IL COMMERCIALISTA VENETO n. 256 - 2020

ASSOCIAZIONE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI DELLE TRE VENEZIE

INSERTO

CoSO Report I e *CoSO Framework SCIGR:* loro applicazione nella Revisione Legale e nel MOGC ex D. Lgs. 231/2001

Alberto Pesenato
ORDINE DI VERONA

CoSO Report I e *CoSO Framework SCIGR*: loro applicazione nella Revisione Legale e nel MOGC ex D. Lgs. 231/2001

Alberto Pesenato[1] - Ordine di Verona

Il documento CoSO Report I (1992: **5** principi e **23** protocolli) *è nato come presidio anticorruzione in capo ai responsabili delle unità operative mentre il successivo documento* CoSO Framework SCIGR (2013: **17** principi guida e **87** punti di attenzione) *ha spostato dai responsabili dei vari cicli operativi a CdA e Management la responsabilità primaria anti-corruttiva. Oltre ad illustrare sinteticamente i due documenti, si presentano cinque check list che accolgono i predetti principi guida e protocolli che assolvono anche ai dettami del P.R. ISA Italia 315. Sono di sicuro supporto nella determinazione del Rischio Intrinseco, elemento essenziale per definire il* Rischio di Revisione *e il* Rischio di Infrazione/Violazione *e fondamentale nella valutazione dei reati cosiddetti "di bilancio" ex D. Lgs. 231/2001.*

1. PREMESSA

Il principio di revisione ISA Italia 315, nelle *Regole* 13/24, nelle *Linee guida* 66/100 e nell'*Appendice 1*[2], illustra i cinque principi enunciati e definiti dai documenti ***CoSO Report I*** (1992) e ***CoSO Framework SCIGR*** (2013). Essi sono:

1. Ambiente di controllo;
2. Valutazione dei rischi;
3. Attività di controllo;
4. Informazione e comunicazione;
5. Monitoraggio.

2. IL DOCUMENTO CoSO REPORT I[3] (1992)

Il principio base di questo documento è che una attenta stesura con conseguente applicazione di procedure impostate dal management e gestite dai responsabili delle varie unità operative (tav.3) siano un valido baluardo contro il rischio di malversazioni o pratiche illecite e/o corruttive.
Negli Stati Uniti, come iniziativa delle Associazioni professionali più prestigiose d'America *(American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Institute of Internal Auditors (IIA), Institute of Management Accountants (IMA), Financial Executive Institute (FEI))* venne costituita la commissione di studio (***anticorruzione***) all'interno della *National Commission on Fraudolent Financial Reporting (NCFFR)*. Tale Commissione *anticorruzione* prese il nome di *(Commitee of Sponsoring Organizations of the Treadway Commission **CoSO**)*, successivamente nota come *Treadway Commission*, dal nome del suo presidente James C. Treadway Jr.
L'intento era di costruire una base di procedure aziendali riconosciuta come comune per combattere la corruzione, partendo dal presupposto che una solida progettazione e applicazione di procedure interne aziendali fosse baluardo di azioni corruttive.
L'Addendum italiano al documento ***CoSO Report I*** a pag. 141 così si esprime[4]: *«il controllo interno è definito come un processo svolto dal **personale di un'azienda** teso a conseguire obiettivi specifici. La definizione è estensiva in quanto raccoglie tutti gli aspetti del controllo di un'azienda e, tuttavia, consente una focalizzazione su obiettivi specifici. Il sistema di controllo interno è costituito da 5 componenti interconnessi, inerenti alle modalità di gestione dell'azienda da parte del suo management. I componenti sono collegati e servono come criteri per valutare l'efficacia del sistema»*.
A pag. 189 dello stesso Addendum: *«Il controllo interno è definito come un processo svolto dal **consiglio di amministrazione, dai dirigenti e da altri soggetti della struttura aziendale**, finalizzato a raggiungere una ragionevole sicurezza sul conseguimento degli obiettivi rientranti nelle seguenti categorie: efficacia ed efficienza delle attività operative; attendibilità delle informazioni di bilancio; conformità delle leggi e regolamenti in vigore»*.
Come già anticipato, il ***CoSO Report I*** (come anche il ***CoSO Framework SCIGR***) esemplifica le cinque componenti del controllo interno (gli stessi del P.R. ISA 315 sopra descritti):

1) Ambiente di controllo;
2) Valutazione dei rischi;
3) Attività di controllo;
4) Informazione e comunicazione;
5) Monitoraggio.

Il documento ***CoSO Report I*** comprende **2 livelli** di controllo:

---

[1] Autore dei manuali: "*Revisore Legale*" IX Edizione 2020 WKI Ipsoa e "*Organismo di Vigilanza*" VII Edizione 2019 WKI Ipsoa. Altri contributi sono disponibili nel sito www.albertopesenato.net e www.formazionerevisori.net
[2] "L'identificazione e la valutazione dei rischi di errori significativi mediante la comprensione dell'impresa e del contesto in cui opera" P.R ISA Italia 315
[3] Ora *CoSO Framework SCIGR* qui elaborato in opportune check lists.
[4] *CoSO Report I* «Il sistema di controllo interno» Addendum Italiano nei *23 principi guida* è considerato come *best practice* di riferimento per l'architettura dei sistemi di controllo interno dal *Serbanes Oxley Act* del 2002. Le procedure riferite ai *23 protocolli* sono ormai pratica comune nelle imprese (si dà per scontata la loro applicazione). Ritengo che gli ICQ (i Questionari sul Controllo Interno) proposti qui nella Tavola 3 s**oddisfino in modo appropriato** detti principi.

