

# IL SISTEMA DI CONTROLLO INTERNO NEL SETTORE PUBBLICO

Un modello di Control Governance  
per la Pubblica Amministrazione

*Febbraio 2024*

*Il presente documento è stato redatto in collaborazione tra Protiviti Government Services, Regione Lombardia, ORAC e il Dipartimento di Scienze Economico-Aziendali e Diritto per l'Economia dell'Università degli Studi di Milano-Bicocca.*

*I suoi contenuti non possono essere riprodotti, in tutto o in parte, o citati per la distribuzione senza il preventivo consenso scritto dei redattori.*

*Prima edizione di stampa: Febbraio 2020*

*Seconda edizione di stampa: Novembre 2021*

*Terza edizione di stampa: Febbraio 2024*

# CONTENUTI

Per maggiori informazioni sulle iniziative del Tavolo di Lavoro, visita:

<https://www.audit-riskmanagement4pa.com/ta-volo-di-lavoro/>

<https://www.protiviti.com/it-it/government>



<b>PREMESSA</b>	<b>5</b>
<b>IL CONTESTO DI RIFERIMENTO</b>	<b>7</b>
Introduzione	8
Il contesto normativo rilevante	10
Il modello proposto dal network PIC	11
Gli elementi del modello	12
La centralità dell'analisi dei rischi	13
Gli standard per la valutazione del S.C.I.	14
<b>IL LAVORO DEI TAVOLI '19/20 - 1° EDIZIONE</b>	<b>16</b>
Tavolo 1: il modello di Control Governance	17
Tavolo 2: l'analisi dei rischi	19
Le dimensioni da sviluppare	21
Le «regole chiave» di un modello efficace	22
<b>IL LAVORO DEI TAVOLI '20/21 - 2° EDIZIONE</b>	<b>23</b>
Tavolo ristretto: la ricognizione e valutazione del S.C.I.	24
<b>IL LAVORO DEI TAVOLI '22/23 - 3° EDIZIONE</b>	<b>27</b>
Metodologia «processi-rischi-controlli» e Matrice «processi-controlli»	29
L'estensione del Questionario COSO agli enti del Sistema Regionale	31
<b>CONCLUSIONI</b>	<b>33</b>
Un bilancio per le attività dei Tavoli di Lavoro	34
<b>ALLEGATI</b>	<b>35</b>
Allegato 1 - Il Glossario dei Rischi	36
Allegato 2 - La Mappatura dei Controlli	40
Contribuiti e ringraziamenti	41



# PREMESSA

---

Il presente documento è stato predisposto come sintesi delle attività svolte, dal 2019 ad oggi, nell'ambito del Tavolo di Lavoro sul Sistema di Controllo Interno nella Pubblica Amministrazione, un' iniziativa, promossa da Regione Lombardia, ORAC - Organismo regionale per le attività di controllo, Università degli Studi Milano-Bicocca e Protiviti, e che si è posto l'obiettivo di stimolare il dibattito tra gli studiosi e gli addetti ai lavori sulle possibili evoluzioni dei processi di Governo e Controllo degli Enti Pubblici.

L'iniziativa si è sviluppata in diversi momenti:

La **prima edizione** del Tavolo (anni 2019/2020) ha concentrato il proprio lavoro sullo sviluppo di un modello unitario di rappresentazione/ricognizione del Sistema di Controllo Interno nonché sull'applicazione delle tecniche di valutazione del rischio nelle Pubbliche Amministrazioni. Gli esiti di tale lavoro sono stati presentati il 12 febbraio 2020 all'università Bicocca di Milano e riassunti nella prima edizione del presente documento datata febbraio 2020.

La **seconda edizione** (anni 2020/2021) ha avuto l'obiettivo di definire, partendo dalla mappatura di tutti i presidi di controllo presenti nel perimetro della Giunta Regionale, uno strumento di diagnosi, ispirato agli standard riconosciuti a livello internazionale, per analizzare e valutare il livello di maturità del sistema di controllo interno delle organizzazioni pubbliche. Gli esiti di tale lavoro, sono stati illustrati durante un webinar tenutosi venerdì 29 ottobre 2021 (per maggiori informazioni su cosa si è discusso durante il webinar si rimanda alla pagina <https://www.audit-riskmanagement4pa.com/tavolo-di-lavoro/>).

La **terza edizione** (anni 2022/2023) ha avuto da un lato l'obiettivo di elaborare una metodologia «processi-rischi-controlli» e formalizzare una proposta pilota di mappatura processi e controlli, dall'altro di estendere lo strumento di diagnosi, «questionario COSO» elaborato nell'ambito della seconda edizione, agli enti del Sistema Regionale lombardo (SIREG) con il fine di testare lo strumento di autovalutazione.

Il presente elaborato rappresenta il compendio dei contenuti sviluppati nelle tre edizioni del Tavolo che per comodità di lettura abbiamo aggiornato (per quanto riguarda i contenuti relativi alla prima e seconda edizione) ed integrato con un nuova sezione dedicata ai contenuti della terza.

Buona lettura!



# IL CONTESTO DI RIFERIMENTO

# INTRODUZIONE

Nel corso degli ultimi decenni, il tema dei controlli interni delle Pubbliche Amministrazioni (PA) italiane è stato a più riprese interessato da **interventi normativi** che hanno contribuito in maniera significativa ad indirizzare le scelte organizzative e i modelli di Control Governance da adottare.

Il Legislatore ha provveduto a formalizzare non solo le **tipologie di controlli** da porre in essere dalle PA italiane, ma spesso anche ad indicare in maniera puntuale quali fossero le **strutture** che gli Enti dovevano costituire ai fini dell'espletamento di tali controlli.

Con il succedersi delle contaminazioni provenienti dal settore privato, inoltre, si è assistito ad un parziale «cambio di rotta» nella definizione di tali controlli: il Legislatore infatti è progressivamente passato dal disciplinare lo svolgimento dei tradizionali **controlli ex ante in merito alla legittimità dell'azione amministrativa** all'introdurre anche attività di **verifica ex post, maggiormente orientati all'efficacia** dell'operato delle PA.

La **sedimentazione** dei numerosi interventi normativi occorsi nel tempo (*come in parte dettagliati di seguito*) restituisce oggi un quadro molto **complesso**, in termini di **pluralità di attori** e **molteplicità di controlli**, che *devono* essere posti in essere dalle Pubbliche Amministrazioni italiane. Tale complessità risulta nell'impostazione di sistemi di controllo interno fortemente **settorializzati rispetto alle aree di competenza discendenti dalla norma**, nonché nella proliferazione di attività di verifica non sempre coordinate e coerenti tra loro (*in termini di metodologie e degli strumenti adottati, flussi informativi tra le diverse strutture organizzative etc.*), con conseguenti inefficienze nell'operatività e poca efficacia nella reportistica verso i Vertici istituzionali.

Se, da una parte, sono numerosi i soggetti deputati allo svolgimento delle attività di controllo, dall'altra non è formalmente individuata una **«cabina di regia»** che possa sovrintendere, indirizzare e coordinare tali iniziative, fungendo nel contempo da interlocutore con i Vertici politico-organizzativi dell'Ente.

Il quadro dei controlli interni nel settore pubblico è stato oggetto di analisi e dibattito non solo nel contesto italiano, ma anche sul **piano internazionale**. Già nei primi anni '90, ad esempio, l'*International Organization of Supreme Audit Institutions (INTOSAI)* ha elaborato delle linee guida<sup>1</sup>, poi aggiornate negli anni successivi, sugli standard di controllo interno nel settore pubblico, dando indicazione degli elementi chiave che costituiscono un «ambiente di controllo» efficace.

Allo stesso modo, la *International Federation of Accountants (IFAC)* e il *Chartered Institute of Public Finance and Accountancy (CIPFA)* si sono pronunciati in merito ai principi che dovrebbero ispirare dei sistemi di «buona governance» nelle Pubbliche Amministrazioni, tra i quali si ritiene rilevante l'esistenza di un sistema di controllo interno efficace<sup>2</sup>.

Infine, un contributo rilevante è stato fornito dal **network PIC**<sup>3</sup>, che ha elaborato un Modello basato sul concetto delle «tre linee di difesa», traslato dal settore privato<sup>4</sup> che a tutt'oggi rappresenta il principale punto di riferimento in materia. Pertanto, si è inteso impostare le analisi e il lavoro dei Tavoli sui sistemi di Control Governance nella Pubblica Amministrazione italiana partendo da tale *framework*.

Il Public Internal Control Network (PIC), composto da rappresentanti di tutti gli Stati Membri dell'UE, è stato istituito in seno alla DG Budget della Commissione europea nel 2012, con l'obiettivo di curare e stimolare il dibattito sui Sistemi di Controllo Interno nel Settore Pubblico dell'UE tramite l'organizzazione di Conferenze periodiche sulla materia. Nell'espletamento dei propri compiti, il PIC Network è assistito da un PIC Working Group, composto da rappresentanti di 7-8 Stati Membri..

Fonte: [https://ec.europa.eu/budget/pic/index\\_en.cfm](https://ec.europa.eu/budget/pic/index_en.cfm).

<sup>1</sup> INTOSAI, «Guidelines for Internal Control Standards for the Public Sector» (1992).

<sup>2</sup> IFAC e CIPFA, «International Framework: Good Governance in the Public Sector» (2014).

<sup>3</sup> PIC Working Group, Discussion Paper no. 9, Ref. 2017-2, «Public Internal Control Systems in the European Union - The three lines of defense in a Public Sector Environment» (2017).

<sup>4</sup> IIA Position Paper, «The three lines of defense in effective risk management and control» (2013).



# INTRODUZIONE

Alla luce di un quadro così delineato per la definizione di un modello di control governance per la Pubblica Amministrazione, si ravvisa comunque **l'esigenza di valutare l'adeguatezza del Sistema di Controllo Interno adottato**, delle relative regole, procedure e strutture organizzative.

La costruzione di un buon Sistema di Controllo Interno è fondamentale tanto quanto la sua manutenzione e la sua valutazione periodica in termini di affidabilità, sia sotto il profilo del disegno che del funzionamento.

La valutazione del Sistema di Controllo Interno deve, in tale ottica, essere il risultato combinato di molteplici fattori:

- processo di valutazione qualitativa del grado di maturità di tutti le componenti del sistema;
- efficienza ed efficacia degli elementi di controllo;
- copertura del sistema di ogni componente e del presidio di ogni linea di difesa;
- analisi dell'insieme dei controlli a presidio del rischio;
- conoscenza che ciascun *owner* possiede del processo e delle situazioni di rischio che potrebbero verificarsi.

Un processo di valutazione del Sistema di Controllo Interno deve partire dall'analisi della situazione attuale degli elementi del controllo rilevanti, in modo da identificare le aree di miglioramento e le migliori prassi rispetto ad un modello ideale che rappresenta la maturità massima raggiungibile per il Sistema di Controllo Interno.

Ad oggi, tuttavia, molto è stato fatto in termini di valutazione dei sistemi di controllo in ambito privatistico ma **in letteratura vi sono pochi casi in cui si è approfondito lo studio della valutazione per i sistemi di controllo in ambito pubblico**.

Un tentativo in tal senso è stato fatto dall'INTOSAI che, con l'elaborazione del INTOSAI 9100 «*Guidelines for Internal Control Standards for the public sector*», ha applicato il framework dello standard internazionale del COSO REPORT al settore pubblico e dalla Commissione Europea, che lo ha espressamente richiamato nella nota C(2017) 2373 final del 19.4.2017 - *Revision of the Internal Control Framework*.

Tale contesto, povero di riferimenti metodologici per la P.A., ha rappresentato, secondo chi scrive, il terreno più adatto e proficuo per la **sperimentazione di nuovi modelli di control governance e di valutazione del sistema**, creando di concerto con le strutture quotidianamente coinvolte nelle attività di controllo, gli strumenti più efficaci per leggere criticamente il quadro in cui essi sono inseriti.

