LA COSTRUZIONE DI UN SISTEMA DI CONTROLLO INTERNO (IL CASO DELLE COMPAGNIE DI ASSICURAZIONE)

Dott. Werther Montanari
Direttore Audit di Gruppo
Società Cattolica di Assicurazione Soc. Coop.

Verona, 9 dicembre 2009

Il Sistema di Controllo Interno

- I principali gruppi aziendali hanno a lungo ricercato metodi efficaci per meglio governare le attività di cui sono responsabili.
- L'esperienza internazionale ha fornito uno schema per la valutazione dei Sistemi di Controllo Interni che porti ad una comune comprensione del concetto di "controllo" e di "sistema dei controlli" ed una condotta comune delle Autorità di Vigilanza nella valutazione dei medesimi.
- Il "**Co.s.o.'s Internal Control Integrated framework**" (cd. Co.s.o. Report) è la metodologia che illustra un modello di controllo virtuoso articolato in cinque elementi e una serie di principi per procedere una valutazione professionale degli stessi.
- In ambito finanziario, i contenuti e le considerazioni riportati nel Coso Report sono state recepite dal Comitato di Basilea e dal Codice di Autodisciplina di Borsa Italiana nonché dal Regolamento ISVAP n. 20.
- L'**ERM** è l'evoluzione del Coso articolato in otto fattori qualificanti che individuano le caratteristiche strutturali dei sistemi di controllo interno.

Committee of Sponsoring Organization of the Treadway Commission è un'associazione privata nata nel 1985 per studiare le cause che hanno condotto alla rappresentazione di un'informativa aziendale non veritiera e per sviluppare raccomandazioni su principi di etica imprenditoriale, controlli interni e corporate governance.

Dal Co.S.O. all'E.R.M.

COSO *

Il **controllo** è il processo (svolto dal consiglio di amministrazione, dai dirigenti e da altri soggetti della struttura aziendale) finalizzato a fornire una ragionevole sicurezza sul conseguimento degli obiettivi rientranti nelle seguenti categorie:

- Efficacia e efficienza delle attività operative
- Attendibilità delle informazioni di bilancio
- Conformità alle leggi e regolamenti in vigore

Enterprise Risk Management **

La gestione del rischio aziendale (*Enterprise Risk Management*) è un processo posto in essere dal consiglio di amministrazione, dai dirigenti e da altri operatori della struttura aziendale; utilizzato per la formulazione delle strategie in tutta l'organizzazione; progettato per individuare eventi potenziali che possono influire sull'attività aziendale, per gestire il rischio entro i limiti del "rischio accettabile" e per fornire ragionevole sicurezza sul conseguimento degli obiettivi aziendali.

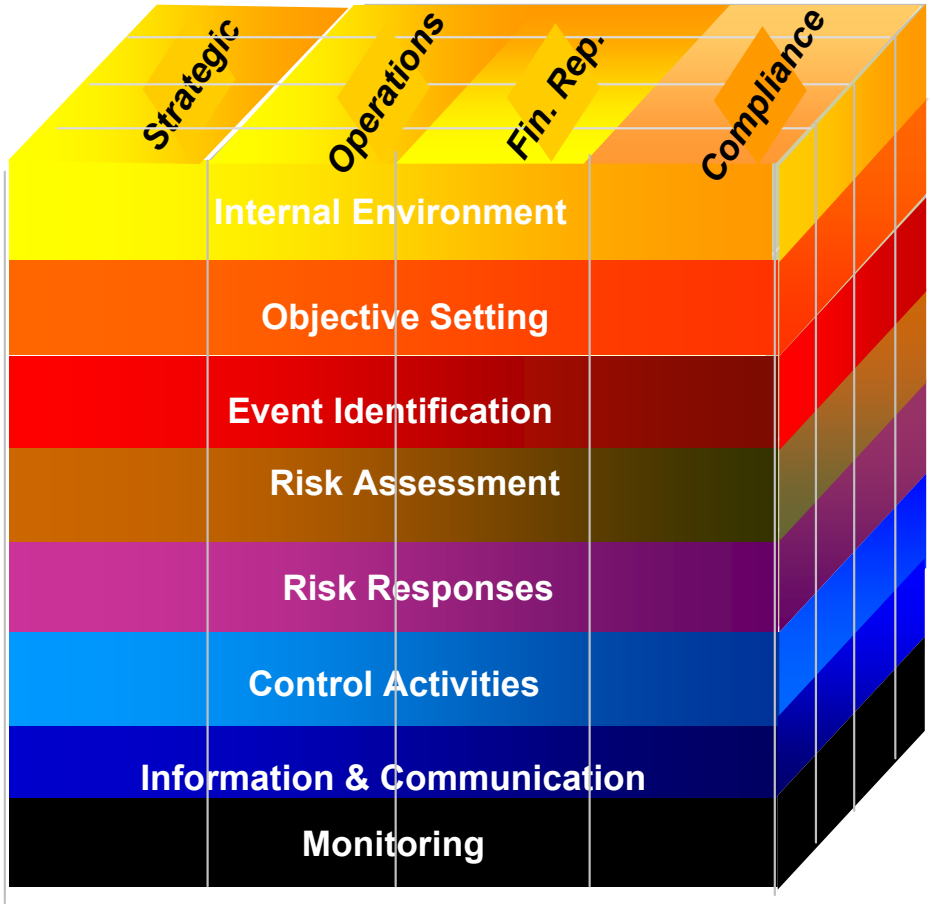
* PriceWaterhouse Coopers, *Il sistema di controllo interno,* ed. Il Sole 24 Ore