- ✓ 1° Livello: una serie di dettami che si derivano dai **5 principi** sopra descritti e si riferiscono alla ***corretta direzione e conduzione*** dell'azienda e concorrono alla determinazione del *Rischio Intrinseco* (qui Tav. 2);
- ✓ 2° Livello: **23 protocolli** che definiscono delle ***corrette procedure aziendali*** riferite ai vari cicli operativi la cui responsabilità ricade sui responsabili del ciclo stesso (qui Tav. 3).

È stato concepito, sin dalla sua prima edizione del 1992, come un modello integrato ovvero idoneo a stabilire un *Sistema di Controllo Interno* a presidio di tutti i rischi aziendali ***e come base per un sistema orientato all'anticorruzione***.

3. IL DOCUMENTO CoSO FRAMEWORK SCIGR (2013)

È doveroso premettere che il ***CoSO Framework SCIGR*** (2013) dà per scontate ed applicate le procedure indicate e pretese dal documento ***CoSO Report I*** e sposta sul **CdA** e la ***direzione (management)*** la responsabilità di eventuali malversazioni o pratiche corruttive e/o illecite. Il ***CoSO Framework SCIGR*** (2013) definisce il Sistema di Controllo Interno come "*un processo messo in atto dal **Consiglio di Amministrazione**, dal **management** e da **tutto il personale**, volto a fornire una ragionevole garanzia sul raggiungimento dei seguenti obiettivi: efficacia ed efficienza delle attività operative; attendibilità delle informazioni (interne ed esterne, finanziarie e non finanziarie); conformità alle leggi e alle norme vigenti cui l'impresa è soggetta*". La definizione sembra non differire di molto dal precedente documento (***CoSO Report I***), ma sono le *17 linee guida* e gli *87 punti di attenzione* che indicano la maggior responsabilità degli organi di *governance.* Il ***CoSO Framework SCIGR*** enfatizza l'importanza del giudizio del management sull'efficacia del sistema di controllo, attraverso la valutazione dell'implementazione e del funzionamento delle sue componenti. Il modello viene definito "*delle tre linee di controllo o di difesa*":

- ***La prima linea*** di controllo riguarda il management operativo, i cosiddetti *risk owner*; spetta a loro il compito di implementare ed eseguire i controlli di processo necessari alla gestione dei rischi nelle attività *day-to-day*.

- ***La seconda linea*** di controllo è composta dalle cosiddette funzioni di controllo, ossia da *funzioni aziendali caratterizzate da autonomia di giudizio e limitata indipendenza* che svolgono attività di monitoraggio dei rischi e dei controlli a supporto del *management* operativo (prima linea di controllo); tali funzioni possono essere molteplici in relazione al settore di attività e alla rilevanza del rischio quali, ad esempio, le funzioni di *risk management, compliance,* controllo di gestione, *security*, qualità, sicurezza sul lavoro, ecc. Si possono identificare nei *responsabili delle varie unità operative* (ciclo attivo, ciclo passivo, ciclo finanziario) che sono a presidio delle singole procedure e tutori dei **23** protocolli indicati dal documento **CoSO Report I**.

- ***La terza linea*** di controllo può essere rappresentata dalla funzione di *Internal Audit* (o anche Revisore, Collegio Sindacale, OdV ndr), che ha il compito di svolgere un monitoraggio indipendente, non potendole essere affidato alcun compito operativo, sull'adeguatezza del Sistema di controllo interno e di gestione dei rischi e di riferire direttamente al Consiglio di Amministrazione e/o al Vertice.

In tale complesso e articolato contesto diviene necessario per le imprese identificare un modello di *leading practice* al quale fare riferimento per sviluppare e valutare nel continuo l'adeguatezza del proprio SCI. Il documento ***CoSO Framework SCIGR*** propone ***17 principi guida*** e ***87 punti di attenzione***.

4. CoSO REPORT I E CoSO FRAMEWORK: PRINCIPI GUIDA E PROTOCOLLI

Vengono qui proposti in forma di check list (Tav. 2 e schemi successivi) i **40** principi guida (**23** protocolli del ***CoSO Report I*** più i **17** del ***CoSO Framework SCIGR***) indicati e sviluppati nei due documenti emanati dalla *Treadway Commission*.

Essendo Il documento ***CoSO Framework SCIGR*** un'evoluzione del documento ***CoSO Report I*** ho voluto inserire

- con numeri arabi i *17 principi guida*[5] del documento ***CoSO Framework SCIGR*** e
- con i numeri romani i ***XXIII*** protocolli del documento ***CoSO Report I***.