L'iniziativa dei Tavoli descritta nelle sezioni successive, tesa a colmare tali «gap metodologici», ha lavorato quindi per l'elaborazione, da un lato, di un modello di control governance basato sulle tre linee di difesa e che rispondesse alle peculiarità e alle esigenze tipiche delle Pubbliche Amministrazioni italiane, dall'altro di un modello dei rischi per il settore pubblico (EDIZIONE TAVOLI 2019/2020). Il lavoro della seconda edizione dei Tavoli (EDIZIONE TAVOLI 2020/2021), condotto in modalità «ristretta» per l'emergenza pandemica contingente, è stato invece rivolto alla definizione di uno strumento diagnostico per i sistemi di controllo interno definiti come al modello di cui alle prime edizioni. Nell'ambito della terza edizione dei Tavoli (EDIZIONE TAVOLI 2022/2023) si è provveduto a testare lo strumento diagnostico estendendolo agli enti del Sistema Regionale lombardo (SIREG), e di elaborare una metodologia «processi-rischi-controlli» formalizzando così una proposta pilota di mappatura processi e controlli.

## IL CONTESTO NORMATIVO RILEVANTE

A livello nazionale, alcune delle norme hanno contribuito in maniera preponderante alla configurazione del sistema dei controlli interni nelle Pubbliche Amministrazioni. Si riporta di seguito l'elenco dei principali interventi normativi che hanno disciplinato le attività di controllo e l'organizzazione delle stesse nei contesti pubblici.



### Attività di controllo / attori previsti dal D.Lgs. 286/1999 e s.m.i.

- **Controllo di regolarità amministrativo-contabile**, svolto dalla Ragioneria / Servizio Finanziario dell'Ente e finalizzato a garantire la legittimità, regolarità e correttezza dell'attività amministrativa;
- **Controllo di Gestione**, finalizzato a monitorare l'andamento generale delle attività dell'Organizzazione rispetto all'efficienza ed efficacia di utilizzo delle risorse;
- **Valutazione della Dirigenza**, finalizzato ad esprimere un giudizio sulle attività svolte dai soggetti con responsabilità dirigenziale dell'Organizzazione;
- **Valutazione e Controllo Strategico**, finalizzato a valutare la congruenza tra gli obiettivi strategici definiti dall'Organizzazione in fase di pianificazione e i risultati effettivamente raggiunti.

### Attività di controllo / attori previsti dal D.Lgs. 81/2008 e s.m.i.

- Introduzione del **Responsabile Servizio Prevenzione e Protezione (RSPP)**, soggetto preposto, tra le altre cose, ad individuare, valutare e monitorare i rischi interni all'Organizzazione con riferimento alla salute e sicurezza sul lavoro.

### Attività di controllo / attori previsti dal D.Lgs. 150/2009 e s.m.i.

- **Valutazione della performance** dell'Organizzazione, sia in termini di raggiungimento degli obiettivi prefissati, sia in termini di economicità ed efficienza della gestione delle risorse a disposizione.

### Attività di controllo / attori previsti dalla L. 190/2012 e s.m.i. e dal D.Lgs. 33/2013 e s.m.i.

- Introduzione del **Responsabile per la Prevenzione della Corruzione e per la Trasparenza (RPCT)**, soggetto con responsabilità rispetto alla formalizzazione e al monitoraggio delle attività di prevenzione della corruzione nell'Organizzazione, nonché rispetto alla gestione degli obblighi di trasparenza da parte della stessa.

### Attività di controllo / attori previsti dal D.Lgs. 90/2017 e s.m.i.

- Introduzione del **Responsabile Antiriciclaggio**, soggetto preposto alla formalizzazione e monitoraggio di regole interne atte a prevenire la commissione di illeciti riconducibili ai reati di antiriciclaggio disciplinati dal Decreto.

Giova inoltre menzionare il **D.Lgs. 231/2001 e s.m.i.** che, pur non rappresentando un obbligo di legge per i soggetti a cui si applica<sup>5</sup>, ha introdotto una ulteriore struttura di controllo nell'Organismo di Vigilanza, incaricato di vigilare sul rispetto dei presidi definiti nel Modello di organizzazione, gestione e controllo adottato dall'Organizzazione ai sensi del Decreto medesimo.

Infine, anche il **Regolamento Europeo UE 2016/679** in materia di protezione dei dati personali (noto anche come "GDPR – General Data Protection Regulation"), che ha ad oggetto la "tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati" (art. 1, par. 1), ha avuto un notevole impatto nelle attività di controllo del settore pubblico.

<sup>5</sup> L'art. 1 del Decreto specifica che lo stesso si applica agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica. Le previsioni del Decreto non si applicano invece allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici nonché agli enti che svolgono funzioni di rilievo costituzionale.

# IL MODELLO PROPOSTO DAL NETWORK PIC

Il **Modello di Control Governance** elaborato dal Network PIC, come detto, si basa sul concetto delle «tre linee di difesa».

Secondo il PIC, tale impostazione riflette la necessità, per i soggetti in capo ai quali risiedono autorità, responsabilità e *accountability* del sistema di governance dell'ente, di stabilire delle «linee di difesa subordinate», che li assistano nell'espletamento di controlli di varia natura.

Nell'elaborazione del Modello, il PIC prende in considerazione sia le interazioni tra i soggetti / controlli interni all'Organizzazione, sia quelle tra l'Organizzazione stessa e i soggetti esterni che ne influenzano e indirizzano il disegno e la gestione del sistema di controllo interno.

Nel proporre il proprio Modello, il PIC riconosce come, ad oggi, ogni Stato Membro dell'UE interpreti il sistema di controllo interno delle Pubbliche Amministrazioni secondo le proprie esigenze normative e le interazioni in essere tra i diversi *stakeholder* coinvolti nel proprio contesto (con riferimento al contesto italiano: Organi Legislativi, Corte dei Conti, Ragioneria Generale dello Stato, ANAC, etc.).

Allo stesso tempo, il PIC ribadisce come, anche internamente a ciascuno Stato Membro, la diversa natura delle Pubbliche Amministrazioni, il loro diverso dimensionamento e gli ambiti di intervento, lascino spazio a rielaborazioni e reinterpretazioni del Modello, per tenere in considerazione le peculiarità di ciascuna e conciliare le diverse esigenze.

Resta quindi inteso che, pur rappresentando un utile *framework* di riferimento per la costruzione di un Modello di Control Governance nel Settore Pubblico, quello proposto dal PIC sia un Modello suscettibile di modifiche e integrazioni, come si vedrà nel prosieguo del documento.

Figura 1 - Il Modello di Control Governance proposto dal PIC



Nella pagina seguente si riporta una breve descrizione delle principali componenti del Modello.

# GLI ELEMENTI DEL MODELLO

## I LINEA DI DIFESA

Controlli manageriali

Misure di controllo interno



La prima linea di difesa è rappresentata da **tutte le funzioni** dell'Ente che, nell'ambito delle responsabilità assegnate, gestiscono i **rischi connessi ai processi** e alle attività operative, e definiscono ed eseguono i **controlli a presidio di tali rischi** (c.d. controlli di linea).



La prima linea di difesa svolge **controlli diffusi a tutti i livelli dell'organizzazione**, e include sia chi esegue una determinata attività, sia chi ne ha la responsabilità di supervisione.

## II LINEA DI DIFESA

Controlli finanziari

Sicurezza

Risk Management

Qualità

Ispezione

Compliance



La seconda linea di difesa presidia il processo di valutazione e controllo dei rischi garantendone la coerenza rispetto agli obiettivi aziendali, e rispondendo a criteri di segregazione organizzativa in modo sufficiente per consentire un efficace monitoraggio.



La seconda linea di difesa include tutte le funzioni dedicate allo sviluppo di **programmi specifici di gestione del rischio**, in virtù di esigenze normative e/o di scelte organizzative, con il compito di **presidiare l'attuazione e il corretto funzionamento** dei relativi sistemi di controllo interno, e di fornire adeguata informativa al Vertice.

## III LINEA DI DIFESA

Internal Audit



La terza linea di difesa, ovvero la funzione indipendente di **Internal Audit**, **svolge una funzione di assurance** in merito all'efficacia e all'efficienza del Sistema di Controllo Interno complessivo. In ragione del suo mandato, svolge compiti di supervisione a supporto degli organi di controllo e di indirizzo dell'Ente.



L'Internal Audit **fornisce mezzi efficaci per migliorare i processi esistenti e assiste l'Ente nell'implementazione di prassi migliorative**.

Senior Management

Livello politico  
esecutivo  
/ Comitato di Audit



Il **senior management** e il **livello politico esecutivo / comitato di audit** non sono parte delle tre linee di difesa, ma ne rappresentano i principali **stakeholder**.



Tali Organi sono responsabili per la **definizione degli obiettivi** generali dell'Ente e delle **strategie** di raggiungimento di tali obiettivi.

Audit esterno



L'organo di **revisione esterna** ha il compito di riferire al livello legislativo circa la **performance** dell'Ente.



Tale Organo esprime un giudizio sulla **correttezza dell'utilizzo di fondi pubblici** da parte dell'Ente e valuta la **completezza e l'affidabilità delle informazioni finanziarie e non finanziarie** fornite dallo stesso.

Organi Legislativi



Anche gli **Organi Legislativi** non fanno parte delle tre linee di difesa, tuttavia sono parti interessate dalle loro attività.



Tali Organi forniscono **assurance sull'efficacia dei Sistemi di Controllo Interno** degli Enti attraverso **specifici atti normativi**.

# LA CENTRALITÀ DELL'ANALISI DEI RISCHI

Per una corretta implementazione del Modello proposto dal PIC è necessario disporre di adeguati processi di analisi e valutazione dei rischi, essendo questo uno degli elementi chiave delle 3 linee di difesa.

Un rischio è un *evento incerto e con conseguenze avverse*. Il grado di incertezza (**probabilità**) e la gravità delle conseguenze (**impatto**) sono gli elementi di valutazione che caratterizzano un rischio.

L'introduzione di processi strutturati di **gestione e controllo dei rischi (c.d. Risk Management)** contribuisce a rendere l'organizzazione **consapevole** dei rischi che corre e **informata** sulle conseguenze derivanti dalle decisioni che prende, assicurando il raggiungimento di **benefici tangibili**:

- Maggiore trasparenza nella gestione del bene pubblico;
- Crescente fiducia da parte dei diversi stakeholder;
- Aumento della responsabilizzazione dei dipendenti;
- Migliore e più efficiente allocazione delle risorse;
- Aumento delle performance economico-finanziarie;
- Maggiore conformità alle leggi e ai regolamenti;
- Riduzione del contenzioso.

Il Risk Management potrebbe quindi rivestire un **ruolo centrale** nel sistema di Control Governance dell'Ente.

Un adeguato sistema di Risk Management si basa sui seguenti elementi caratterizzanti:

- 1) Introduzione di un linguaggio comune dei rischi:** Partendo dall'analisi dei processi aziendali, è necessario identificare le "famiglie" di rischio che possono pregiudicare il raggiungimento degli obiettivi definiti giungendo alla definizione di un Modello dei Rischi per l'organizzazione. I rischi possono essere legati a fattori esterni (l'economia, l'ambiente, la politica, il sociale, il mercato) oppure interni (le infrastrutture, il personale, i processi e i flussi informativi).
- 2) Definizione di un processo di valutazione periodica dei rischi aziendali:** Si tratta di un insieme strutturato di strumenti e metodi per l'identificazione e la valutazione periodica dei rischi aziendali che partendo dal concetto di rischio "inerente" (rischio valutato senza tener conto di alcuna misura di mitigazione) giunge a valutare il c.d. rischio "residuo" (rischio mitigato dalle azioni poste in essere dal personale aziendale), passando attraverso la valutazione del sistema dei controlli a presidio dei rischi di volta in volta individuati.
- 3) Implementazione di adeguati strumenti per la gestione dei rischi identificati:** Al termine dell'attività di valutazione, occorre definire un sistema di gestione dei rischi che definisca le priorità di intervento per ridurre i rischi individuati a un livello ritenuto accettabile.

Le numerose iniziative di analisi e valutazione dei rischi in essere nel settore pubblico in Italia, in gran parte guidate da esigenze di conformità normativa, sono spesso gestite in maniera autonoma e **a livello di processo**, senza considerare tutte le possibili sinergie e / o le sovrapposizioni le une con le altre, con la conseguenza di fornire una visione spesso **frammentata e incompleta** che non consente l'adozione di contromisure efficaci per la riduzione dei rischi esistenti.

L'introduzione di modelli uniformi e di un linguaggio comune, che possano aiutare una ricognizione dei rischi anche **a livello di sistema**, può supportare l'ente nell'individuazione di **tutti gli elementi di rischio rilevanti** e nell'indirizzare in maniera più efficace i relativi presidi di controllo, tenendo altresì in considerazione tutte le iniziative già in essere in **ottica integrata**.