** Committee of Sponsoring Organization of the Treadway Commission, *Enterprise Risk Management*

Rappresentazione grafica

COSO – Internal Control Integrated Framework

COSO- Enterprise Risk Management (ERM)



Diritto societario

- La riforma del diritto societario (D. Lgs.n. 6/03 e succ. mod. e int.) ha innovato la nozione attribuita al sistema dei controlli societari in sintonia con la *best pratice* internazionale e nazionale in materia di governo societario.
- La trattazione organica da parte del legislatore (sotto il titolo "***dell'amministrazione e controllo***", capo V, libro V del Codice Civile) delle funzioni di amministrazione e controllo consente di codificare il contenuto della generale funzione di governo societario nei due specifici profili in commento.
- Il termine "*controllo*" nella nuova formulazione viene utilizzato con riferimento ad una funzione che investe la conduzione della società nel suo complesso e che, in varie guise, compete a tutti gli organi istituiti nei diversi sistemi alternativi ("tradizionale", "dualistico" e "monistico").

Nelle slides successive è contenuta una chiave di lettura del nuovo sistema di amministrazione e controllo disegnato dal legislatore italiano con riferimento al modello tradizionale.

Modello di amministrazione tradizionale

Un’ulteriore visione del modello tradizionale

GOVERNO SOCIETARIO

CONSIGLIO DI AMMINISTRAZIONE

Responsabile ultimo dello SCI:

deve garantirne la costante completezza,

funzionalità ed efficacia

Finalità di AMMINISTRAZIONE

Finalità di CONTROLLO

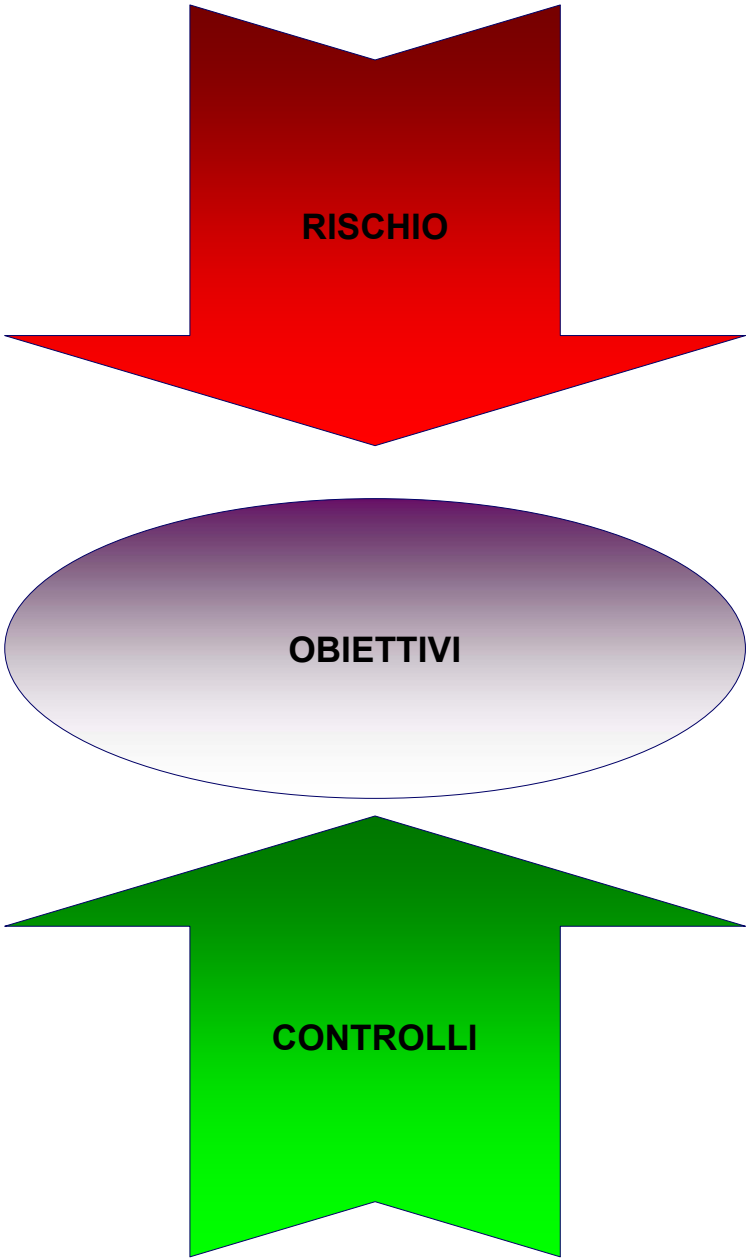
ORGANI DELEGATI

Responsabile dell’attuazione, mantenimento e monitoraggio dello SCI e della gestione dei rischi