I ventitré (XXIII) protocolli del documento ***CoSO Report I*** si danno per scontati ed acquisiti (*pratica professionale*), ma ben si integrano con i diciassette (**17**) principi guida del documento ***CoSO Framework SCIGR***. In questo modo il professionista (revisore legale, sindaco, componente dell'OdV o altro organo di controllo) ha la possibilità concreta di utilizzare uno strumento unico e completo e che accoglie la *summa* della disciplina in materia. Il CNDCEC e la FNC nel documento del 12/5/2020 sul Covid 19[6] indicano i cinque principi come riferimento e forniscono applicazioni che qui non sono incluse in quanto si focalizzano solo i due documenti *CoSO*.

5. I DOCUMENTI CoSO REPORT I E CoSO FRAMEWORK SCIGR NELLA DETERMINAZIONE DEL RISCHIO INTRINSECO

Per determinare il Rischio di Revisione[7] il revisore legale, **dopo** aver stimato il *Rischio Intrinseco*, deve definire il *Rischio di Controllo*. In seguito, ponderando i due rischi, deve misurare il *Livello (Rischio) di Individuazione* e solo **successivamente** valuterà il *Rischio di Revisione*. Tale procedura sarà valutata contestualmente alle altre pretese dal *controllo della qualità* dagli ispettori del MEF. Per accertare il grado di *Rischio Intrinseco*, il revisore valuta numerosi fattori, quali ad esempio:

- l'integrità, l'esperienza e la competenza della Direzione e gli eventuali avvicendamenti nella sua composizione;
- le pressioni anomale sul management;
- la natura dell'attività svolta dalla società;
- i fattori che influenzano il settore nel quale opera la società;
- i singoli conti di bilancio che sono suscettibili di errori;
- la complessità delle operazioni effettuate o di altri eventi, che rendono necessario l'intervento di un esperto;
- il grado di soggettività connesso alla determinazione delle varie voci di bilancio;
- il grado di possibilità che i beni aziendali possano essere persi o soggetti ad appropriazioni indebite a causa del loro valore e perché

[5] Si sviluppano poi in 87 *punti di attenzione* che supportano il *management* nell'implementazione e nella conduzione del Sistema di Controllo Interno e nel valutare se i relativi principi sono di fatto presenti e funzionanti. Il principio è attuato nel caso in cui tutti o parte degli aspetti declinati nei *punti di attenzione* risultino efficacemente applicati

[6] CNDCEC e FNC – "Le procedure di revisione ai tempi del COVID 19: La resilienza del Sindaco Revisore" 12 maggio 2020 inserite nel manuale "Revisore Legale" IX edizione 2020 (CD 01) non sono riportate nelle check lists qui presentate.

[7] A differenza del Revisore l'Organismo di Vigilanza determinerà il Rischio Intrinseco al fine della valutazione del Rischio di Infrazione riferito ai reati cosiddetti "di bilancio" ex D. Lgs. 231/2001.

facilmente trasferibili;

- operazioni complesse o anomale poste in essere in prossimità della data di chiusura del bilancio;
- operazioni non rientranti nell'elaborazione ordinaria.

Per determinare il Rischio Intrinseco il revisore legale[8] utilizza alcune check lists tratte dai principi di revisione ISA Italia e dalla pratica professionale (qui Tav.1).

TAVOLA 1 - ***P.R. ISA Italia utili alla determinazione del Rischio Intrinseco*** *– principi etici del CdA e del management e organizzazione del SCI (Due metodi A e B)*

RISCHIO INTRINSECO **Determinazione finale della valutazione**		**B) Metodo del "Rischio Residuo"**	**A) Metodo Professionale o Critico**		
Check List	**Descrizione check list**	**%**	**Alto**	**Medio**	**Basso**
9.1	Documenti *CoSO Report I* e *CoSO Framework SCIGR*: Principi guida P.R. ISA Italia 315 App. 1 (corretta direzione e conduzione dell'azienda)				
9.2	Documento *CoSO Framework (SCIGR)*: P.R. ISA Italia 315 App. 1				
10.3	Antiriciclaggio P. R . ISA Italia 250				
10.4	Transazioni con le parti correlate P. R. ISA Italia 550				
10.5	Eventi successivi – P.R. ISA Italia 560				
10.6	Continuità aziendale - P. R. ISA Italia R. 570				
10.7.1	1) FaIsa informativa economico – finanziaria 2) Appropriazioni illecite di beni e attività dell'impresa - P.R. ISA Italia 240 App. 1				
10.7.2	Esempi di circostanze che indicano la possibile esistenza di frodi - P.R. ISA Italia 240 App. 3				
10.7.3	Condizioni ed eventi che possono indicare rischi di errori significativi P.R. ISA Italia 315 App. 2				
10.7.4	Corretta amministrazione e conformità alle leggi P.R. ISA Italia 250				
10.7.5	Possibili procedure di revisione in risposta a rischi identificati e valutati di errori significativi dovuti a frodi P.R. ISA 240 App. 2				
Descrizione Questionari I.C.Q. (Dossier Procedure)					
1.a	a) Conoscenza dell'attività aziendale P.R. ISA Italia 315				
A) Valutazione finale Rischio Intrinseco metodo "PROFESSIONALE O CRITICO" Sulla base dei risultati delle valutazioni sopra eseguite il Revisore Legale dia il Suo giudizio sul ***Livello*** Rischio Intrinseco complessivo (da riportare in ogni singolo ciclo)			**Alto**	**Medio**	**Basso**
B) Valutazione finale Rischio Intrinseco con il metodo del "RISCHIO RESIDUO" Sulla base dei risultati delle valutazioni sopra eseguite il Revisore Legale dia il Suo giudizio sull' ***indice*** di Rischio Intrinseco complessivo da 0 a 100% (da riportare in ogni singolo ciclo)			%		
Commento					
Completamento *Check lists* ed aggiornamento	20____	20____	20____	20____	
	20____	20____	20____	20____	