# GLI STANDARD PER LA VALUTAZIONE DEL S.C.I.

Per l'individuazione di standard internazionali utili alla valutazione dei sistemi di controllo interno per la p.a., il riferimento è sicuramente rappresentato dai modelli utilizzati nel settore privato, per i quali ritroviamo numerose metodologie ed applicazioni.

Dalla ricognizione effettuata, gli standard maggiormente aderenti a colmare il gap metodologico relativo ai sistemi diagnostici dei sistemi di controllo interno nell'ambito pubblico, dalla testata efficacia e diffusamente utilizzati in ambito privatistico, risultano essere i seguenti:

## 1) COSO - Internal Control Integrated Framework;

## 2) Capability Maturity Model.

Il COSO - Internal Control Integrated Framework, emanato dalla Treadway Commission (ultima edizione 2013), rappresenta lo standard di riferimento maggiormente riconosciuto a livello internazionale e persegue lo scopo di «determinare il "quantum" di rischio che l'impresa/ente è disposta ad accettare per creare valore per i suoi stakeholders e fornire un unico riferimento per gestire le varie tipologie di eventi incerti con efficacia, in relazione agli obiettivi prestabiliti».

Il COSO, nella sua versione semplificata ed adottata dall'INTOSAI GOV 9100, propone una visione su tre obiettivi: efficienza operativa (controllo di gestione); adeguatezza informativa (controllo amministrativo contabile); conformità alla normativa (compliance) e identifica cinque componenti del sistema, permettendo all'organizzazione di prendere in considerazione diversi aspetti del controllo interno:

### AMBIENTE DI CONTROLLO (Control Environment)

L'ambiente di controllo è l'insieme di standard di condotta, processi e strutture che forniscono la base per lo svolgimento del controllo interno in un'organizzazione.

### VALUTAZIONE DEI RISCHI (Risk Assessment)

La valutazione dei rischi è un processo dinamico per identificare e valutare i rischi che potrebbero influenzare il raggiungimento degli obiettivi e per determinare come tali rischi dovrebbero essere gestiti.

### ATTIVITÀ DI CONTROLLO (Control Activities)

Le attività di controllo assicurano la mitigazione dei rischi connessi al raggiungimento degli obiettivi dell'Ente. Vengono eseguite a tutti i livelli dell'organizzazione, in varie fasi nell'ambito dei processi così come nei sistemi IT.

### INFORMAZIONE E COMUNICAZIONE (Information & Communication)

L'informazione e la comunicazione sono necessarie affinché l'organizzazione possa svolgere efficacemente il controllo interno e supportare il raggiungimento degli obiettivi; essa può essere rivolta all'esterno o all'interno dell'organizzazione.

### MONITORAGGIO (Monitoring Activities)

Valutazioni continue e specifiche sono utilizzate per accertare se i controlli interni siano presenti e funzionanti. I risultati vengono valutati e le eventuali carenze vengono comunicate e corrette in modo tempestivo.

Le 5 componenti del COSO sono a loro volta declinate in **17 principi applicativi associati ai 5 elementi costitutivi del controllo** interno che ogni parte del Sistema dovrebbe presidiare ed assicurano alla funzione di illustrare i requisiti necessari per realizzare un Sistema dei Controlli Interni efficace.

L'applicazione dello standard di riferimento è agevolata dalla compilazione di **questionari di autovalutazione** che guidano il soggetto nella completa analisi di ogni componente del sistema.

# GLI STANDARD PER LA VALUTAZIONE DEL S.C.I.

Per quanto concerne l'aspetto valutativo del sistema, si è inteso individuare uno standard che consentisse di esprimere giudizi graduali evitando l'espressione di pareri positivi/negativi tout court. A seguito di un'approfondita ricognizione degli standard in letteratura, è stato identificato quale modello maggiormente idoneo alla valutazione del SCI un altro standard diffusamente utilizzato in ambito privatistico: il **Capability Maturity Model**, alla base del quale vi sono due concetti chiave: "Maturity" e "Capability".

La "**Capability**" fornisce un'indicazione di quanto la pratica sia istituzionalizzata e in uso da parte dell'organizzazione, mentre la "**Maturity**", o "maturità" restituisce l'informazione sul grado di controllo che si è riusciti ad ottenere su di un insieme di processi. In entrambi i casi, al crescere del livello, aumenta sia il livello di definizione dei processi sia la loro affidabilità, intesa come capacità di raggiungere gli obiettivi prefissati.

Il modello suddivide la maturità organizzativa in cinque livelli; per le organizzazioni che si cimentano con questo standard, l'obiettivo è elevare l'organizzazione fino al Livello 5, il livello di maturità ottimizzato.

Si riporta di seguito uno schema illustrativo del modello:

LIVELLO DI MATURITÀ	DESCRIZIONE	CARATTERISTICHE
5. OTTIMIZZATO	<i>I sistemi di valutazione e gestione di rischi e controlli sono sottoposti a revisione e miglioramento continuo</i>	<ul style="list-style-type: none"> <li>• Processi integrati nelle strategie dell'organizzazione</li> <li>• Sistemi di indicatori strutturati e costantemente aggiornati</li> <li>• Informazione e Comunicazione continua anche verso l'esterno</li> </ul>
4. GESTITO	<i>I rischi e I controlli sono gestiti a tutti i livelli dell'organizzazione, anche con il ricorso a sistemi di tipo informatico</i>	<ul style="list-style-type: none"> <li>• Sistema di Governance strutturato e articolato</li> <li>• Processi integrati e gestiti con strumenti/piattaforme IT</li> <li>• Sistemi di Comunicazione e reporting continui e sistematici</li> </ul>
3. DEFINITO	<i>Sono definite procedure, metodologie e standard comuni per l'identificazione, la valutazione e la gestione di rischi e controlli</i>	<ul style="list-style-type: none"> <li>• Ruoli e responsabilità chiaramente identificate</li> <li>• Procedure, metodologie e standard formalizzati e comuni</li> <li>• Sistemi di Comunicazione e reporting definiti</li> </ul>
2. RIPETIBILE	<i>Esistono processi per l'identificazione e la gestione di rischi e controlli essenzialmente guidati da esigenze normative</i>	<ul style="list-style-type: none"> <li>• Ruoli e responsabilità definite in ambiti specifici</li> <li>• Iniziative e processi gestiti in maniera autonoma</li> <li>• Sistemi di Comunicazione e reporting non sistematici</li> </ul>
1. INIZIALE	<i>La gestione dei rischi e dei controlli è demandata ad iniziative dei singoli, e non è ritenuta prioritaria per l'organizzazione</i>	<ul style="list-style-type: none"> <li>• Ruoli e responsabilità non definite</li> <li>• Analisi dei rischi non sistematica</li> <li>• Controlli non formalizzati</li> </ul>

ORGANIZZAZIONE, PROCESSI E SISTEMI

In sintesi, i modelli sopra individuati hanno caratteristiche tali da presidiare i due ambiti di attività principali nella valutazione di un sistema di controllo interno di un'organizzazione pubblica:

- 1) la propedeutica mappatura ed individuazione delle aree applicative del SCI e la conseguente indagine sulla copertura delle stesse da parte del sistema;
- 2) la valutazione e reporting delle risultanze su un modello scalare che colga tutte le sfaccettature di una organizzazione complessa come quella pubblica.

# IL LAVORO DEI TAVOLI 2019/2020

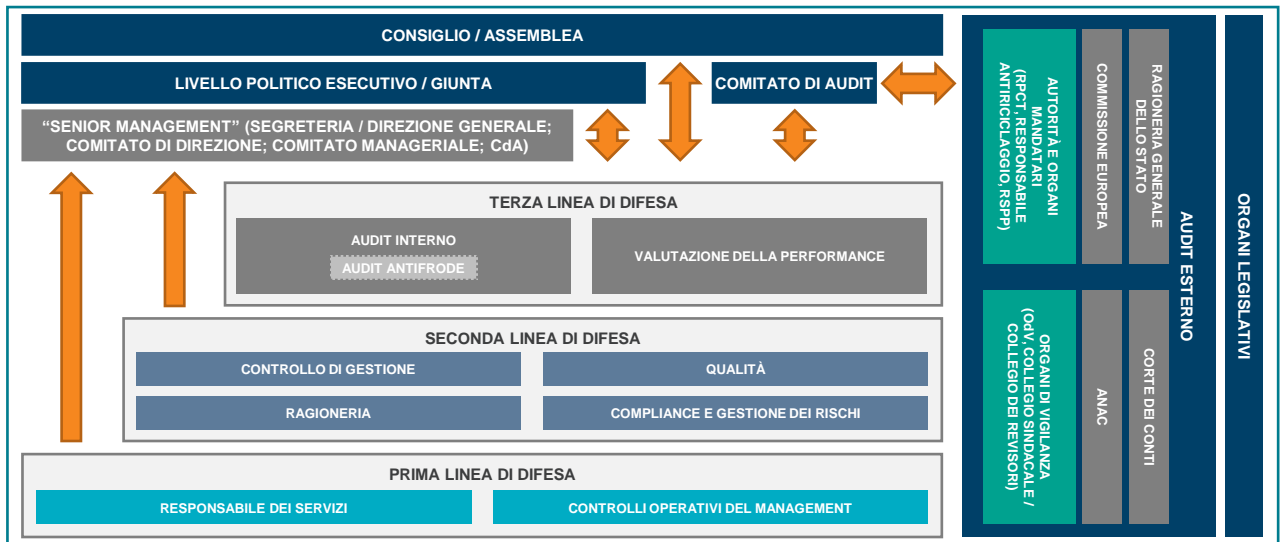
1° EDIZIONE



# TAVOLO 1: IL MODELLO DI CONTROL GOVERNANCE

Il Tavolo 1 si è posto come obiettivo quello di elaborare un Modello di Control Governance che, come quello proposto dal PIC, fosse basato sulle tre linee di difesa e che rispondesse alle peculiarità e alle esigenze tipiche delle Pubbliche Amministrazioni italiane, sia in termini di soggetti deputati al controllo, sia di attività di controllo.

Il Modello elaborato alla luce dell'analisi svolta è illustrato in *Figura 2*.



## GLI ELEMENTI PECULIARI DEL MODELLO

### 1. La Prima Linea di Difesa

La prima linea di difesa definisce e gestisce i **controlli insiti nei processi operativi** volti ad assicurare che le operazioni siano effettuate in modo corretto. Nell'ambito della prima linea di difesa sono incluse le funzioni responsabili dei diversi servizi erogati dall'ente, nonché le funzioni deputate alla gestione dei processi e dei controlli operativi.

### 2. La Seconda Linea di Difesa

La seconda linea di difesa comprende le funzioni responsabili per **l'individuazione, la valutazione, la gestione e il controllo dei rischi tipici e peculiari dell'ente**. In tale ambito sono ricomprese le funzioni e i soggetti introdotti e/o richiesti dei numerosi vincoli normativi e regolamentari cui le Pubbliche Amministrazioni sono esposte.

A tal proposito, anche al fine di assicurare un adeguato coordinamento alle diverse iniziative in essere, nella seconda linea di difesa è prevista la **Funzione di Compliance e Gestione dei Rischi**, che possa sovrintendere e indirizzare le analisi dei rischi in una logica coerente e integrata, con il duplice obiettivo di armonizzare i sistemi di controllo interno esistenti, e di fornire adeguata e tempestiva informativa al Vertice circa i principali rischi cui l'Ente è esposto.

# TAVOLO 1: IL MODELLO DI CONTROL GOVERNANCE

## 3. La Terza Linea di Difesa

La terza linea di difesa include le funzioni deputate al presidio e alla verifica, nel continuo, dell'adeguatezza e dell'effettiva applicazione dei sistemi di controllo in essere, tipicamente attribuite alla **Funzione di Audit Interno**. Nel contesto italiano, tuttavia, la norma ad oggi non prevede l'attribuzione di formali responsabilità di controllo di terzo livello ad un preciso soggetto, lasciando alle singole Organizzazioni la facoltà di istituire o meno tale funzione. Ritenendo tuttavia necessaria l'*assurance* sull'efficacia ed efficienza del Sistema di Controllo Interno, il Modello proposto prevede l'individuazione e la costituzione formale di una struttura che fornisca supporto nel monitorare i rischi e nel migliorare i processi e i controlli in essere.

Oltre alla Funzione di Audit Interno, nel Modello proposto sono state incluse in questo ambito anche le funzioni deputate alla **prevenzione e al controllo delle frodi**, nonché quelle deputate alla valutazione e al **monitoraggio delle performance**.