COMITATO DI CONTROLLO INTERNO

Assistenza al CDA nella definizione delle linee di indirizzo del SCI

Definizione di rischio



Qualsiasi evento che possa influenzare negativamente il raggiungimento degli obiettivi aziendali, sino al punto da comprometterne la perfetta realizzazione

Gli obiettivi definiscono i risultati attesi

Il controllo è il mezzo mediante il quale gestire il rischio

Regolamento ISVAP n.20

Capo I – Disposizioni di carattere generale

Capo II – Sistema dei controlli interni

Capo III – Revisione interna

Capo IV – Gestione dei rischi

Capo V – Funzione di *compliance*

Capo VI – Disp. in materia di gruppo ass.vo

Capo VII – Obblighi di comunicazione all'ISVAP

Capo VIII – Disp. in materia di esternalizzazione

Capo IX – Disposizioni transitorie e finali

Capo II – Sistema dei controlli interni

Sezione I – Principi generali

Art. 4 (Obiettivi del sistema dei controlli interni)

Sezione II – Ruolo degli organi sociali

Art. 5 (Organo amministrativo)

Art. 6 (Comitato per il controllo interno)

Art. 7 (Alta direzione)

Art. 8 (Organo di controllo)

Art. 9 (Formalizzazione degli atti)

Sezione III – Componenti del sistema dei controlli interni

Art. 10 (Cultura del controllo interno)

Art. 11 (Attività di controllo e separazione dei compiti)

Art. 12 (Flussi informativi e canali di comunicazione)

Art. 13 (Funzione per la produzione di dati e informazioni ai fini della vigilanza supplementare)

Art. 14 (Sistemi informatici)

Obiettivi del sistema di controllo interno (art. 4)

*Le imprese di assicurazione si dotano di un'idonea **organizzazione amministrativa e contabile** e di un adeguato **sistema dei controlli interni**, proporzionati alle dimensioni e alla caratteristiche operative dell'impresa e alla natura e alla intensità dei rischi aziendali.*

PROPORZIONALITA'

Il sistema dei controlli interni è costituito dall'insieme delle regole, delle procedure e delle strutture organizzative volte ad assicurare il corretto funzionamento ed il buon andamento dell'impresa e a garantire, con un ragionevole margine di sicurezza:

a) l'efficienza e l'efficacia dei processi aziendali;

b) l'adeguato controllo dei rischi;

c) l'attendibilità e l'integrità delle informazioni contabili e gestionali;

d) la salvaguardia del patrimonio;

e) la conformità dell'attività dell'impresa alla normativa vigente, alle direttive e alle procedure aziendali.