Le check lists qui proposte **hanno carattere pluriennale***, vanno compilate il primo anno ed aggiornate negli anni successivi, esse seguono il lavoro del Revisore per più anni e quindi vanno inserite nel nuovo Dossier Generale ad ogni revisione. Si potrà, in questo modo, monitorare l'evoluzione del Rischio Intrinseco nel tempo.*

Vengono qui proposti nella check list 9.1 i **17** *principi guida* indicati e sviluppati nel documento ***CoSO Framework SCIGR*** emanato dalla *Treadway Commission*. I **XXIII** protocolli del documento ***CoSO Report I*** qui riferiti alla gestione operativa del Controllo interno sono trattati diffusamente e nel dettaglio da tutti i Questionari sul Controllo Interno (ICQ) e integrati dai **30** *protocolli Covid 19* indicati dalla Fondazione

[8] Anche l'OdV nella determinazione del *Rischio di Infrazione*.

Nazionale Commercialisti e CNDCEC il 20/4/2020 e posti nei 5 principi qui analizzati.
Il documento ***CoSO Report I*** (1992) nei suoi **23** *Protocolli guida* nasce come presidio anticorruzione basato su un affidabile sistema di controllo interno. Il documento ***CoSO Framework SCIGR*** *(2013)* nei suoi **17** *principi guida* e **87** *Punti di attenzione* sposta su CdA e management la responsabilità primaria della gestione anti-corruttiva. Essi sono sviluppati in 5 check list che raccolgono i **40** *Principi guida* come utile strumento che assolve anche ai dettami del P.R. ISA Italia 315, Appendice 1.

TAVOLA 2 - ***Rischio Intrinseco (CoSO Report I – CoSO Framework SCIGR) e tabelle da 1 a 6***

VALUTAZIONE DEL RISCHIO INTRINSECO [9]			
Descrizione check list			
9.1	Documento *CoSO Framework SCIGR*: Principi Guida sulla corretta direzione e conduzione dell'azienda		
Valutazione finale Rischio Intrinseco metodo del "PROFESSIONALE O CRITICO" Sulla base dei risultati delle valutazioni sopra eseguite il Revisore Legale dia il Suo giudizio sul ***Livello*** Rischio Intrinseco complessivo		**Alto**	**Medio**	**Basso**
Valutazione finale Rischio Intrinseco con il metodo del "RISCHIO RESIDUO" Sulla base dei risultati delle valutazioni sopra eseguite il Revisore Legale dia il Suo giudizio sulla ***Percentuale*** di Rischio Intrinseco complessivo			

DOCUMENTO *CoSO FRAMEWORK* CHECK LISTS RISCHIO INTRINSECO – GENERALE – PRINCIPI GUIDA[10] ***ESERCIZIO 20__***					
Documento COSO FRAMEWORK		**ANNO 20__ Prima stesura**	**ANNO 20__ Aggiornamento**	**ANNO 20__ Aggiornamento**	**ANNO 20__ Aggiornamento**
		Data + sigla	**Data + sigla**	**Data + sigla**	**Data + sigla**
1	Ambiente di controllo				
2	Valutazione dei rischi				
3	Attività di controllo				
4	Informazione e comunicazione				
5	Monitoraggio				
6	Covid 19				
VALUTAZIONE GLOBALE del RISCHIO INTRINSECO Sezione Documento *CoSO Framework* - GENERALE Sulla base dei risultati delle valutazioni sopra eseguite il Revisore Legale dia il Suo giudizio sul Rischio Intrinseco **Commento**				ALTO	MEDIO	BASSO
Completamento *Check lists* ed aggiornamento		20____	20____	20____	20____	
		20____	20____	20____	20____	

Le check lists qui proposte ***hanno carattere pluriennale****, vanno compilate il primo anno ed aggiornate negli anni successivi, esse seguono il lavoro del Revisore per più anni e quindi vanno inserite nel nuovo Dossier Generale ad ogni revisione. Si potrà, in questo modo, monitorare l'evoluzione del Rischio Intrinseco nel tempo.*

Ogni risposta NO corrisponde generalmente ad un punto di debolezza o ad una mancanza del controllo interno, che può generare un commento da parte del sindaco/revisore.
Se una risposta NO non comporta un punto di debolezza, essa va adeguatamente giustificata

[9] Rischio Intrinseco / Inerente da riportare al punto 6.2 dell'Archivio Generale - qui Tav. 1
[10] I Questionari vanno completati una prima volta e puntualmente aggiornati negli anni successivi.
Fondazione Dottori Commercialisti e CNDCEC . 20/4/2020 - "Le procedure di revisione ai tempi del Covid 19" - Vedi anche Archivio Procedure la "Conoscenza dell'attività aziendale" Archivio generale e **Check list 10.7.1**.

