha emesso linee guida sulla cyber security per le società quotate, che riguardano anche primari gruppi italiani. Viene richiesto alle aziende di considerare il cyber risk e tenere conto di tutte le informazioni disponibili pertinenti, tra cui incidenti precedenti e la gravità e la frequenza degli stessi. Inoltre va valutata la probabilità degli incidenti e verificata l'entità quantitativa e qualitativa di tali rischi, inclusi i costi potenziali e altre conseguenze derivanti da appropriazione indebita di beni o di informazioni sensibili, corruzione di dati o interruzione dell'operatività. Tra fattori specifici, citati dalla SEC, da considerare nella valutazione del cyber risk ci sono:

- L'adeguatezza delle azioni preventive adottate per ridurre i cyber risk, nel contesto societario e del settore in cui opera la società;
- Le vulnerabilità ad attacchi e minacce di cui la società è a conoscenza, gli incidenti subiti e se si tratta di eventi singoli o di eventi più rilevati e sostanziali;
- Gli aspetti dell'operatività di business che danno luogo ai cyber risk rilevanti;
- I costi potenziali e le conseguenze di tali rischi.

Ritornando ai requisiti italiani il Principio 7.P.3 individua, in coerenza con gli orientamenti dei Framework internazionali, anche gli attori coinvolti a vario titolo nell'indirizzo, nella gestione, nella valutazione e nel monitoraggio del SCIGR, ciascuno per le proprie rispettive competenze. Ci si riferisce, più precisamente, a:

- il Consiglio di Amministrazione, sia collegialmente nel suo ruolo di indirizzo e definizione delle linee guida del sistema, sia attraverso l'individuazione di soggetti delegati (l'amministratore incaricato del sistema di controllo interno e di gestione dei rischi) e di comitati al suo interno (il comitato controllo e rischi);
- il management;
- le funzioni aziendali di primo e secondo livello con compiti di gestione del SCIGR;
- la funzione internal audit quale linea di difesa di terzo livello;
- il Collegio Sindacale quale organo di controllo.

Il ruolo centrale è senza dubbio affidato al Consiglio di Amministrazione, il quale, tra l'altro, "definisce le linee di indirizzo del sistema di controllo interno e di gestione dei rischi, in modo che i principali rischi afferenti all'emittente e alle sue controllate risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati" e in tale ambito devono essere ricondotti i cyber risk . Il Consiglio di Amministrazione è altresì chiamato, ai sensi del criterio applicativo 1.C.1, a definire "la natura e il livello di rischio compatibile con gli obiettivi strategici dell'emittente". Si può facilmente ravvisare in tale disposizione il riferimento al concetto di risk appetite (ovvero il livello di rischio complessivo che l'emittente è disposto ad assumere per raggiungere i propri obiettivi), in linea con l'approccio suggerito dal Framework nella valutazione dei rischi cyber. Fermo restando quanto sopra, emerge in termini generali che: "un sistema dei controlli, per essere efficace, deve essere "integrato": ciò presuppone che le sue componenti siano tra loro coordinate e interdipendenti e che il sistema, nel suo complesso, sia a sua volta integrato nel generale assetto organizzativo, amministrativo e contabile della società" (cfr. Commento all'art. 7). Il già richiamato Principio 7.P.3 raccomanda inoltre agli emittenti l'individuazione di modalità di coordinamento tra i vari soggetti coinvolti nel SCIGR: "al fine di massimizzare l'efficienza del sistema di controllo interno e di gestione dei rischi e di ridurre le duplicazioni di attività". In particolare, il Consiglio di

Amministrazione esplica la sua centralità nella definizione dei limiti di rischio assumibili e delle linee guida per la gestione del rischio, la cui effettiva applicazione è demandata all'intera struttura organizzativa, attraverso la:

- definizione dei piani strategici, finanziari e industriali della società, al fine di accertare la coerenza delle strategie e degli obiettivi delineati con i livelli di rischio assumibili, nonché fornire le linee di indirizzo del SCIGR riguardo i livelli di rischio ritenuti accettabili (che possono essere rivisti sulla base degli esiti delle attività di monitoraggio);
- valutazione dell'adeguatezza e dell'efficacia del SCIGR rispetto alle caratteristiche dell'impresa e del Gruppo e al profilo di rischio assunto;
- sistema delle deleghe, con relativo conferimento di poteri al management, a cui il Consiglio di Amministrazione affida il controllo del rischio assunto.