## 4. Il Senior Management e il Livello Politico

Nell'ambito della categoria che il PIC definisce come «**Senior Management**», il Modello include organi quali la Segreteria / Direzione Generale, il Comitato Manageriale ovvero il Consiglio di Amministrazione, a seconda della natura dell'Organizzazione di riferimento.

Il Modello inoltre distingue, a livello politico, tra organi esecutivi e organi di indirizzo, in ragione delle diverse attività svolte da ciascuno.

## 5. Il Comitato di Audit

Separato dal livello politico, il Comitato di Audit è ritenuto l'organo di Vertice deputato a indirizzare e a presidiare nel suo complesso i sistemi di governance e di gestione dei rischi in essere presso l'Ente, con le seguenti principali attribuzioni:

- Dialogare con le strutture di Audit Interno, Compliance, Gestione dei rischi etc. e con i c.d. «Organi Mandatari», fornendo adeguato **indirizzo e cordinamento** a garanzia del **corretto funzionamento del Sistema di Controllo Interno**;
- Fungere da interlocutore nei confronti dei Vertici politico-organizzativi dell'Ente, fornendo **supporto e presidio** sui principali rischi che possono compromettere il raggiungimento degli obiettivi prefissati;
- Rappresentare una **funzione di raccordo** tra l'interno e l'esterno dell'Organizzazione.

## 6. Organi Mandatari

Quali elementi caratterizzanti del contesto della PA italiana, il Modello prevede una sezione dedicata nella quale si collocano gli attori e le attività di controllo specificatamente previsti dalla **normativa nazionale** (c.d. «Organi Mandatari» quali RPCT, DPO, Responsabile Antiriciclaggio, Organismo di Vigilanza ex D.Lgs. 231/2001, ove applicabile, etc.).

## 7. Organi di Audit Esterni

Congiuntamente agli organi mandatari, il Modello include quegli organi di Audit Esterno che esprimono un giudizio sulla **correttezza dell'utilizzo di fondi pubblici** da parte dell'Ente e valutano la **completezza e l'affidabilità delle informazioni finanziarie e non finanziarie** fornite dallo stesso. Rispetto a quanto già previsto dal PIC, in questa sezione il Modello annovera entità di controllo tipiche della realtà italiana (Corte dei Conti, ANAC, Ragioneria Generale dello Stato).

## TAVOLO 2: L'ANALISI DEI RISCHI

Contestualmente alle attività per il disegno di un Modello di Control Governance, si è inteso lavorare, all'interno del Tavolo 2, alla definizione di un possibile **Modello dei Rischi per la Pubblica Amministrazione italiana**, prendendo come riferimento gli standard e le best practices in materia. Nelle intenzioni del tavolo il modello proposto potrebbe rappresentare un riferimento per l'identificazione dei principali domini di rischio cui l'Ente è esposto, facilitando altresì la progressiva introduzione di un linguaggio comune e uniforme all'interno delle organizzazioni.

Il modello proposto e descritto nelle pagine seguenti, elaborato a seguito di un confronto interno al Tavolo di Lavoro dedicato che ha assunto come base il Modello adottato da Regione Lombardia, rappresenta un possibile **framework concettuale di riferimento** utile per indirizzare l'identificazione e la classificazione dei rischi a livello integrato e di sistema.

### IL MODELLO DEI RISCHI PROPOSTO

La prima parte del Modello identifica i **domini di rischio trasversali** a tutte le tipologie di realtà pubbliche italiane, ovvero:



#### RISCHI STRATEGICI

Rischi derivanti dal manifestarsi di eventi che possono condizionare e/o modificare in modo rilevante le strategie e il raggiungimento degli obiettivi dell'Ente. Possono avere origine esterna, ma anche interna.



#### RISCHI DI CONFORMITÀ

Rischi di mancata conformità a norme, regole o standard impartiti dal legislatore (comunitario, nazionale e locale), nonché a disposizioni e regolamenti interni all'Ente stesso (istruzioni, procedure etc.).



#### RISCHI OPERATIVI / DI PROCESSO

Rischi connessi alla normale operatività dei processi dell'Ente, che possono pregiudicare il raggiungimento di obiettivi di efficienza / efficacia, di qualità dei servizi erogati, di salvaguardia del patrimonio (pubblico e privato).



#### RISCHI DI REPORTING

Rischi connessi alla capacità di gestire in maniera efficace le attività di reporting verso gli organismi di controllo e di informazione / comunicazione verso l'esterno, nei confronti di tutti i portatori di interesse dell'Ente, coerentemente con gli obiettivi perseguiti dallo stesso.

La seconda parte del Modello invece si concentra sulle possibili **categorie di rischio specifiche** che ciascuna Organizzazione può declinare nel proprio Modello coerentemente con i propri ambiti di intervento peculiari, a seconda della tipologia di attività svolta.

Per una descrizione completa delle singole categorie di rischio incluse nel modello si rimanda all'Allegato 1.

## TAVOLO 2: L'ANALISI DEI RISCHI

### 1. DOMINI DI RISCHIO TRASVERSALI

*\*applicabili universalmente e declinabili ulteriormente in sotto-domini*

RISCHI STRATEGICI	
<ul style="list-style-type: none"> <li>• Politico</li> <li>• Legislativo</li> <li>• Scenario economico-finanziario</li> <li>• Evoluzione tecnologica</li> </ul>	<ul style="list-style-type: none"> <li>• Pianificazione strategica</li> <li>• Investimenti e patrimonio</li> <li>• Governance</li> <li>• Reputazionale</li> <li>• Eventi catastrofici</li> </ul>
RISCHI DI CONFORMITA'	
<ul style="list-style-type: none"> <li>• Normativa interna / esterna</li> <li>• Frodi e corruzione</li> <li>• Privacy e Security</li> <li>• Conflitto di interessi / abuso di potere</li> </ul>	<ul style="list-style-type: none"> <li>• Contrattualistica</li> <li>• Ambiente, salute, sicurezza</li> <li>• Trasparenza</li> <li>• Antiriciclaggio</li> </ul>
RISCHI OPERATIVI / DI PROCESSO	
<ul style="list-style-type: none"> <li>• Gestione risorse umane</li> <li>• Gestione sistemi informativi</li> <li>• Gestione vertenze legali</li> <li>• Soddisfazione dell'utenza</li> </ul>	<ul style="list-style-type: none"> <li>• Gestione progetti / programmi</li> <li>• Gestione economico-finanziaria</li> <li>• Qualità del servizio</li> <li>• Gestione approvvigionamenti</li> </ul>
RISCHI DI REPORTING	
<ul style="list-style-type: none"> <li>• Informativa strategica / di programmazione</li> <li>• Informativa economico-finanziaria</li> <li>• Misurazione delle performance</li> </ul>	

### 2. DOMINI DI RISCHIO SPECIFICI

#### RISCHI PECULIARI DI SETTORE

*Il Modello sarà di volta in volta integrato con categorie e domini di **rischio specifici e peculiari**, che ciascuna Organizzazione riterrà opportuno declinare, coerentemente con i propri ambiti di intervento e in base alle tipologie di attività svolte.*

## LE DIMENSIONI DA SVILUPPARE

Sulla base del confronto avuto nell'ambito dei Tavoli di Lavoro, è emerso come la situazione dei sistemi di Control Governance nella Pubblica Amministrazione italiana sia **estremamente variegata**, con l'adozione di modelli più o meno avanzati ma in **assenza di una visione coordinata** e di insieme.

Rispetto alle **esigenze di razionalizzazione e armonizzazione** delle diverse iniziative di gestione e controllo dei rischi in essere, avvertite da più parti come necessarie per l'evoluzione e il miglioramento generale dei sistemi di gestione e controllo degli Enti, sono stati identificati i seguenti **elementi** sui quali si ritiene necessario porre l'accento in ottica evolutiva:



### COMITATO DI AUDIT

Non essendo previsto un obbligo di legge in tal senso, risulta scarsamente presente nelle Pubbliche Amministrazioni un Comitato di Audit che, come precedentemente descritto, assuma un ruolo di coordinamento tra le strutture di controllo esistenti e che abbia una visione complessiva della governance e del sistema di gestione dei rischi in essere dell'Ente.

Le attività di compliance (spesso condotte da Funzioni differenti) risultano ad oggi focalizzate sull'esecuzione di controlli di conformità *ex post*, mentre appaiono poco implementati i controlli *ex ante*, a riflettere una diffusa concezione della compliance come prevalentemente dedicate alle attività di verifica e meno a quelle di presidio preventivo.

Analogamente, le attività di analisi e gestione dei rischi ad oggi svolte nelle Pubbliche Amministrazioni tendono a rispondere in maniera puntuale ad esigenze normative (*ad es. nel caso del rischio corruttivo*) che tuttavia sono spesso indipendenti l'una dall'altra. Da qui la tendenza alla proliferazione di attività di analisi specifiche, poco o per nulla armonizzate e coordinate, che penalizzano una visione organica del profilo di rischio dell'Ente.



### COMPLIANCE E GESTIONE DEI RISCHI



### FUNZIONE DI AUDIT INTERNO

Anche in questo caso, non essendo prevista per legge, la Funzione di Internal Audit risulta ad oggi poco sviluppata nel panorama delle Pubbliche Amministrazioni italiane. Tuttavia, anche in considerazione della numerosità degli attori e dei controlli previsti dalla normativa nazionale, la costituzione di tale Funzione potrebbe contribuire a salvaguardare l'Ente da una proliferazione potenzialmente incontrollata e scoordinata delle attività di controllo svolte.

## LE «REGOLE CHIAVE» DI UN MODELLO EFFICACE

I lavori fin qui svolti nell'ambito dei Tavoli di Lavoro hanno evidenziato la necessità, in un contesto come quello pubblico, altamente regolato da norme e principi di controllo vincolanti, di dotarsi di un Modello di Control Governance efficace, che individui in maniera chiara e formale non solo **i ruoli e le responsabilità** attribuite ai soggetti coinvolti, ma anche **i flussi informativi** in essere tra tali soggetti.

Se, da un lato, il Modello proposto può essere preso come riferimento per la definizione della Governance dell'Ente, dall'altro è comunque necessario tenere in considerazione le caratteristiche peculiari della specifica realtà in cui il Modello è adottato, ad esempio in termini di dimensione e complessità, al fine di garantire una efficace implementazione del sistema dei controlli interni.

A tal proposito, si forniscono alcune «**regole chiave**» che, a prescindere dalle specifiche scelte organizzative, possono fungere da principi ispiratori per il disegno, l'implementazione e il mantenimento di un efficace sistema di Control Governance.

1. **Analisi del sistema di Governance in essere**, con rilevazione dei diversi livelli di controllo esistenti, e con individuazione dei ruoli e delle responsabilità attribuite per la gestione e controllo dei rischi cui l'organizzazione è esposta.
2. **Definizione di un Modello di Control Governance**, che tenga in considerazione una struttura a tre linee di difesa, e che preveda (ove possibile):
  - I. *Identificazione / istituzione di strutture organizzative specificatamente deputate allo svolgimento di controlli di secondo livello in tema di **Compliance e Gestione dei rischi**.*
  - II. *Identificazione / istituzione di strutture organizzative specificatamente deputate allo svolgimento di controlli di terzo livello (**Audit Interno**), che diano assurance alla Dirigenza in merito all'efficacia del Sistema di Controllo Interno e diano supporto nella promozione di prassi migliorative.*
  - III. *Identificazione / istituzione di una struttura (**Comitato di Audit**) che abbia una visione complessiva del sistema di Control Governance in essere e che sia responsabile del coordinamento tra le strutture di controllo esistenti.*
3. **Definizione di metodologie e strumenti per l'analisi dei rischi**, in ottica integrata, per facilitare l'adozione di un «linguaggio comune» e l'introduzione di un **approccio sistemico** e di opportuni flussi di coordinamento e di comunicazione tra i diversi attori coinvolti, su tutte le iniziative di controllo e gestione dei rischi in essere.
4. **Implementazione di adeguati sistemi informativi** per la gestione nel continuo dei processi di gestione e controllo dei rischi, al fine di facilitare la condivisione delle informazioni tra i diversi attori coinvolti, e supportare i flussi di comunicazione e reporting agli organi di controllo e di vertice.

Le «**regole chiave**», così come sopra identificate, sono da considerarsi come **linee guida di alto livello** per la definizione di Modelli di Control Governance efficaci nella Pubblica Amministrazione italiana.