1) Ambiente di controllo

	Descrizione	Sì	No	w.p.	Note e sigla
	CoSO Framework SCIGR				
1	**Principio n. 1** – L'organizzazione dimostra il proprio impegno rispetto ai valori etici e all'integrità;				
2	**Principio n. 2** – Il Consiglio di Amministrazione è indipendente rispetto al *management* ed esercita la propria supervisione sullo sviluppo e sull'implementazione del Sistema di controllo interno e di gestione dei rischi;				
3	**Principio n. 3** – Il *management* definisce, sotto la supervisione del Consiglio di Amministrazione, la struttura organizzativa, le linee di riporto, i livelli autorizzativi e le responsabilità funzionali al fine di perseguire gli obiettivi aziendali;				
4	**Principio 4** – L'organizzazione dimostra il proprio impegno ad attrarre, sviluppare e trattenere risorse competenti, in linea con il conseguimento degli obiettivi aziendali;				
5	**Principio n. 5** – L'organizzazione, nel raggiungimento degli obiettivi aziendali, ritiene i singoli individui responsabili per la parte del Sistema di controllo interno di propria competenza				
	CoSO Report I				
I.	Esiste ed è in uso presso l'azienda un Codice Etico e di Comportamento*?*				
II.	Gli organi di governance e la direzione comunicano in forma appropriata i principi del Codice Etico e di Comportamento riferiti al fatto che l'integrità dell'azienda non può essere oggetto di compromessi?				
III.	Gli Organi di governance e la direzione curano con l'adeguato impegno l'applicazione dei principi sopra descritti?				
IV.	Gli Organi di governance e la direzione tengono e divulgano il concetto di "Comportamento esemplare?"				
V.	Esistono direttive e principi di controllo interno ben definiti, per effetto dei quali si riscontra all'interno dell'azienda una consapevolezza diffusa dell'importanza dell'applicazione delle procedure di controllo interno?				
VI.	La competenza del personale dell'azienda è commisurata - Ai compiti assegnati? - alle responsabilità richieste?				
VII.	Lo stile con cui agiscono gli organi di governance e la direzione è appropriato? nella delega dei poteri e responsabilità? nell'organizzazione della struttura? Nella gestione del personale? Nel favorirne la crescita professionale dello stesso?				
VIII.	Gli Organi di governance e la direzione curano con l'adeguato impegno l'applicazione dei principi sopra descritti?				
	COVID - 19				
1 **2** **3** **4** **5**	Le norme di comportamento sono adeguatamente codificate, diffuse e comunicate tra i diversi livelli aziendali anche in fase di emergenza sanitaria? La società è dotata di un assetto organizzativo in grado di adeguarsi ai mutamenti del contesto di riferimento a seguito dell'emergenza sanitaria? Sono chiaramente definite le responsabilità e i compiti dei dipendenti aziendali in costanza di crisi da COVID-19? È garantito un adeguato livello di formazione del personale sugli aspetti critici connessi all'emergenza sanitaria? Sono implementate procedure di valutazione e monitoraggio delle competenze e dei risultati conseguiti dai dipendenti che lavorano in				

2) Valutazione dei rischi (risk assessment)

	Descrizione	Sì	No	w.p.	Note e sigla
	CoSO Framework SCIGR				
6	**Principio n. 6** – L'organizzazione esplicita con sufficiente chiarezza i propri obiettivi, consentendo l'identificazione e la valutazione dei rischi ad essi legati				
7	**Principio n. 7** – L'organizzazione identifica i rischi connessi al conseguimento degli obiettivi aziendali e ne determina le modalità di				
8	**Principio n. 8 –** L'organizzazione prende in considerazione potenziali frodi nel valutare i rischi di conseguimento dei propri obiettivi aziendali				
9	**Principio n. 9** – L'organizzazione identifica e valuta i cambiamenti che potrebbero avere impatti significativi sul Sistema di controllo interno				
	CoSO Report I				
IX.	Sono stati definiti gli obiettivi: Strategici a livello aziendale? Tattici per ogni singola attività? È stata accertata la loro coerenza?				
X.	I rischi generati esternamente ed internamente che potrebbero determinare il mancato raggiungimento degli obiettivi stabiliti: Sono stati individuati? Sono stati valutati?				
XI.	L'organizzazione prende in considerazione potenziali frodi nel valutare i rischi di conseguimento dei propri obiettivi aziendali				
XII.	I cambiamenti che potrebbero influenzare la capacità dell'azienda di raggiungere gli obiettivi prefissati: Possono essere facilmente individuati? Possono essere intraprese tempestive azioni correttive?				
XIII.	Gli indirizzi strategici e le procedure operative possono essere tempestivamente modificate di conseguenza?				
XIV.	L'organizzazione identifica e valuta i cambiamenti che potrebbero avere impatti significativi sul Sistema di controllo interno				
	COVID - 19				
1	Sono predisposti piani strategici finalizzati al raggiungimento degli obiettivi aziendali adeguati al contesto di crisi da COVID-19?				
2	L'impresa dispone di processi idonei ad identificare e valutare i rischi rilevanti a seguito dell'emergenza sanitaria?				
3	La direzione è in grado di stimare la significatività e la probabilità di accadimento dei rischi correlati agli obiettivi di informativa finanziaria da fornire a seguito dell'emergenza sanitaria?				
4	La direzione utilizza piani e processi di controllo della situazione finanziaria in grado di recepire il mutato contesto di riferimento?				
5	La direzione è in grado di individuare e valutare correttamente i rischi connessi all'emergenza sanitaria con impatto sull'informativa finanziaria?				
6	L'impresa è in grado di predisporre le migliori azioni in risposta ai mutati rischi identificati e valutati?				