Affinché il consiglio di amministrazione possa acquisire tutte le informazioni necessarie per definire gli obiettivi attesi coerentemente con i livelli di rischio sostenibili, nonché per monitorare il perseguimento degli stessi e l'efficacia di sistemi di controllo e di gestione del rischio, i flussi informativi tra tutti gli attori del SCIGR devono imprescindibilmente essere affidabili, chiari, completi e tempestivi; essi rappresentano dunque un elemento cruciale su cui si fonda l'intero sistema di risk oversight. Da tutto quanto sopra riportato si evince chiaramente come il Framework Nazionale per la Cyber Security nell'ambito delle società quotate potrà fornire elementi a supporto del Codice di Autodisciplina consentendo un adeguata valutazione e gestione dei cyber risk.

Ringraziamenti

I curatori di questo volume desiderano ringraziare gli autori per il tempo speso in questo esercizio. Un grande team pubblico-privato che ha lavorato perfettamente in sincrono e armonia. Un grazie particolare va agli autori e alle organizzazioni che hanno partecipato alla stesura del testo e che hanno scelto di rimanere anonime. Infine, il documento è stato sottoposto a una consultazione pubblica che ha fortemente contribuito al miglioramento del testo e del contenuto attraverso commenti specifici ed emendamenti puntuali. Ognuno dei circa cinquecento emendamenti e commenti ricevuti è stato attentamente valutato da un tavolo di lavoro specifico. Si ringraziano tutti gli autori di tali commenti ed emendamenti. Infine, un ringraziamento particolare agli autori di commenti ed emendamenti accettati e quindi integrati nel testo. Di seguito i nomi degli autori che hanno accettato di essere ringraziati pubblicamente:

Romano Stasi (ABI Lab)

Liberato Pesticcio (Almaviva)

Panfilo Ventresca (Almaviva)

Alessandro Vinciarelli (Almaviva)

Giancarlo Butti (Banco Popolare)

Claudio Ciccotelli (CIS-Sapienza)

Federico Lombardi (CIS-Sapienza)

Mauro Alovisio (CSIG Ivrea Torino)

Riccardo Abeti (CSIG Ivrea-Torino, Unione Avvocati Europei)

Marco Baldassari (CSIG Ivrea-Torino)

Raoul Chiesa (CSIG Ivrea-Torino)

Selene Giupponi (CSIG Ivrea-Torino)

Giulio Cantù (Comitato AICQ)

Antonio Rassu (Comitato AICQ)

Valerio Teta (Comitato AICQ)

Francesco Di Maio (ENAV)

Maria Doris Di Marco (ENAV)

Wang Yujun (Huawei Technologies Italia SRL)

Pier Luigi Rotondo (IBM Italia S.p.A.)

Glauco Bertocchi (ISACA)

Alberto Piamonte (ISACA)

Petro Caruso (Palo Alto Networks)

Palma Ombretta (Poste Italiane)

Rocco Mammoliti (Poste Italiane)

Riccardo Roncon (RSA Assicurazioni)

Damiano Bolzoni (Security Matters)

Enrico Cambiaso (Università degli studi di Genova)

Sandro Bologna

Luigi Carrozzi

Questo lavoro rientra nelle attività di ricerca finanziate dal progetto Italiano MIUR TENACE.
Si ringraziano le seguenti organizzazioni che hanno generosamente supportato l'evento di presentazione del 4 febbraio 2016.

Bibliografia

[1] Maria Cristina Arcuri, Roberto Baldoni, Marina Brogi, Giuseppe Di Luna, Attacchi alle infrastrutture finanziarie attraverso armi cibernetiche. Franco Angeli Editore, 20pg, ISBN: 9788820440145, 2013.

[2] Bank for International Settlement (BIS), Guidance on cyber resilience for financial market infrastructures - consultative paper, Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions, November 2015 http://www.bis.org/cpmi/publ/d138.htm

[3] Roberto Baldoni, Rocco De Nicola Editors, Il Futuro della Cyber Security in Italia, Consorzio Interuniversitario Nazionale Informatica, November 2015 https://www.consorzio-cini.it/labcs-home/libro-bianco

[4] Roberto Baldoni, Luisa Franchina, Luca Montanari. Verso una struttura nazionale di condivisione ed analisi delle informazioni. Franco Angeli Editore, 20pg, ISBN 9788891706881, 2014.