Da un **punto di vista operativo**, tali regole si traducono in specifiche attività, che saranno oggetto di analisi e approfondimento nel prosieguo dei lavori, e che si possono sintetizzare come di seguito (elenco esemplificativo e non esaustivo):

- Definizione di **idonei strumenti** organizzativi che definiscano le modalità di funzionamento e coordinamento (i) tra le strutture deputate al controllo interno e (ii) tra tali strutture e gli Organi Collegiali (es. mandato della Funzione di Audit interno, regolamento del Comitato di Audit, meccanismi di comunicazione e flussi informativi, etc.)
- Definizione di **specifici processi** per l'analisi, la valutazione e la gestione dei rischi, con l'obiettivo di armonizzare le iniziative esistenti e di facilitare un approccio di tipo integrato e sistemico (es. modelli e tassonomie comuni e univoche, metodologie e scale di valutazione, strumenti e flussi di reporting, etc.).

# IL LAVORO DEI TAVOLI 2020/2021

2° EDIZIONE

# TAVOLO RISTRETTO: LA RICOGNIZIONE E VALUTAZIONE DEL S.C.I.

In continuità con i lavori del Tavolo permanente sul Sistema di Controllo Interno nella Pubblica Amministrazione italiana, la cui descrizione è stata riportata nelle pagine precedenti, a partire dal mese di giugno 2020 il Tavolo si è nuovamente riunito in forma ristretta, vista l'emergenza pandemica contingente, per riprendere le attività di studio.

In coerenza con gli obiettivi che ORAC si era posto nel proprio piano di attività, il Tavolo ha inteso svolgere un approfondimento volto a **definire uno strumento di diagnosi, ispirato agli standard riconosciuti a livello internazionale**, per analizzare e valutare il livello di maturità del sistema di controllo interno delle organizzazioni pubbliche, oltre ad identificare i possibili ambiti di miglioramento di quest'ultimo.

Tra le varie metodologie presenti in letteratura, si è inteso individuare quale standard valutativo il **COSO REPORT**, Internal Control Integrated Framework aggiornato nel 2013, emanato dalla Treadway Commission, ossia l'insieme di Standard e Best Practice, riconosciute a livello internazionale, per la gestione dei sistemi di Controllo Interno, unitamente al **Capability Maturity Model**, descritti entrambi nelle pagine precedenti.

Per ottemperare all'obiettivo di creare un diagnostico in grado di valutare l'efficacia ed efficienza strutturata del Sistema di Controllo Interno, il Tavolo, sulla base delle ricognizioni fatte, ha ritenuto strutturare un **questionario COSO-based attorno ai 17 principi, riconducibili alle 5 componenti del SCI, adatto alla realtà pubblica**, quale strumento di indagine per il sistema di controllo interno oggetto di analisi.

Pertanto, le attività del Tavolo sono consistite dapprima **nell'analisi di ogni principio previsto dal COSO Report** e alla relativa revisione delle formulazioni per renderle maggiormente aderente al contesto pubblico italiano. Si riporta, di seguito, l'elenco dei principi «rivisti in chiave pubblica», risultato di tale attività di revisione:

## AMBIENTE DI CONTROLLO

1. L'Ente dimostra impegno per l'integrità e i valori etici
2. La Governance dell'Ente garantisce l'esercizio di una adeguata supervisione dello sviluppo e del funzionamento del Sistema di Controllo Interno
3. I ruoli e le responsabilità con riferimento al Sistema di Controllo Interno sono chiaramente definiti a tutti i livelli dell'organizzazione
4. L'Ente dimostra un impegno ad attrarre, sviluppare e trattenere persone competenti in linea con gli obiettivi di presidio del Sistema di Controllo Interno
5. L'Ente promuove la responsabilizzazione delle persone con riferimento al Sistema di Controllo Interno

## VALUTAZIONE DEI RISCHI

6. Gli obiettivi dell'Ente sono chiaramente definiti ed articolati a tutti i livelli dell'organizzazione
7. L'Ente identifica i rischi connessi al raggiungimento dei propri obiettivi e valuta le modalità con cui sono gestiti
8. L'Ente considera il rischio di frode nell'ambito delle attività di valutazione del rischio
9. L'Ente identifica e valuta i cambiamenti che potrebbero avere un impatto significativo sul sistema di controllo interno

## ATTIVITA' DI CONTROLLO

10. L'ente identifica, valuta e sviluppa le attività di controllo associandole ai rischi identificati
11. L'Ente seleziona e sviluppa attività di controllo generale sulla tecnologia
12. L'Ente implementa le attività di controllo attraverso politiche e procedure

## INFORMAZIONE E COMUNICAZIONE

13. L'Ente dispone di una base di informazioni completa e attendibile per supportare il funzionamento del Sistema di Controllo Interno.
14. L'ente comunica internamente le informazioni necessarie per supportare il funzionamento del controllo interno (inclusi gli obiettivi e le responsabilità)
15. L'ente comunica con parti esterne/terze parti le questioni che riguardano il funzionamento del Sistema di Controllo Interno

## MONITORAGGIO

16. L'ente esegue valutazioni continue per accertare se le componenti del controllo interno siano presenti e funzionanti
17. L'organizzazione valuta e comunica tempestivamente le carenze del controllo interno alle parti responsabili dell'adozione di azioni correttive, inclusi il senior management (Direttori) e la Giunta



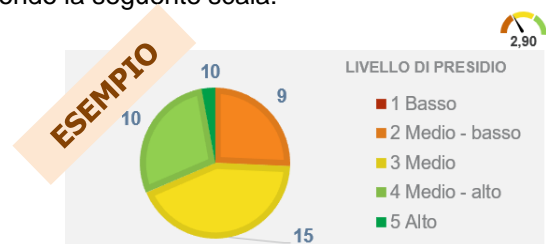
# TAVOLO RISTRETTO: LA RICOGNIZIONE E VALUTAZIONE DEL S.C.I.

Ispirandosi ai questionari di valutazione previsti dal COSO, il Gruppo di Lavoro ha elaborato **un questionario di 50 domande, riconducibili ai 17 principi enunciati dal COSO**. Per ciascuna domanda, il questionario è stato predisposto con l'obiettivo di rilevare:

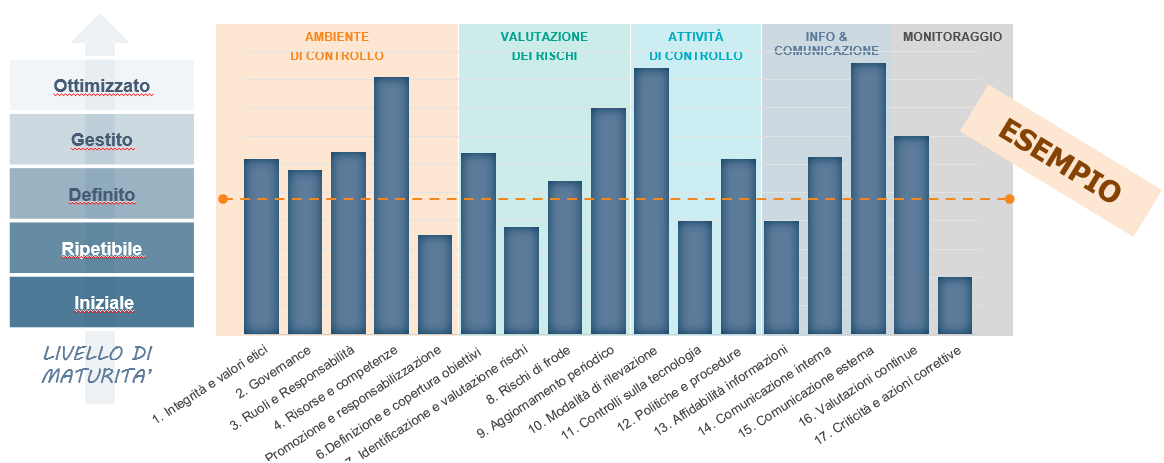
- la situazione generale del sistema di controllo interno dell'ente
- l'esistenza di presidi specifici sulle tre linee di difesa
- la presenza di eventuali punti di miglioramento, considerando la conformità normativa quale requisito necessario, e pertanto garantito a priori

Ogni singolo componente del Gruppo di Lavoro ha potuto esprimere la propria valutazione applicata al contesto di Regione Lombardia, sulla base delle informazioni raccolte e della propria sensibilità e/o giudizio professionale. Per ciascuna domanda, di fatto, è stata prevista la possibilità di fornire una **auto-valutazione di tipo qualitativo, sulla base di una scala da 1 a 5 indicativa del livello di adeguatezza dei presidi di controllo** percepito delle singole tematiche affrontate, secondo la seguente scala:

1. **presidio della tematica non adeguato** (Basso),
2. **gap significativi** (Medio-basso),
3. **presenza di qualche gap** (Medio),
4. **Possibili aree di miglioramento** (Medio-alto),
5. **presidio adeguato** (Alto).



La **sintesi per ciascun principio**, riportata nel seguente istogramma, espressa quale media delle singole valutazioni, **fornisce una rappresentazione del livello di maturità** (secondo il metodo del Capability Maturity Model): iniziale, ripetibile, definito, gestito od ottimizzato, secondo la seguente scala: **Fino a 1: livello di maturità "iniziale"; Da 1 a 2: livello di maturità "ripetibile"; Da 2 a 3: livello di maturità "definito"; Da 3 a 4: livello di maturità "gestito"; Da 4 a 5: livello di maturità "ottimizzato"**



La **combinazione delle valutazioni ottenute, insieme agli elementi qualitativi rilevati, hanno consentito di fornire una rappresentazione di sintesi del livello di maturità del sistema di controllo interno** nel suo complesso, e di identificare i possibili ambiti di miglioramento e migliori prassi da porre all'attenzione del decisore.

Si precisa che la finalità delle attività di auto-valutazione effettuate è stata quella di stimolare il confronto su una nuova metodologia di analisi. Pertanto, i risultati ottenuti in questa fase sperimentale non devono considerarsi espressione di un giudizio circa l'efficacia del sistema di controllo interno.

## TAVOLO RISTRETTO: LA RICOGNIZIONE E VALUTAZIONE DEL S.C.I.

Lo strumento diagnostico elaborato, e la sua successiva sperimentazione sul contesto di Regione Lombardia, rappresenta un elemento innovativo nel contesto pubblico italiano.

Il lavoro ha permesso di sviluppare una modalità di analisi «sistemica» svincolata dalle esigenze di conformità consentendo di raggiungere i seguenti risultati:



### RICOGNIZIONE PUNTUALE DEL SCI

Ricognizione puntuale e condivisa del Sistema di Controllo Interno regionale attraverso la mappatura di tutti i controlli e soggetti deputati al controllo. A seguito di tale ricognizione è stato possibile collocare ogni tipologia di controllo sul modello delle 3 Linee di difesa, alimentando concretamente il modello delineato nella prima edizione dei Tavoli.

Dall'analisi effettuata su ciascun elemento contemplato nel diagnostico emerge l'opportunità di validare le risultanze emerse e di identificare le iniziative prioritarie da attuare volte a valorizzare le best practices individuate e ad implementare azioni correttive, in coerenza con gli obiettivi di sviluppo del sistema di controllo interno regionale.

Di fatto si rende disponibile uno strumento che potrà essere utilizzato per monitorare la salute del sistema di controllo interno regionale utile anche ad identificare specifici elementi su cui apportare correttivi puntuali.



### INDIVIDUAZIONE DI AREE DI MIGLIORAMENTO E DI BEST PRACTICES



### APPLICABILITÀ ESTESA DELLO STRUMENTO

Lo strumento diagnostico è stato elaborato in maniera tale che possa essere reso fruibile, seppur in forma semplificata, da altre amministrazioni che valicano il perimetro della Giunta Regionale, ad esempio le organizzazioni del SIREG. Le caratteristiche della metodologia, inoltre, consentono l'applicazione anche su altre amministrazioni pubbliche

# IL LAVORO DEI TAVOLI 2022/2023

3° EDIZIONE

## PREMESSA

In continuità con i lavori del Tavolo permanente sul Sistema di Controllo Interno nella Pubblica Amministrazione italiana, la cui descrizione è stata riportata nelle pagine precedenti, a partire dal mese di gennaio 2022 il Tavolo si è nuovamente riunito ponendosi nuovi ambiziosi obiettivi per l'edizione 2022/2023.