3) Attività di controllo (control activities)

Descrizione		Sì	No	w.p.	Note e sigla
CoSO Framework SCIGR					
10	**Principio n. 10** – L'organizzazione definisce e implementa Attività di Controllo che contribuiscono a ridurre i rischi entro livelli accettabili6				
11	**Principio n. 11** – L'organizzazione definisce e implementa Attività di Controllo sulla tecnologia, per supportare il raggiungimento degli obiettivi aziendali;				
12	**Principio n. 12:** L'organizzazione declina le Attività di Controllo in politiche che definiscono i comportamenti attesi e in procedure che ne determinano le modalità operative di applicazione;				
	CoSO Report I				
XV.	Le attività di controllo per garantire la conformità alle linee di condotta ed alle direttive stabilite: In che forma sono state istituite? Sono operative? Nel caso di individuazione di rischi contingenti: esistono procedure atte a fronteggiarli?				
XVI.	Nel caso di individuazione di rischi contingenti: esistono procedure atte a fronteggiarli?				
XVII.	Esistono e sono applicate adeguate procedure di controllo per ciascuna de lle attività dell'azienda?				
	COVID - 19				
	Sono predisposti e rispettati chiari livelli di rappresentanza e procedure di autorizzazione nello svolgimento delle operazioni aziendali in costanza di emergenza sanitaria? Sono implementati sistemi di identificazione del personale che assicurino la sicurezza negli accessi alle differenti funzioni? Sono previsti sistemi di protezione dei dati, dei documenti rilevanti e dei beni aziendali anche da remoto? La direzione è in grado di adeguare politiche e procedure di controllo ai cambiamenti aziendali? È assicurato il rispetto di leggi, regolamenti, contratti e protocolli a seguito dell'emergenza sanitaria? Il personale preposto, a vari livelli, alla predisposizione della informativa finanziaria, è adeguatamente informato circa le eventuali variazioni delle strategie aziendali				

4) Informazione e comunicazione (information & communication)

Descrizione		Sì	No	w.p.	Note e sigla
CoSO Framework SCIGR					
13	**Principio n. 13** – L'organizzazione ottiene o genera e utilizza informazioni rilevanti e di qualità a supporto del funzionamento del Sistema di controllo interno e di gestione dei rischi;				
14	**Principio n. 14** – L'organizzazione comunica internamente le informazioni, compresi gli obiettivi e le responsabilità di controllo interno, necessarie a supportare il funzionamento del Sistema di controllo interno e di gestione dei rischi nel suo complesso;				
15	**Principio n. 15 –** L'organizzazione comunica con parti terze relativamente a questioni che interessano il funzionamento del Sistema di controllo interno e di gestione dei rischi;				

	CoSO Report I				
XVIII.	I sistemi informativi (I.T.) aziendali sono in grado: - di individuare e raccogliere le informazioni significative: Finanziarie Produzione Gestione entrate Gestione uscite Altro specificare Tali informazioni sono trasmesse a personale competente ed in forma che consenta di assolvere i compiti assegnati?				
XIX.	Il sistema di informazione interna dell'azienda: è efficace e quindi consente a tutti gli utenti di ottenere le informazioni appropriate allo svolgimento del proprio compito? la comunicazione avviene in modo chiaro in rapporto alle attese ed alle responsabilità dei singoli utenti? 1) sono predisposte di soddisfare l'esigenza di dar conto dei risultati?				
XX.	Il sistema I.T. adottato mette in condizione tutti gli utenti interessati ad ottenere informazioni complete? – - informazioni attendibili?				
	COVID - 19				
	• È assicurato un adeguato livello di comunicazione in remoto con tutte le funzioni aziendali? • Il sistema informativo è strutturato attraverso meccanismi che evidenzino anomalie e punti di debolezza del sistema di controllo interno in risposta ai rischi connessi all'emergenza sanitaria?				