[5] Roberto Baldoni, Luca Montanari Editors. 2013 Italian Cyber Security Report - Critical Infrastructure and Other Sensitive Sectors Readiness. Università degli Studi di Roma La Sapienza. 2014 https://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html

[6] Roberto Baldoni, Luca Montanari Editors. 2014 Italian Cyber Security Report - Consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione Italiana. Università degli Studi di Roma La Sapienza. November 2015 http://www.cis.uniroma1.it/csr2014

[7] Roberto Baldoni, Gregory Chockler: Collaborative Financial Infrastructure Protection - Tools, Abstractions, and Middleware. Springer 2012 http://www.springer.com/us/book/9783642204197

[8] Borsa italiana - Codice di Autodisciplina, Luglio 2015 http://www.borsaitaliana.it/borsaitaliana/regolamenti/corporategovernance/corporategovernance.htm

[9] Tim Casey, Kevin Fiftal, Kent Landfield, John Miller, Dennis Morgan, Brian Willis. The Cybersecurity Framework in Action: An Intel Use Case. Intel 2014 http://www.intel.com/content/www/us/en/government/cybersecurity-framework-in-action-use-case-brief.html

[10] ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems – Overview and vocabulary http://www.iso.org

[11] ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity http://www.iso.org

[12] Confindustria, Università Cà Foscari, Demos & Pi, Afferrare il futuro! Strategie di risk management per l'impresa di domani, 2011 http://www.giovanimprenditori.org/confindustria_afferrare_ilfuturo.pdf

[13] Stephen Coraggio, John Rogers, Nicholas Hilgeman NIST Cybersecurity Framework: Implementing the framework Profile. Booz-Allen-Hamilton, 2014 https://www.boozallen.com/insights/2015/07/nist-cybersecurity-framework

[14] COSO Enterprise Risk Management - Integrated Framework 2004 http://www.coso.org/

[15] Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0) National Institute of Standards and Technology. 2014 http://www.nist.gov/cyberframework/

[16] Douglas Gray, et al. "Improving Federal Cybersecurity Governance Through Data-Driven Decision Making and Execution." TECHNICAL REPORT, CMU/SEI-2015-TR-0112015, September 2015 http://resources.sei.cmu.edu/asset_files/TechnicalReport/2015_005_001_444963.pdf

[17] Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012

[18] Robert Mayer, Brian Allen (editors). Cybersecurity Risk Management and best practices:Final Report The Communications Security, Reliability and Interoperability (CSRIC) Council - Working Group 4, 2015 https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf

[19] Presidenza del Consiglio dei Ministri: Quadro strategico nazionale per la sicurezza dello spazio cibernetico http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf

[20] Presidenza del Consiglio dei Ministri: Piano nazionale per la protezione cibernetica e la sicurezza informatica, http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf.

[21] Presidenza del Consiglio dei Ministri: Decreto del 24 gennaio 2013 - Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, 2013 http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg

[22] Presidenza del Consiglio dei Ministri, Sistema di informazione per la sicurezza della Repubblica, Relazione sulla politica per la Sicurezza della Repubblica, III Parte, pag. 81-87, 2014, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2015/02/relazione-2014.pdf

[23] Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris, 2015

[24] David Patt. Cyber security is not just the IT department's problem. Financial Times. November 2015. http://www.ft.com/intl/cms/s/0/f6b50038-92a1-11e5-bd82-c1fb87bef7af.html?desktop=true#axzz3srZntwJX

[25] 2015 Cost of Cyber Crime: Global. Ponemon Institute, 2015 http://www.ponemon.org/

[26] Perry Pederson. A RIPE Implementation of the NIST Cyber Security Framework. Langner 2014 http://www.langner.com/en/wp-content/uploads/2014/10/A-RIPE-Implementation-of-the-NIST-CSF.pdf

[27] ENISA, A simplified approach to Risk Management for SMEs, ENISA Deliverable: Information Package for SMEs, febbraio 2007, https://www.enisa.europa.eu/publications/archive/RMForSMEs

[28] Shackelford, S. et al. Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices. Texas International Law Journal, 2015 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446631