La terza edizione dei Tavoli si è sviluppata lungo **due direttrici principali**:

- Applicazione della metodologia **«processi-rischi-controlli» e formalizzazione di una proposta pilota di mappatura processi e controlli**, circoscritta a un ambito ben definito del contesto di Regione Lombardia, in risposta ad un'esigenza emersa in sede di questionario COSO in relazione al principio 10 e in linea con il **Modello dei Rischi per la Pubblica Amministrazione italiana** delineato nell'ambito della prima edizione del Tavolo.
- **Estensione del questionario COSO agli enti del Sistema Regionale lombardo (SIREG)**, con la predisposizione di uno **strumento diagnostico semplificato**, calato sulle peculiarità del sistema e basato su un questionario a risposte chiuse, da somministrare ad ogni ente del SIREG mediante trasmissione informatica.

Nell'ambito di entrambe le attività è stata di fondamentale importanza la partecipazione al Tavolo dell'Organismo Regionale di Controllo (ORAC) e di alcuni enti afferenti al Sistema Regionale Lombardo, la cui **visione privilegiata sul contesto regionale** ha permesso da un lato di avere una puntuale ricognizione e classificazione del sistema dei controlli interni di Regione Lombardia, dall'altro di poter sperimentare il diagnostico di autovalutazione basato sui principi del COSO Framework.

### IL CONTESTO REGIONALE LOMBARDO

Regione Lombardia rappresenta una tra le poche realtà regionali ad aver avviato, sin dal 2014 (L.R. n. 17/2014), una riflessione interna circa l'efficacia del SCI al fine di superare la frammentazione legislativa e dare un assetto organico al sistema di controllo interno, oltre all'istituzione di una funzione centrale di Internal Audit. Il contesto lombardo si caratterizza per un sistema di rete tra enti dipendenti, aziende, agenzie e altri organismi della regione: il **Sistema Regionale, o SIREG**, che ritrova **nell'Organismo Regionale di Controllo (ORAC) un punto di riferimento per le attività di audit e di controllo interno**. ORAC, istituito nel 2018 con la L.R. n. 13/2018 è una funzione organizzativa in staff all'organo esecutivo con lo scopo di verificare il corretto funzionamento delle strutture organizzative della Giunta e degli enti del sistema regionale in merito a trasparenza, regolarità, efficacia del sistema dei controlli interni e supporto ai piani di prevenzione della corruzione.

La struttura organizzativa del SCI, articolata sul modello delle tre linee di difesa, si inquadra nel disegno organizzativo di Regione Lombardia: il ruolo di governo politico, previsto dal modello, può essere individuato negli organi esecutivi di governo e di indirizzo politico quali **la Giunta e il Consiglio regionale**. In questa prospettiva, l'ORAC svolge una funzione di supporto dal punto di vista tecnico ed attuativo della redazione, programmazione e controllo applicativo delle linee di indirizzo relative al sistema dei controlli e che relazioni direttamente all'organismo di governo (Giunta regionale), oltre che all'organismo legislativo-rappresentativo (Consiglio). L'ORAC può effettuare **istruttorie** di propria iniziativa e su segnalazione, svolgere **verifiche ispettive**, emettere **linee guida**, raccomandazioni e **formulare pareri in tema di SCI**.

# METODOLOGIA «PROCESSI-RISCHI-CONTROLLI» E MATRICE «PROCESSI-CONTROLLI»

La prima parte dell'edizione 2022/2023 del Tavolo è stata dedicata all'elaborazione di una metodologia «**processi-rischi-controlli**» e alla **formalizzazione di una proposta pilota di mappatura processi e controlli**, circoscritta a un ambito ben definito del contesto di Regione Lombardia.

## DESCRIZIONE DELLA METODOLOGIA

Nell'ambito della sperimentazione del Questionario COSO sul contesto di Regione Lombardia è emersa l'esigenza, in relazione al principio 10, («*L'Ente identifica, valuta e sviluppa le attività di controllo associandole ai rischi identificati*») di **sistematizzare la mappatura del complesso dei processi interni e dei relativi principi di controllo dell'Amministrazione regionale** – in particolare per quanto concerne la prima linea di difesa – facendo leva sulle mappature già disponibili, che sono state riviste, integrate, e validate. L'attività è in linea con il **Modello dei Rischi per la Pubblica Amministrazione italiana** delineato nell'ambito della prima edizione del Tavolo.

La metodologia «**Processi-rischi-controlli**» prevede l'identificazione dei controlli sulla base dei processi rilevanti dell'organizzazione, e dei rischi ad essi correlati, basandosi sull'assunto che i controlli interni sono più efficaci quando sono integrati nei processi e nelle procedure dell'organizzazione. L'approccio metodologico per formalizzare tale collegamento prevede di identificare i **processi chiave** che influiscono materialmente sugli obiettivi strategici ed operativi dell'Ente, **documentare input, attività e output** per ciascun processo analizzato, **individuare i rischi e identificare i punti di controllo** chiave, associando tali rischi ai processi in modo da ottenere una «Risk and Control Matrix».

Stante la complessità e la peculiarità del contesto regionale, caratterizzato dall'esistenza di leggi e regolamenti definiti di volta in volta con l'obiettivo di mitigare essenzialmente **il rischio di conformità normativa**, nelle sue diverse articolazioni, si è optato per applicare una **metodologia semplificata** dove la dimensione di rischio non è stata presa in considerazione in quanto considerata implicita in ogni Macroprocesso. Sono stati altresì analizzati i processi e i controlli associati al Macroprocesso preso in esame.

## L'APPROCCIO UTILIZZATO

Grazie al contributo attivo di Regione Lombardia e al documento predisposto nella scorsa edizione del Tavolo «Ricognizione e classificazione del sistema dei controlli interni di Regione Lombardia» è stato possibile **identificare i principali processi e controlli da attenzionare**. Per una più accurata strutturazione dell'output e per una maggior disamina delle attività e dei controlli, Regione Lombardia ha condiviso diverso materiale, in particolare Decreti Legislativi, Leggi Regionali e deliberazioni della giunta regionale della Lombardia (ad esempio decreti specifici sulle attività di controllo svolte da diversi attori, Delibera di costituzione Fondo accordi Competitività presso Finlombarda, ecc.)

In coerenza con la metodologia sopracitata e tenendo conto delle complessità del sistema regionale, l'approccio utilizzato è consistito nell'analizzare **uno specifico macroprocesso** («Erogazione finanziamenti») **con l'obiettivo di identificare** i principali componenti della **Matrice «processi-controlli»**, ovvero:

- Fase** (programmazione, selezione, attuazione, ecc.);
- Attività** (predisposizione avvisi, pubblicazione, istruttorie, valutazioni formali, pubblicazione, presentazione risultati, ecc.)
- Principali attori coinvolti** (DG, Nucleo di valutazione, Assessore, ecc.)
- Riferimento normativo**
- Presidi di controllo** (controllo di regolarità amministrativa sulle proposte di deliberazione della giunta regionale, verifica preventiva della conformità dei bandi, controllo ex art. D.Lgs. 33/2013, ecc.)
- Responsabili del controllo** (DG, RPCT, Direzione Affari Istituzionali, imprese, ecc.)
- Attributi del controllo** (rispetto della normativa anticorruzione - Legge 19/2012, rispetto della disciplina del sistema di controllo interno – Legge Regionale 4/6/2014 n. 17, ecc.)
- Output** (schede, pareri, checklist, ecc.).

# METODOLOGIA «PROCESSI-RISCHI-CONTROLLI» E MATRICE «PROCESSI-CONTROLLI»

## RISULTATI RAGGIUNTI

Ispirandosi alla metodologia sopra descritta si è inteso lavorare, all'interno del Tavolo, per la **creazione di una Matrice «Processi-controlli»** funzionale alla sistematizzazione della mappatura del macroprocesso preso ad esempio tra quelli afferenti alla Struttura di Audit regionale: «Erogazione finanziamenti». Il procedimento realizzato dal Tavolo si può riassumere come in figura:



La Struttura di Audit ha proceduto nella **ricognizione di tutti gli elementi sopra riportati** (fase, attività, ecc.) riferiti al macroprocesso «Erogazione finanziamenti» nell'ambito del bando «Fondo accordi di competitività», generando la mappatura di cui si riporta una schermata:

MACROPROCESSO	FASE	ATTIVITA'	PRINCIPALI ATTORI COINVOLTI	RIFERIMENTO NORMATIVO	PRESIDI DI CONTROLLO	RESPONSABILI DEL CONTROLLO	ATTRIBUTI DEL CONTROLLO	OUTPUT
Erogazione Finanziamenti: Bando Accordi di competitività	Programmazione	Approvazione legge regionale che individua le attività principali finanziabili sui capitoli dedicati dalla Legge di bilancio	Consiglio regionale	Legge regionale 19 febbraio 2014 - n. 11 Impresa Lombardia: per la libertà di impresa, il lavoro e la competitività	CONTROLLO SULL'IMPATTO DELLA LEGISLAZIONE descrizione: per tutti i progetti di legge proposti ogni anno dagli assessorati della Giunta regionale, si procede alla verifica del rispetto della tecnica legislativa e della qualità normativa, della conformità con le disposizioni e competenze statali, della compatibilità con i principi costituzionali, regionali e delle autonomie locali, nonché con la disciplina comunitaria (a cura dell'Unità Organizzativa Legislativo, Riforme istituzionale, Semplificazione normativa e Rapporti con il Consiglio regionale, anche avvalendosi del supporto del Comitato Tecnico-Scientifico legislativo istituito ai sensi dell'art. 8, comma 1, lett. b) della l.r. 20/2008)	Unità Organizzativa Legislativo, Riforme istituzionale, Semplificazione normativa e Rapporti con il Consiglio regionale	Rispetto dello Statuto d'autonomia della Lombardia	Scheda giuridica
Erogazione Finanziamenti: Bando Accordi di competitività	Selezione	Definizione dei criteri di selezione/indirizzi per l'attivazione del percorso volto alla definizione degli accordi	Giunta su proposta dell'assessore	Dgr N° X/ 1452 seduta del 28/02/2014 indirizzi per l'attivazione del percorso volto alla definizione degli accordi per la competitività in attuazione dell'articolo 2 comma 1, lettera a) della legge regionale n. 11 del 19.02.14	CONTROLLO DI REGOLARITÀ AMMINISTRATIVA SULLE PROPOSTE DI DELIBERAZIONE DELLA GIUNTA REGIONALE descrizione: i Direttori e i Dirigenti esprimono, congiuntamente, parere di regolarità amministrativa sulle proposte di atti da sottoporre al Presidente della Regione e alla Giunta regionale per l'approvazione. Potrebbero derivare segnalazioni al Sg e al Presidente ai fini dell'iscrizione all'odg della Giunta, della mancanza di passaggi obbligatori a sistema (rilascio pareri obbligatori, attestazioni di mancanza di oneri finanziari ecc), segnalazioni al Presidente delle proposte che non sono state adeguate da parte del proponente alle osservazioni in materia di bilancio e ragioneria.	DG Sviluppo Economico	Rispetto Disciplina del sistema dei controlli interni	Parere di regolarità amministrativa
					CONTROLLO DI REGOLARITÀ AMMINISTRATIVA SULLE PROPOSTE DI DELIBERAZIONE DELLA GIUNTA REGIONALE descrizione: si sostanzia nella verifica di regolarità dell'intero iter informativo; in particolare, il Segretario di Giunta verifica			

Infine, i lavori del Tavolo hanno avuto l'obiettivo di **informatizzare la mappatura** utilizzando una piattaforma di cloud computing che – se sviluppata ulteriormente – permetterà potenzialmente di **gestire in maniera agevole la complessità del procedimento**, e di **snellire i processi di verifica dei SCI**, potendo visualizzare velocemente, all'interno di un processo, i controlli che sono stati realizzati e quelli in sospeso.

Per il futuro, la metodologia identificata potrebbe essere applicabile al complesso dei processi interni all'amministrazione regionale, in quanto **facilmente estendibile su una serie di processi**, ad esempio quelli mappati nell'ambito della Legge n. 190/2012. Per replicare l'impostazione si renderebbe necessaria l'identificazione e l'**associazione dei rischi** alle attività e ai controlli (costruzione della RISK & CONTROL MATRIX, RCM) e **reiterare l'impostazione della piattaforma informatica** in modo agevole e veloce.