5) Monitoraggio (monitoring activities)

Descrizione		**Sì**	**No**	**w.p.**	**Note e sigla**
CoSO Framework SCIGR					
16	**Principio n. 16** – L'organizzazione definisce, sviluppa ed esegue valutazioni continuative (*ongoing*) e obiettive (*separate*) per accertare che le componenti del controllo interno siano presenti e funzionanti;				
17	**Principio n. 17** – L'organizzazione valuta e comunica tempestivamente le carenze del Sistema di controllo interno ai soggetti responsabili di intraprendere le necessarie azioni correttive, incluso il *senior management* e il Consiglio di Amministrazione per quanto necessario e di competenza				
	CoSO Report I				
XXI.	Il monitoraggio del sistema di controllo interno è attuato da: Audit commetee Internal auditing Organo di Controllo Organo di Vigilanza Collegio Sindacale Revisore contabile Società di revisione Altro specificare Oltre agli organi di vigilanza sopra descritti Sono state introdotte ulteriori procedure di monitoraggio continuo o periodico del funzionamento del sistema di controllo interno**?** **Specificare**				

XXII.	Gli scostamenti dalle procedure vengono segnalati, per mezzo di lettera alla direzione, agli organi di governance competenti?				
XXIII.	Le politiche aziendali e le procedure vengono modificate per adeguarle all'evoluzione dell'azienda?				
	COVID - 19				
	L'impresa effettua valutazioni sul sistema di controllo interno a seguito degli effetti dell'emergenza sanitaria? La direzione è in grado di predisporre le azioni correttive necessarie? Sono predisposti ed implementati specifici controlli atti a fronteggiare rischi collegati a frodi connesse a nuovi scenari originati dalla diffusione dei provvedimenti a sostegno delle imprese afflitte dall'emergenza sanitaria				

6) Emergenza Covid 19

Descrizione		**Sì**	**No**	**w.p.**	**Note e sigla**
Accesso a programmi e dati					
1	Sono utilizzate procedure e regole che disciplinino l'accesso in rete dei dipendenti fuori dalle mura aziendali				
2	Sono presenti sistemi di autorizzazione all'accesso per il personale (anche da remoto				
3	I responsabili delle funzioni IT sono sottoposti ad adeguata formazione in tema di *privacy*, *smart working* ed accesso in *cloud*?				
Assetto *hardware* e *software*					
4	Le infrastrutture *hardware* sono gestite in modo da rendere identificabili strutture, sistemi operativi e utenti anche in caso di accesso da remoto?				
5	Sono utilizzati sistemi di protezione quali antivirus e controlli sulla rete?				
6	Sono implementati sistemi di ripristino e salvataggio dei dati in caso di malfunzionamenti *hardware* e *software*?				
Conservazione dati e salvataggio					
7	È stata incrementata la frequenza delle procedure di *backup in cloud*?				
8	Esistono dei report di sistema attraverso i quali monitorare e/o mitigare errori degli addetti alle operazioni contabili che operano in *smart working*?				

6. RISK APPROACH NELLA COSTRUZIONE DEL MOGC EX D. LGS. 231/2001

Tutte le check lists qui riassunte in Tav. 1, compresa la 9.1 riferita ai due documenti *CoSO* (qui tav. 2), essenziali per la determinazione del *Rischio Intrinseco*, sono valido aiuto all'*Organismo di Vigilanza* (OdV) nella costruzione del MOGC (Modello di Organizzazione Gestione e Controllo) e nel determinare gli stessi aspetti riferiti al *risk approach* per i reati ed illeciti così detti "di bilancio".

6.1 Illeciti e Reati "di bilancio" e «fuori bilancio»

La commissione di illeciti e reati può essere allocata in due particolari categorie:

a) Reati ed illeciti che sono rilevabili nelle scritture contabili come fatti di gestione artefatti ed occultati tramite espedienti ed accorgimenti basati su falsa documentazione, accordi fittizi ed altro.

b) Illeciti e reati che nulla hanno a che vedere con i fatti di gestione registrati nelle scritture contabili e nei prospetti di bilancio (*Financial Reporting*) ma che possono essere commessi ugualmente recando nocumento all'Ente od azienda.

Ecco che la metodologia applicata nel primo caso si sviluppa con l'*auditing* e la verifica delle procedure in essere (*as is analysis*), con la ricerca dei punti di debolezza nelle stesse determinando il *Rischio di Infrazione/Violazione*[12] con la successiva interruzione e chiusura delle falle.

[12] La metodologia adottata dall'OdV per la verifica della commissione di reati ed illeciti "di bilancio" parte dalla valutazione del *Rischio Intrinseco*, in seguito del *Rischio di Controllo* per le unità operative per individuare e valutare il *Rischi* o *Livello di Individuazione* per identificare (eventuale esistenza di transazioni *sensibili*/*illecite* **volute e significative**) infine il ***Rischio di Infrazione***. Esso si discosta dal Rischio di Revisione in quanto non si riferisce al fatto che i *saldi di bilancio* siano inesatti ma che essi possano contenere *importi sensibili* dovuti ad *operazioni illecite o illegali*.