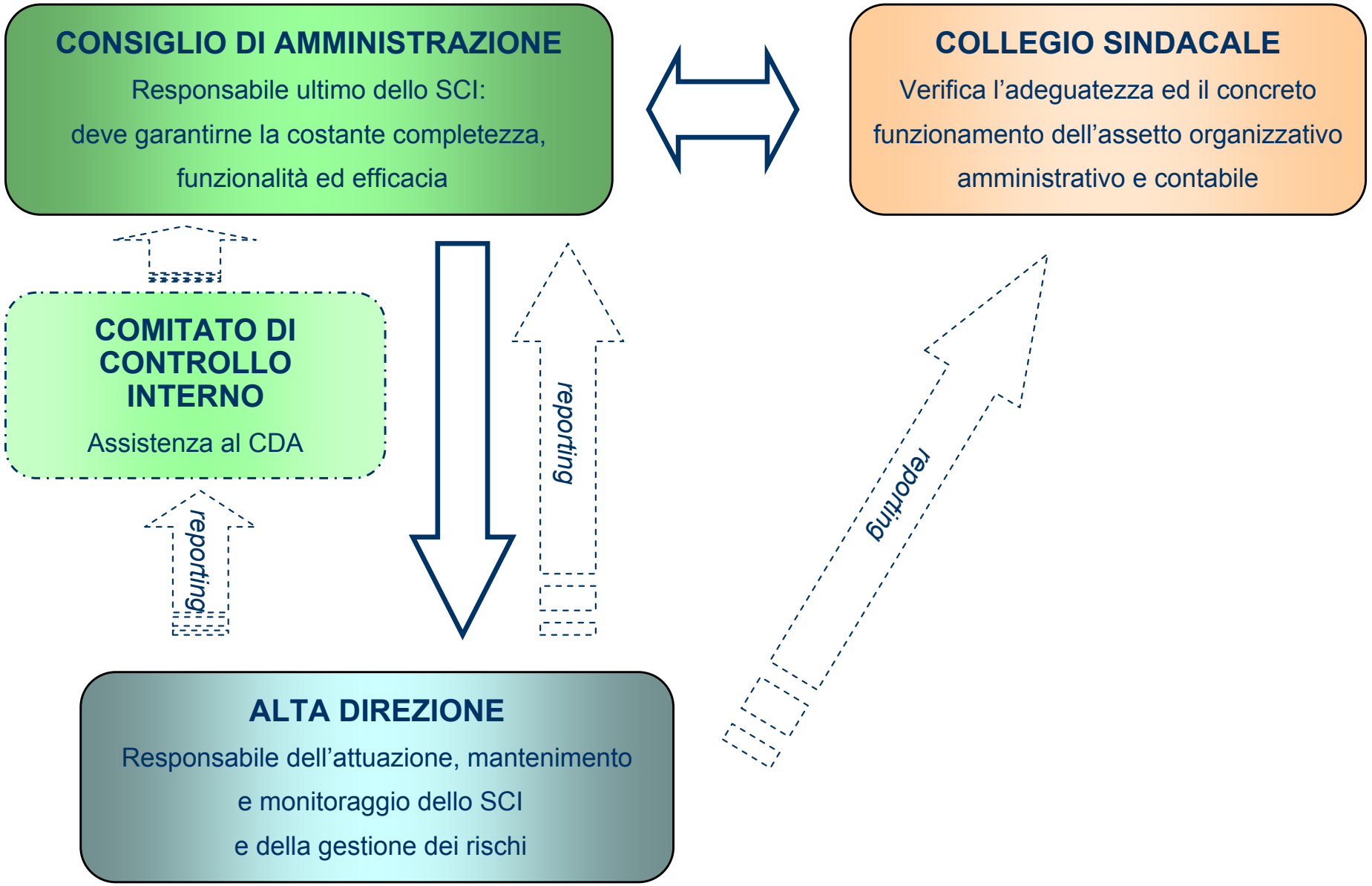
COSO

OPERATIONS

FINANCIAL REPORTING

COMPLIANCE

Ruolo degli organi sociali (sez. II)



Componenti dello SCI (sez. III e capi III e segg.)

ISVAP

Art. 10 Cultura del controllo interno

Art. 11 Attività di controllo e separazione dei compiti

Art. 12 Flussi informativi e canali di comunicazione

Art. 13 Funzione per la produzione di dati e informazioni

ai fini della vigilanza supplementare

Art. 14 Sistemi informatici

Capo III – Revisione interna

Capo IV – Gestione dei rischi

Capo V – Funzione di *compliance*

Capo VIII – Disposizioni in materia di esternalizzazione

COSO

AMBIENTE DI CONTROLLO
(control environment)

ATTIVITA' DI CONTROLLO
(control activities)

INFORMAZIONE E COMUNICAZIONE
(information & communication)

MONITORAGGIO
(monitoring)

VALUTAZIONE DEI RISCHI
(risk assessment)

MONITORAGGIO
(monitoring)

VALUTAZIONE DEI RISCHI
(risk assessment)

Ambiente di controllo

Definisce l'attitudine e la sensibilità del management all'azione di controllo. E' influenzato dalla storia e cultura aziendale e dai valori del sistema umano. I fattori caratterizzanti sono l'integrità e i valori etici, la competenza del personale, la filosofia e lo stile di management, la delega delle responsabilità, la politica organizzativa e il sistema motivazionale del personale, la legalità dei comportamenti e la leadership.

Art. 10

- L'organo amministrativo promuove un alto livello di integrità e una cultura del controllo interno.
- L'alta direzione è responsabile della promozione della cultura del controllo interno. A tal fine assicura la formalizzazione e l'adeguata diffusione tra il personale del sistema delle deleghe e delle procedure che regolano l'attribuzione di compiti, i processi operativi e i canali di reportistica.
- Le imprese adottano un codice etico che disciplini anche le situazioni di potenziale conflitto di interesse.
- Le imprese evitano politiche e pratiche di remunerazione che possano essere di incentivo ad attività illegali o devianti rispetto agli standard etico-legali.

Valutazione dei rischi

L'identificazione dei rischi presuppone l'individuazione degli obiettivi aziendali e degli eventi scatenanti. Le imprese si devono dotare di meccanismi che consentano di cogliere i rischi nonostante la continua evoluzione del proprio ambiente interno e di quello esterno. I rischi devono essere individuati, misurati in termini di probabilità e impatto, gestiti in ottica strategica e monitorati mediante tecniche di autovalutazione e di auditing.