# L'ESTENSIONE DEL QUESTIONARIO COSO AGLI ENTI DEL SISTEMA REGIONALE

La seconda parte del Tavolo 2022/2023 ha avuto l'obiettivo di **estendere il questionario di autodiagnosi per la Valutazione del Sistema di Controllo Interno** elaborato nella precedente edizione **agli enti del Sistema Regionale lombardo (SIREG)**. Ciò è stato possibile anche grazie al coinvolgimento attivo nel Tavolo di ORAC e di molteplici strutture afferenti al SIREG, la cui visione privilegiata è stata fondamentale per la realizzazione dell'attività.

## DESCRIZIONE DELLA METODOLOGIA

Al fine di creare e perfezionare tale output per gli Enti del SIREG, il Tavolo ha lavorato di concerto e con il prezioso contributo di ARIA SpA e ATS INSUBRIA. A livello metodologico, il Tavolo ha elaborato prospetti ad hoc per ognuno dei principi analizzati all'interno dello strumento diagnostico al fine di predisporre un **questionario di autovalutazione "semplificato" per gli enti del SIREG**. Per ognuno dei principi, le domande sono state declinate in un linguaggio più chiaro per i principali attori coinvolti e con alcune precisazioni, considerando anche le tipizzazioni dei diversi enti del SIREG. All'interno del questionario sono state aggiunte – per ogni principio – legende ed approfondimenti relativamente alla legislazione a cui fare riferimento e precisazioni circa le modalità ed interlocutori coinvolti nella compilazione.

Una volta definito lo strumento «semplificato», il Tavolo ha svolto una prima fase di sperimentazione al fine di testarne l'efficacia, che ha coinvolto una società in house e un'Agenzia di Tutela della Salute (ATS).

La restituzione ha consentito di individuare gli elementi minimi per il presidio delle tematiche di controllo rilevanti e per la valutazione del SCI, e di **perfezionare la versione finale del questionario** strutturato secondo i principi previsti dal COSO Framework.

## RISULTATI RAGGIUNTI

Lo strumento di autovalutazione è stato quindi trasmesso dall'ORAC a tutti gli enti del SIREG, indirizzandolo ai Direttori Generali. L'invio del questionario è affiancato da una **lettera di presentazione** e da un'**appendice esplicativa della metodologia** utilizzata (il modello di control Governance delle «tre linee di difesa» delineato nel COSO report) per l'elaborazione del questionario contenente una serie di definizioni e indicazioni atte ad orientare il compilatore nel rispondere alle domande a risposta chiusa.

Tutti i 50 enti del Sistema regionale lombardo hanno compilato il diagnostico, che ha infatti ottenuto un **tasso di risposta pari al 100%** e ha permesso ad ORAC di avere un **quadro complessivo** del sistema dei controlli interni del SIREG in essere, individuando, in un'ottica di vigilanza collaborativa, **possibili azioni di sensibilizzazione** e supporto e/o fornendo indicazioni circa le **aree di miglioramento**. Dal punto di vista metodologico l'elaborazione dei dati dei questionari è avvenuta in forma aggregata, anonima e per tipologia di enti SIREG.

## GLI ESITI DEI QUESTIONARI

Si riporta nella pagina successiva una **sintesi dei risultati emersi dai questionari per ciascuna delle cinque componenti del COSO Framework**. Per maggiori dettagli si rimanda alla Deliberazione di ORAC n. 9/2023 con cui è stato approvato il documento "Relazione relativa agli esiti dei questionari di autodiagnosi, per la valutazione dei sistemi di controllo interno secondo "L'INTERNAL CONTROL INTEGRATED FRAMEWORK, C.D. COSO REPORT".

# L'ESTENSIONE DEL QUESTIONARIO COSO AGLI ENTI DEL SISTEMA REGIONALE

	PUNTI DI FORZA	POSSIBILI AREE DI EVOLUZIONE
AMBIENTE DI CONTROLLO	<ul style="list-style-type: none"> <li>• <b>Comunicazione</b> del codice di comportamento a tutti i livelli dell'Ente</li> <li>• <b>Responsabilizzazione</b> del personale attraverso la chiara attribuzione di deleghe e formazione specifica</li> <li>• Chiara definizione dei <b>ruoli e delle responsabilità</b> con riferimento al SCI</li> <li>• Chiara definizione degli <b>obiettivi</b> di controllo e dei <b>risultati attesi</b> da parte del Vertice</li> </ul>	<ul style="list-style-type: none"> <li>• Processi di analisi e valutazione in termini di:               <ul style="list-style-type: none"> <li>➢ <b>Dimensionamento</b> delle funzioni di controllo interno</li> <li>➢ <b>Competenze specifiche</b> necessarie</li> </ul> </li> <li>• Definizione degli <b>ambiti</b> di intervento delle funzioni di Internal Audit e relativa <b>obiettività / indipendenza</b> (con particolare riferimento agli Enti sanitari)</li> </ul>
VALUTAZIONE DEI RISCHI	<ul style="list-style-type: none"> <li>• <b>Identificazione dei rischi</b> connessi al raggiungimento degli obiettivi, e relative modalità di gestione</li> <li>• Riconoscimento di <b>fattori</b> che potrebbero impattare il SCI, <b>sia interni che esterni</b></li> </ul>	<ul style="list-style-type: none"> <li>• Evoluzione sistema di valutazione dei rischi in termini di <b>integrazione</b> e definizione <b>soglie di tolleranza</b></li> <li>• Partecipazione da parte del <b>Management</b> ai processi di valutazione dei rischi</li> <li>• Modalità e strumenti di <b>aggiornamento periodico</b> della valutazione dei rischi,</li> <li>• Analisi e valutazione del rischio di <b>frodi informatiche</b></li> </ul>
ATTIVITA' DI CONTROLLO	<ul style="list-style-type: none"> <li>• Considerazione dei rischi individuati in fase di <b>risk assessment</b> per le attività di controllo</li> <li>• Processo di gestione delle <b>policy e procedure</b> strutturato in cui si evincono ruoli, responsabilità e modalità</li> </ul>	<ul style="list-style-type: none"> <li>• Attività di controllo sui <b>sistemi informativi</b></li> <li>• Processo di analisi e verifica del principio di <b>segregazione dei compiti</b></li> <li>• Aggiornamento sistema procedurale</li> <li>• Monitoraggio periodico degli <b>esiti</b> dei controlli e della corretta applicazione delle <b>misure correttive</b></li> </ul>
INFORMAZIONE E COMUNICAZIONE	<ul style="list-style-type: none"> <li>• Disposizione delle <b>informazioni necessarie</b> per espletare in modo efficace i controlli (esiti di controlli passati, modifiche normative e organizzative, ecc.)</li> <li>• Presenza di <b>canali</b> che consentono di <b>comunicare informazioni</b> sul SCI agli stakeholders esterni rilevanti</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Flussi informativi</b> - da e verso le strutture di controllo - strutturati e supportati da adeguati sistemi informatici</li> <li>• <b>Canali e strumenti</b> per la condivisione delle informazioni rilevanti (intranet, cruscotti di monitoraggio, piattaforme, incontri periodici istituzionalizzati, ecc.)</li> </ul>
MONITORAGGIO	<ul style="list-style-type: none"> <li>• Definizione di processi per il <b>monitoraggio continuo</b> del corretto funzionamento del SCI</li> <li>• Verifica da parte del Vertice dell'attuazione dei <b>piani di azione</b> e coinvolgimento del management su eventuali <b>criticità o ritardi</b></li> </ul>	<ul style="list-style-type: none"> <li>• Modalità di valutazione e condivisione periodica delle risultanze con i soggetti controllati e con il Vertice</li> <li>• Evoluzione dei processi di monitoraggio con la combinazione di attività di <b>monitoraggio continuo e valutazioni puntuali</b></li> </ul>



# CONCLUSIONI

# UN BILANCIO PER LE ATTIVITÀ DEI TAVOLI DI LAVORO

A distanza di quasi tre anni dall'avvio del Tavolo di Lavoro, è possibile fare **un primo bilancio** di quanto ottenuto:



## BENEFICI DERIVANTI DALLA VISIONE D'INSIEME

L'approccio collaborativo e aperto delle strutture che hanno partecipato al percorso ha permesso di dare valore alle analisi effettuate: la capacità di riconoscere punti di forza e debolezza è una qualità determinante per l'efficacia del percorso. Inoltre, lo strumento individuato agevola una visione d'insieme del sistema, coinvolgendo tutti gli attori rilevanti, e pertanto è ritenuto molto utile per razionalizzare e fare ordine su tutte le iniziative. L'estensione del diagnostico agli enti del SIREG permette infatti di scattare una fotografia complessiva dello stato dei controlli interni al sistema, individuando, in un'ottica di vigilanza collaborativa, possibili azioni di sensibilizzazione e supporto e aree di miglioramento.



## PECULIARITÀ DEL MODELLO LOMBARDO

La realtà lombarda rappresenta il contesto ideale per sperimentare e ragionare criticamente sui modelli di control governance e lo sviluppo di nuove metodologie poiché Regione Lombardia vanta il primato tra le regioni italiane ad avere istituito la funzione di internal audit e successivamente istituzionalizzato un organismo assimilabile ad un Audit Committee quale è l'ORAC. Il coinvolgimento di questo Organismo e di molteplici strutture afferenti al SIREG nei lavori del Tavolo ha permesso di avere una visione privilegiata sul SCI e di estendere il questionario a tutti gli enti del Sireg, ottenendo un tasso di risposta pari al 100%.



## CENTRALITÀ DEL SISTEMA DI PREVENZIONE DELLA CORRUZIONE

Dalle analisi effettuate emerge lampante il ruolo pivotale del RPCT e delle procedure afferenti all'ambito anticorruzione nel sistema di controllo interno regionale



## APPLICABILITÀ DI MODELLI CONCETTUALI OGGI NON CONTEMPLATI NEL CONTESTO PUBBLICO

Il Modello dei Rischi per la Pubblica amministrazione italiana elaborato dal Tavolo in riferimento agli standard internazionali è stato il punto di partenza - nel contesto lombardo - per la formalizzazione di una proposta pilota di mappatura dei processi e dei controlli basata sulla metodologia «processi-rischi-controlli». I lavori del Tavolo hanno dunque consentito di spingerci oltre il confine tra ambito pubblico e ambito privatistico poiché si è dimostrato che taluni standard internazionali se opportunamente adattati al contesto e applicati con talune avvertenze metodologiche possono rilevarsi efficaci anche per il settore pubblico.



## NECESSITÀ DI INVESTIRE IN CULTURA, COMPETENZE E STRUMENTI

La cultura del controllo deve essere instillata nelle organizzazioni, abbandonando la percezione di mera attività ispettiva in favore di fattore abilitante ed innovativo del funzionamento delle stesse.

ALLEGATI

# ALLEGATO 1: GLOSSARIO DEI RISCHI

## RISCHI STRATEGICI

**Rischi derivanti dal manifestarsi di eventi che possono condizionare e/o modificare in modo rilevante le strategie e il raggiungimento degli obiettivi dell'Ente. Possono avere origine esterna, ma anche interna.**

### Legislativo

Rischio legato alla necessità di monitorare l'evoluzione normativa, primaria e secondaria (comunitaria e nazionale) che incide per numerosi aspetti sulle regole di esecuzione delle attività e può richiedere significativi aggiornamenti o adeguamenti di carattere operativo.

### Scenario economico-finanziario

Rischio legato ad avvenimenti nel contesto economico esterno (es. cambiamenti macro-economici, crisi economico-finanziaria) e all'andamento delle variabili di mercato (es. tassi d'interesse, valute), che possono incrementare i costi dell'indebitamento dell'Ente; esso potrebbe non disporre di adeguati strumenti per monitorare l'andamento del mercato finanziario e delle altre variabili economiche con possibili ripercussioni in termini di errate decisioni strategiche.

### Evoluzione tecnologica

Rischio connesso alla possibilità che l'Ente non colga le opportunità di implementazione delle innovazioni derivanti dall'applicazione di nuove tecnologie disponibili o scelga di utilizzare una tecnologia innovativa che potrebbe non rivelarsi quella più premiante.

### Pianificazione strategica

Rischio connesso alla definizione di obiettivi che si rivelino inadeguati, non realizzabili, incoerenti con l'interesse degli stakeholders o non raggiungibili anche a causa di errori o carenze di fondo nei processi decisionali alla base di scelte rilevanti, e che potrebbe esporre l'Ente a non cogliere opportunità di tipo strategico.