6.2 Rischio Intrinseco, Rischio di Controllo, Livello di individuazione e Rischio di Infrazione/Violazione.

1) Rischio Intrinseco (corretta direzione e conduzione dell'azienda): anche nell'approccio di realizzazione del MOGC il professionista dovrà valutare il livello di conduzione e direzione dell'azienda (*IR Inherent Risk*) e le check list derivanti dai documenti *CoSO* nonché le altre che sottendono alla determinazione di ciò (**tav. 1**) sono certamente utili ed utilizzabili.
2) Rischio di controllo (divisione dei compiti e procedure ben definite, affidabili ed applicate): il ***Rischio di Controllo*** (*CR Control Risk*) è il rischio che esistano transazioni *sensibili* (illecite) **volute e significative**, che si verifichino in un conto o in una classe di operazioni individualmente considerate o sommate ad altre, non siano prevenute o comunque tempestivamente individuate e corrette dai sistemi contabile e di controllo interno.
L'OdV deve analizzare gli elementi caratteristici della società che possono influire sulla possibilità dell'esistenza di transazioni *sensibili* (illecite). L'OdV può assumere un *Rischio di Controllo* basso se decide di affidarsi al sistema di controllo interno dell'azienda. Questo avviene dopo aver completato i questionari (ICQ qui tav. 3) ed eseguito un attento *walk through* per ogni singolo ciclo.
L'OdV deve documentare nelle carte di lavoro:

a) la conoscenza acquisita dei sistemi contabile e di controllo interno;
b) la valutazione del *Rischio di Controllo*.

Tutto ciò è **preteso anche** dalle *linee guida di Confindustria* e dalla *circolare della GdF 83607 /2012* nel volume terzo da pag. 51.
Livello (Rischio) di Individuazione (*DR Detection Risk*) e **Rischio di Infrazione/Violazione**: dalla ponderazione del *rischio intrinseco* e del *rischio di controllo* l'OdV determina il (*rischio*) *livello di individuazione* e di conseguenza il ***rischio di infrazione/violazione*** (*DR Infringiment Risk*) riferito alla possibilità che nei fatti di gestione possano essere incluse delle operazioni sensibili (illecite o peggio). Questa metodologia è richiesta dalla circolare GdF 83607/2012 che nel terzo volume da pag. 69 la richiede espressamente.

TAVOLA 3 - ***ARCHIVIO PROCEDURE: QUESTIONARI SUL CONTROLLO INTERNO - ASSERZIONI***

Nome Azienda _____

Esercizio 200_

	Descrizione[1]	**Anno 20.. Prima preparazione _**	**Anno 20.._ Aggiornam.**	**Anno 20.._ Aggiornam.**	**Anno 20.._ Aggiornam.**
		Data + Sigla	*Data + Sigla*	*Data + Sigla*	*Data + Sigla*
1.	a) Conoscenza dell'attività aziendale b) Documento *CoSO Report I*				
1.1					
2.	a) Rischio di Revisione e guida ai programmi di revisione da adottare in riferimento al Rischio di Revisione e Poste di Bilancio. b) Altre informazioni organizzative				
2.1					
3.	Ciclo: Passivo - Spese – Debiti				
3.1	*Walk Through*				
4.	Ciclo: Attivo - Ricavi - Crediti				
5.	Ciclo: Produttivo - Magazzino				
6.	Ciclo: Finanziario – Cassa e Banche Tesoreria e Derivati				
7.	Ciclo: Risorse umane				
8.	Ciclo: Immobilizzazioni a) materiali b) immateriali				
9.	Ciclo I.T. (Information Technology)				
10.	Ciclo: Titoli e Partecipazioni				
11.	Ciclo: Debiti a lungo termine				
12.	Ciclo: Patrimonio netto				
13.	Ciclo: Fair value				
	Altre Voci del CICLO PASSIVO				
14	Ciclo: Marketing				
15	Ciclo: Omaggi – Spese di rappresentanza				
16	Ciclo: Consulenze e prestazioni professionali				
17	Ciclo: Sponsorizzazioni				
18	Ciclo: Liberalità e no profit				
19	Ciclo: Procedimenti giudiziali ed arbitrali				
20	Ciclo: Accordi transattivi				
21	Ciclo: Rapporti con la Pubblica amministrazione				
22	Ciclo: Autorizzazioni e concessioni				

	Altri Cicli				
23	Ciclo: Sicurezza sul lavoro				
24	Ciclo: Ambiente				
25	Controllo di gestione				
26 X	Conto Economico X in Archivio del Bilancio				

1 Il documento ***CoSO Report I*** (1992) nei *23 Protocoll* è considerato come *best practice* di riferimento per l'architettura dei sistemi di controllo interno dal *Serbanes Oxley Act* del 2002. Le procedure riferite ai *23 Protocolli* sono considerati pratica professionale comune nelle imprese (si dà per scontata la loro applicazione da parte dei responsabili e quadri delle varie unità operative). Ritengo che gli ICQ (i Questionari sul Controllo Interno) qui elencati **soddisfino in modo appropriato** detti principi guida.