Capo IV

- Le imprese si dotano di un adeguato sistema di gestione dei rischi, secondo proporzionalità, che consenta l'identificazione, la valutazione e il controllo dei rischi maggiormente significativi per il conseguimento degli obiettivi aziendali.
- Raccolgono in via continuativa informazioni sui rischi, interni ed esterni, esistenti e prospettici, documentandone il censimento. Per le fonti di maggior rischio, l'impresa predispone piani di emergenza.
- L'analisi è qualitativa o mediante metodologie di misurazione del rischio che includono, ove appropriata, la determinazione della perdita massima potenziale.
- Le imprese effettuano analisi prospettiche quantitative attraverso l'uso di *stress test.*
- Si dotano di presidi volti a prevenire il rischio di incorrere in sanzioni o perdite, anche reputazionali, a causa di violazioni di norme imperative o di autoregolamentazione.
- Le imprese istituiscono una funzione di risk management e una funzione di compliance secondo requisiti sanciti dalla normativa.
- L'organo amministrativo definisce la politica per l'esternalizzazione delle attività dell'impresa, in quanto fonte di rischio. Il ricorso all'outsourcing è consentito alle condizioni stabilite dalla norma.

Il processo di gestione dei rischi (Regolamento Isvap n. 20)

Regolamento n. 20 del 26 marzo 2008

CONSIGLIO DI AMMINISTRAZIONE

DEFINISCE e VALUTA

le strategie e le politiche di assunzione, valutazione e gestione dei rischi più rilevanti

FISSA E RIVEDE

almeno annualmente i livelli di tolleranza al rischio sulla base delle risultanze dei processi di individuazione e valutazione

IMPRESA ASSICURATIVA

ALTA DIREZIONE

ATTUA

le strategie e le politiche di assunzione, valutazione e gestione dei rischi, **ASSICURANDO:**

- la definizione dei limiti operativi
- la verifica tempestiva dei limiti
- il monitoraggio delle esposizioni ai rischi
- il rispetto dei livelli di tolleranza

IMPRESA

INDIVIDUA E VALUTA I RISCHI

- qualitativamente

-con metodologie di misurazione dell'esposizione ai rischi (inclusa la massima perdita potenziale)

PIANI DI EMERGENZA

RISK MANAGEMENT

CONCORRE alla definizione dei limiti operativi
FISSA le procedure per la verifica dei limiti
VALIDA i flussi informativi necessari per il monitoraggio delle esposizioni ai rischi
RIFERISCE dell'evoluzione dei rischi e della violazione dei limiti operativi

STRESS TEST

Rilevazione e valutazione qualitativa dei rischi operativi

Scheda di rilevazione qualitativa dei rischi

Scheda di rilevazione rischi

Area: Vita

Canale: Banche/Agenti

Business Chain: Sviluppo prodotti/Gestione comm./ Assunzione/Post vendite/Liquidazione

Processo: .....

CPE: .....

Data rilevazione: .....

Process/Risk Owner: .....

Referente di processo: .....

					Valutazione rischio lordo				Valutazione rischio netto				Valutazione rischio post mitigazione		
Attività	Classificazione rischio	Tipo rischio	Descrizione	Risk owner	Frequenza/ probabilità di accadimento	Impatto Potenziale	SCORE	Attività di controllo	Frequenza/ probabilità di accadimento	Impatto Potenziale	SCORE NETTO	Attività di mitigazione	Frequenza/ probabilità di accadimento	Impatto Potenziale	SCORE M

Esemplificativo

Attività di controllo

Consistono nell'applicazione delle politiche e procedure che garantiscono al management l'attuazione delle direttive impartite. Esse assicurano l'adozione dei provvedimenti necessari per far fronte ai rischi che possono compromettere il raggiungimento degli obiettivi aziendali. Si attuano in tutti i livelli gerarchici e funzionali della struttura organizzativa. Sono di tipo preventivo, concomitante o successivo; manuali o automatiche; fisiche o mediante indicatori.

Art. 11

- Lo SCI prevede l'esecuzione, a tutti i livelli dell'impresa, di attività di controllo che contribuiscono a garantire l'attuazione delle direttive aziendali e a verificarne il rispetto.
- Le attività di controllo sono proporzionate alle dimensioni, natura e complessità degli affari.
- Sono formalizzate e riviste su base periodica.
- Coinvolgono tutto il personale.
- Comprendono meccanismi di doppie firme, autorizzazioni, verifiche e raffronti, liste di controllo e riconciliazioni dei conti; accessi limitati alle operazioni, registrazione e verifica periodica delle operazioni effettuate.
- Le imprese assicurano un'adeguata separazione dei compiti nell'ambito delle funzioni aziendali

Segregation of duties

Informazione e comunicazione (1)