### Investimenti e patrimonio

Rischio connesso ad una gestione inefficiente / inefficace del patrimonio e degli investimenti da parte dell'Ente. Il rischio rileva anche in caso di errate decisioni in merito alle iniziative di investimento da intraprendere con conseguenze di tipo economico.

### Governance

Rischio legato alla possibilità che l'Ente non sia in grado di esercitare un'adeguata Governance ovvero di svolgere in maniera efficiente/efficace un'attività di monitoraggio e controllo.

### Reputazionale

Rischio legato al deterioramento della reputazione intesa come l'insieme di tutte le aspettative, percezioni ed opinioni sviluppate nel tempo nella collettività dove l'Ente opera, in relazione alla qualità dei servizi erogati, alle caratteristiche e ai comportamenti dei suoi dipendenti e ogni altra azione che comporti un'esposizione dell'Ente.

### Eventi catastrofici

Rischio legato al manifestarsi di eventi incontrollabili dovuti a catastrofi ambientali (ad es. terremoti, inondazioni, attentati terroristici etc.) che possono comportare dei danni temporanei e/o permanenti alle strutture aziendali e mettere a repentaglio la continuità dell'attività dell'Ente.

# ALLEGATO 1: GLOSSARIO DEI RISCHI

## RISCHI DI CONFORMITÀ

**Rischi di mancata conformità a norme, regole o standard impartiti dal legislatore (comunitario, nazionale e locale), nonché a disposizioni e regolamenti interni all'Ente stesso (istruzioni, procedure etc.).**

### Normativa interna / esterna

Rischio connesso alla possibilità che vengano compiuti atti contrari alle normative in vigore (comunitarie, nazionali, locali o disposizioni interne) con conseguente esposizione a contenziosi, sanzioni e danni reputazionali.

### Frodi e corruzione

Rischio connesso alla possibilità che soggetti esterni o soggetti operanti all'interno dell'Ente agiscano attraverso comportamenti fraudolenti pregiudicando l'attività o i risultati della stessa (il rischio comprende tutte le fattispecie di illecito, inclusa la corruzione soggetta alle specifiche prescrizioni derivanti dal DDL Anticorruzione).

### Privacy e Security

Rischio connesso alla possibilità che si agisca nel mancato rispetto della normativa in materia di Privacy / Sicurezza e Protezione dei dati personali (Regolamento UE 2016/679). Il rischio rileva anche in relazione a possibili violazioni di dati confidenziali (propri e di terzi) anche a seguito di episodi di *cyber attack*.

### Conflitto di interessi / Abuso di potere

Rischio legato alla possibilità che si configurino situazioni di conflitto di interesse ovvero che venga fatto utilizzo del potere in modo eccessivo, ingiusto (o, in *extrema ratio*, illegale), al di fuori dei limiti circoscritti e conferiti per lo svolgimento di una mansione, al fine di trarne dei vantaggi propri o per conto di terzi.

### Contrattuali- stica

Rischio connesso alla possibilità che vengano commesse irregolarità nell'ambito della gestione degli appalti pubblici (di fornitura, lavori pubblici, servizi, ecc), oppure al mancato rispetto, totale o parziale, di contratti, convenzioni oppure incarichi che regolano i rapporti con soggetti esterni all'Ente, incluse società partecipate (ad es. non ottemperanza degli impegni relativi alle modalità e tempistiche di erogazione dei servizi / fornitura di beni, dei pagamenti, omissione di adempimenti contrattuali, ecc).

### Ambiente, Salute e Sicurezza

Rischio connesso alla possibilità che si agisca nel mancato rispetto della normativa in tema di ambiente, salute e sicurezza sul luogo di lavoro, con possibili ripercussioni in tema di sanzioni e danni reputazionali / di immagine.

### Trasparenza

Rischio di non conformità alle previsioni normative in materia di trasparenza delle informazioni messe a disposizione dall'Ente, ad esempio tramite pubblicazione sul proprio sito web, con possibili ripercussioni in termini di sanzioni comminate all'Ente stesso.

### Antiriciclaggio

Rischio che vengano commesse irregolarità, ad esempio nell'ambito di concessioni, affidamenti o sovvenzioni, in violazione delle previsioni normative in materia di antiriciclaggio, con possibili ripercussioni in termini di sanzioni amministrative e responsabilità penali.

# ALLEGATO 1: GLOSSARIO DEI RISCHI

## RISCHI OPERATIVI / DI PROCESSO

**Rischi connessi alla normale operatività dei processi dell'Ente, che possono pregiudicare il raggiungimento di obiettivi di efficienza / efficacia, di qualità dei servizi erogati, di salvaguardia del patrimonio (pubblico e privato).**

*Tali rischi sono normalmente declinati in sotto-categorie in base a domini di rischio peculiari relativi a sotto-processi specifici.*

### Gestione Risorse Umane

Insieme di rischi connessi all'organizzazione e alla gestione delle risorse umane dell'Ente nell'ottica di raggiungimento degli obiettivi, e riguardano la capacità dell'Ente di disporre di personale adeguato e di processi interni idonei a garantire una corretta gestione e valorizzazione del capitale umano.

### Gestione Sistemi Informativi

Insieme di rischi correlati al verificarsi di situazioni, interne o esterne, che possono mettere a repentaglio la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione. Suddette situazioni possono essere causate anche dall'inadeguatezza ed dall'obsolescenza degli strumenti informatici impiegati (hardware) e/o alla scarsa funzionalità dei software, in termini di architettura del sistema, rapidità nei tempi di elaborazione dei dati, facilità di utilizzo, ecc.

### Gestione vertenze legali

Rischio connesso alla possibilità che i processi interni di gestione delle vertenze e controversie legali non siano adeguatamente presidiati e gestiti, con conseguenti ripercussioni in termini di possibili maggiori costi sostenuti, situazioni di possibile soccombenza con ricadute di natura economica ma anche reputazionale.

### Soddisfazione dell'utenza

Rischio connesso alla possibilità che l'Ente non sia in grado di misurare adeguatamente i bisogni e le aspettative dei cittadini / utenti del servizio e dei diversi stakeholder, in termini di soddisfazione per i servizi erogati, e conseguentemente di rispondere tempestivamente e in modo adeguato alle esigenze della collettività.

### Gestione progetti / programmi

Rischio connesso alla possibilità che una errata gestione di progetti / della programmazione delle attività svolte dall'Ente possa avere ripercussioni negative in termini economico-finanziari ovvero sulla qualità del servizio offerto agli utenti o ancora ricadute negative sulla reputazione dell'Ente stesso

### Gestione Economico- Finanziaria

Rischio legato alla capacità di gestire e monitorare attraverso idonei processi, le variabili finanziarie impattanti sui flussi di cassa dell'organizzazione necessario per lo svolgimento delle attività ed il raggiungimento degli obiettivi previsti.

### Qualità del Servizio

Rischio connesso alla possibilità che i processi interni non presidino adeguatamente la qualità delle attività svolte e dei servizi erogati, con conseguenti ripercussioni in termini di servizi non in linea con gli standard necessari e conseguenti danni alla reputazione e all'immagine dell'Ente.

### Gestione approvvigiona- menti

Rischio connesso alla possibilità che i prodotti e/o i servizi resi dai fornitori non siano in linea con le aspettative, le esigenze, gli standard e gli obblighi definiti contrattualmente. Il rischio rileva anche in caso di errate decisioni in merito alle valutazioni di economicità delle scelte operate ovvero alla presenza di situazioni di dipendenza da fornitori "chiave".

# ALLEGATO 1: GLOSSARIO DEI RISCHI

## RISCHI DI REPORTING

**Rischi connessi alla capacità di gestire in maniera efficace le attività di reporting verso gli organismi di controllo e di informazione / comunicazione verso l'esterno, nei confronti di tutti i portatori di interesse dell'Ente, coerentemente con gli obiettivi perseguiti dallo stesso.**

### Informativa strategica / di programmazione

Rischio connesso alla carenza o mancanza di informazioni del contesto interno e/o esterno di riferimento necessarie alla formulazione e al disegno della programmazione strategica ed in generale al corretto funzionamento dei processi direzionali. Il manifestarsi di questo rischio potrebbe privare i vertici del necessario quadro d'insieme per procedere a decisioni consapevoli nell'ambito della definizione degli obiettivi strategici o nell'ambito della pianificazione operativa.

### Informativa economico-finanziaria

Rischio legato alla possibilità che l'informativa economico-finanziaria (e.g. bilancio di esercizio e relativi allegati, reporting, prospetti entrate e spese) non sia in linea con i principi contabili di riferimento, oppure includa errori e/o omissioni di fatti significativi e rilevanti.

### Misurazione delle performance

Rischio riferito alla potenziale inadeguatezza ed inaffidabilità delle informazioni per la misurazione delle performance dei servizi erogati. Tale carenza informativa può precludere al management la possibilità di effettuare le necessarie valutazioni per migliorare i servizi erogati dall'Ente nonché di fornire un'adeguata informativa agli stakeholders.

# ALLEGATO 2: MAPPATURA DEI CONTROLLI



Controlli di III  
livello  
e valutazione  
del SCI

- ORGANISMO REGIONALE PER LE ATTIVITÀ DI CONTROLLO (ORAC)
- COLLEGIO DEI REVISORI DEI CONTI
- AUDIT INTERNO



Controlli di  
II livello

## CONTROLLO DELLA PERFORMANCE

- Controllo strategico
- Valutazione della performance
- Controllo di gestione
- Valutazione degli investimenti pubblici
- Controllo finanziario



Controlli esercitati  
su rischi  
specifici

- Controlli sulla gestione fondi UE \*
- Prevenzione della corruzione e trasparenza\*

- Attività anticiclaggio
- Protezione dati personali
- Sicurezza informatica
- Servizio prevenzione protezione (rspp)
- Sist. di controllo e gestione progr. Comunitario Feasr e Feaga ( PAC )

## CONTROLLO DI REGOLARITÀ

- Controllo di regolarità amm.va successivo sui decreti dirigenziali
- Controllo di regolarità iter amm.vo sulle proposte di deliberazione della Giunta
- Controllo di regolarità contabile
- Controllo del conto giudiziale degli agenti contabili
- Controllo sulla qualità della legislazione
- Controllo sull'impatto della legislazione
- Aiuti di Stato



Controlli sul SIREG

- Controlli sulle società *in house* e sugli enti regionali – controllo analogo
- Controlli sul Sistema Sanitario regionale
- Controlli su Aler

\* Strutture dotate di autonomia e indipendenza



Controlli di I  
livello

## CONTROLLI DI LINEA



# CONTRIBUTI E RINGRAZIAMENTI

---

Si desidera esprimere un sincero ringraziamento a tutti coloro che hanno contribuito alla realizzazione del presente lavoro, per gli stimoli forniti ed il tempo dedicato all'iniziativa.

Con riferimento all'Edizione 2022/2023 si desidera ringraziare:

## COMITATO PROMOTORE

- Regione Lombardia (*M.V. Fregonara Direttore Struttura Audit, E. Gasparini, Direttore U.O. Sistema dei controlli, prevenzione della corruzione e trasparenza*)
- Università degli Studi di Milano-Bicocca (*E. Guarini, F. Magli e M. Martinelli, Professori Associati di Economia Aziendale presso il Dipartimento di Scienze Economico-Aziendali e Diritto per l'Economia*)
- Protiviti Government Services (*A. Cencioni, A. Rista, V. Cattaneo, S. Gobetti*)

## PARTECIPANTI AI TAVOLI DI LAVORO

- Regione Lombardia (*M.V. Fregonara, E. Gasparini, L. Baldini, C. Barbaro, S. Bubba, M. Santarelli, L. Terlizzi*)
- Università degli Studi di Milano-Bicocca (*E. Guarini, F. Magli e M. Martinelli*)
- Protiviti Government Services (*A. Cencioni, A. Rista, V. Cattaneo, S. Gobetti*)
- Aria s.p.a. (*M. Bucco, F. Coda Canati*)
- Ats Insubria (*D. De Bernardi, S. Giotta*)
- ORAC (*S. Morello, S. Piazza*)
  
- *Si ringrazia per la partecipazione anche G. Fasano*

### **Regione Lombardia**

Piazza Città di Lombardia, 1  
20124 Milano

### **Università degli Studi di Milano-Bicocca, Dipartimento di Scienze Economico-Aziendali e Diritto per l'Economia**

Piazza dell'Ateneo Nuovo, 1  
20126 Milano

### **Protiviti Government Services**

Via Tiziano, 32  
20145 Milano