Le informazioni permettono al management di valutare l'andamento della gestione e di intraprendere eventuali azioni correttive. Le informazioni pertinenti devono essere identificate, selezionate e diffuse nella forma e nei tempi che consentano a ciascuno di prendere le proprie decisioni e di assumersi le proprie responsabilità. Di fondamentale importanza sono i sistemi informativi che producono rapporti contenenti dati contabili, operativi e di rispetto degli obblighi legali e regolamentari, coadiuvando il management nella gestione e nel controllo dell'attività aziendali. Nella progettazione dello SCI le informazioni devono essere complete, aggiornate, tempestive, accurate ed accessibili. Il personale aziendale deve avere una conoscenza dettagliata dei controlli che deve porre in essere e delle responsabilità connesse al mancato o errato controllo. Devono essere attivati meccanismi interni di segnalazione di presunte violazioni o malfunzionamenti dello SCI.

Art. 12
e segg.

- Le imprese devono possedere informazioni contabili e gestionali che garantiscano adeguati processi decisionali e consentano di definire e valutare se siano stati raggiunti gli obiettivi strategici fissati dall'organo amministrativo in modo da sottoporli ad eventuale revisione.
- A tal fine, l'alta direzione assicura che l'organo amministrativo abbia una conoscenza completa dei fatti aziendali rilevanti, anche attraverso la predisposizione di un'adeguata reportistica.
- Le imprese istituiscono e mantengono canali di comunicazione efficaci sia all'interno, in ogni direzione, sia all'esterno.
- Il sistema delle rilevazioni contabili e gestionali interne registra correttamente i fatti di gestione e fornisce una rappresentazione corretta e veritiera della situazione patrimoniale, finanziaria ed economica dell'impresa e in conformità con le leggi e la normativa secondaria.
- Il sistema deve favorire le segnalazioni di criticità anche attraverso la previsione di modalità che consentano al personale di portare direttamente all'attenzione dei livelli gerarchici più elevati le situazioni di particolare gravità.

Informazione e comunicazione (2)

- l'organo amministrativo approva un piano strategico sulla tecnologia della informazione e comunicazione (ICT), volto ad assicurare l'esistenza e il mantenimento di una architettura complessiva dei sistemi altamente integrata dal punto di vista applicativo e tecnologico e adeguata ai bisogni dell'impresa;
- gli ambienti di sviluppo e di produzione sono separati;
- le procedure per l'approvazione e l'acquisizione dell'*hardware* e del *software*, nonché per la cessione all'esterno di determinati servizi, sono formalizzate;
- sono adottate procedure che assicurino la sicurezza fisica dell'*hardware*, del *software* e delle banche dati, anche attraverso procedure di *disaster recovery* e *back up;*
- sono adottate e documentate procedure e standard operativi orientati alla individuazione e gestione degli eventi che possono pregiudicare la continuità del *business;*
- l'impresa predispone un piano di integrazione dei sistemi informatici nel caso di operazioni straordinarie nel quale sono specificati i sistemi, le tempistiche e i presidi organizzativi.

- per la produzione di dati e informazioni ai fini della vigilanza supplementare, le imprese istituiscono efficaci flussi informativi, procedure di controllo e individuano speicifica funzione aziendale.

Monitoraggio

Il monitoraggio garantisce nel tempo l'efficacia e l'efficienza dello SCI. Si articola in tre livelli:

1°) controllo operativo è l'attività di supervisione continua svolta dal personale nello svolgimento delle mansioni e svolta dalla linea gerarchica

2°) controllo sulla gestione del rischio è l'attività svolta dalle funzioni di risk management e compliance

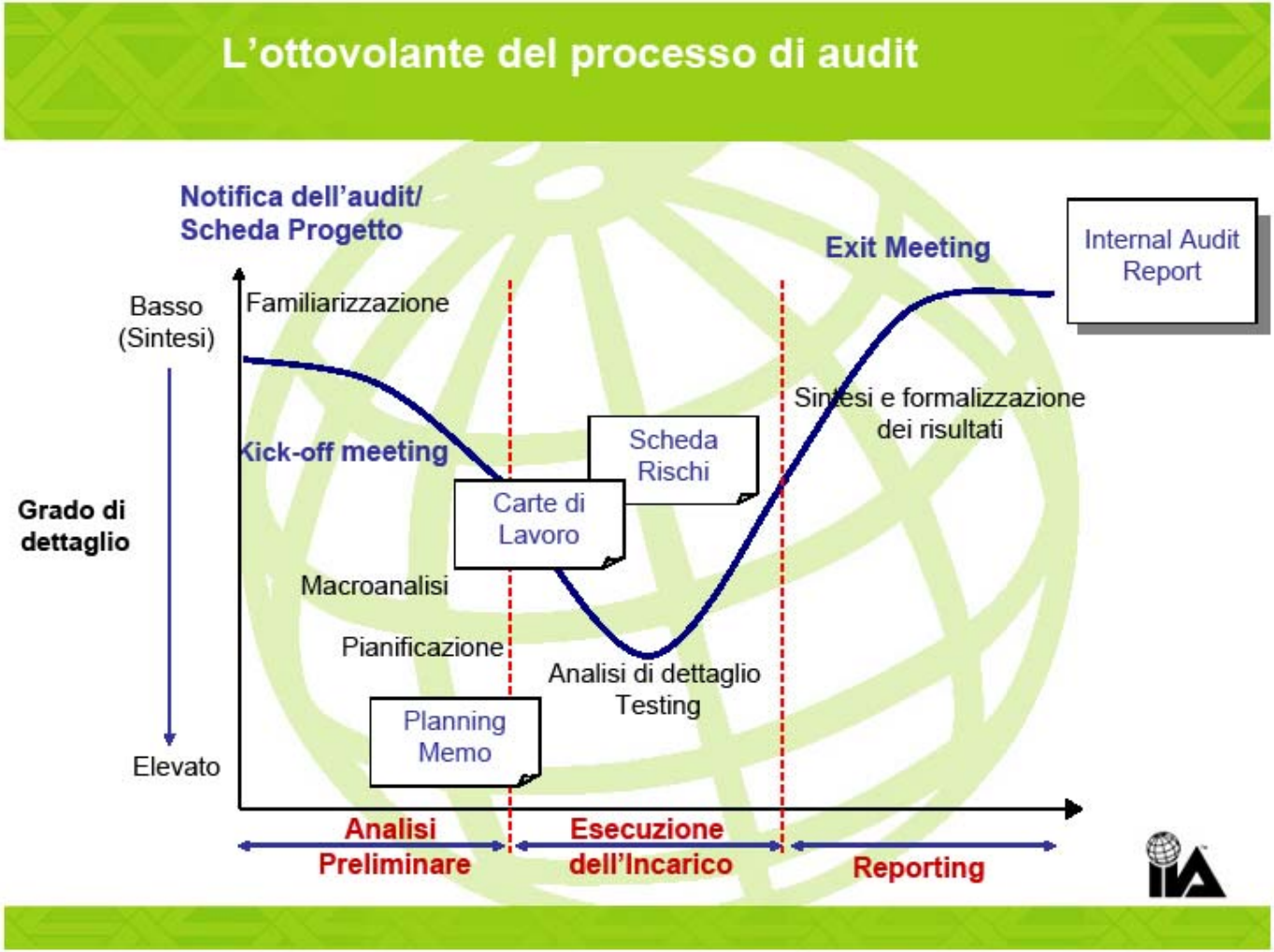
3°) controllo della revisione interna consiste in valutazioni periodiche svolte su base campionaria

La revisione interna deve capire come sono state analizzate a livello strategico le coppie "rischio/attività" e valutare se le contromisure sono adeguate rispetto alla scelta strategica. Valuta la funzionalità dei controlli di 1° e 2° livello in funzione del perseguimento della stretegia aziendale.

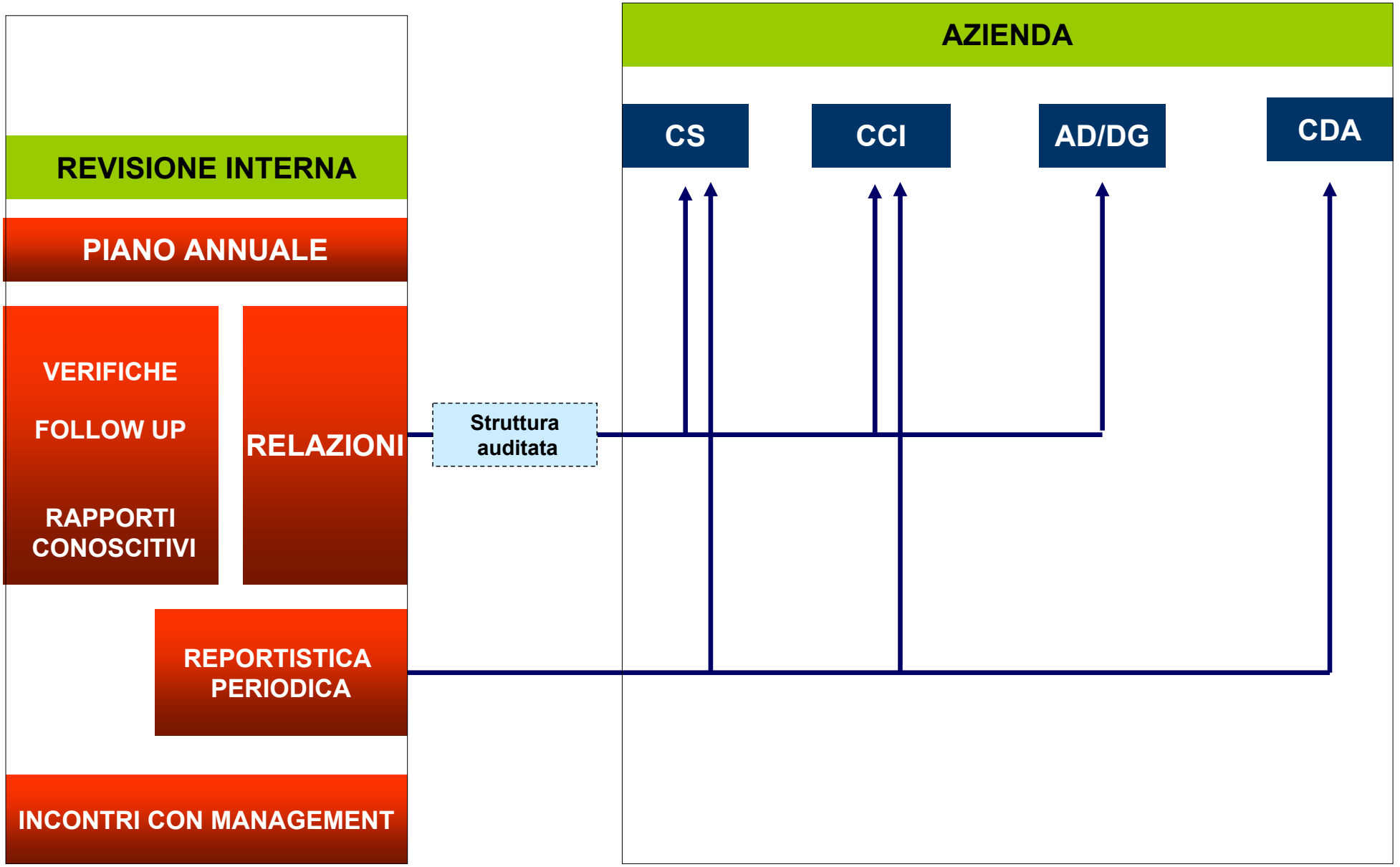
Capo III
e segg.

- Le imprese istituiscono le funzioni di revisione interna, risk management e compliance secondo requisiti sanciti dalla normativa.
- La revisione interna è incaricata di monitorare e valutare l'efficacia e l'efficienza del sistema di controllo interno e le necessità di adeguamento.
- Uniforma la propria attività agli standard professionali comunemente accettati a livello nazionale ed internazionale (*Associazione Italiana Internal Auditors*).
- L'organo amministrativo stabilisce le modalità e la periodicità con cui la revisione interna comunica al CDA, all'Alta Direzione e al Collegio Sindacale la valutazione delle risultanze e le eventuali disfunzioni e criticità.

Il processo di audit (standard AIIA)



I flussi informativi di audit



L'Architettura d'Impresa in azienda

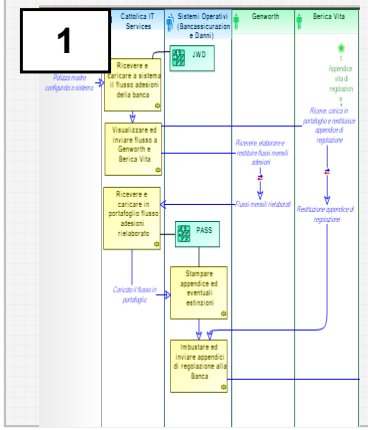
Architettura d'Impresa

Business Process Analisys	Modello organizzativo	Enterprise Risk Management	Compliance	Internal auditing	Business Continuity	IT Management
Funzione Processi	***Funzione Organizzazione***	***Risk Management***	***Compliance – Bilancio Consolidato***	***Audit***	***Informaton Technology Unit***	***Informaton Technology Unit***
Descrizione dei processi aziendali	Descrizione e gestione del modello organizzativo aziendale (organigrammi, competenze aziendali, carichi di lavoro).	Identificazione, e gestione dei rischi operativi, legali e reputazionali.	Identificazione e gestione dei rischi e dei controlli di compliance in un framework unitario, per assicurare la conformità alle normative vigenti (compliance a L.231/01, antiriclaggio e privacy e compliance a L. 262/ 05)	Definizione, implementazione e monitoraggio dei controlli di audit.	Identificazione e gestione dei potenziali rischi informatici in cui l'azienda può incorrere Definizione e implementazione di soluzioni per garantire e migliorare la disponibilità dei servizi erogati.	Gestione delle informazioni aziendali e delle attività di analisi e controllo dei processi e dei flussi aziendali coinvolti nell'erogazione e nell'utilizzo dei servizi IT.

Disporre di un modello di Architettura d'Impresa consente di conoscere a fondo gli attori e le modalità di funzionamento dell'azienda e le relazioni tra i diversi processi e i molteplici sistemi che la governano, in modo da valutare l'effettivo impatto delle azioni di *management* su ogni componente interessata e creare valore dalla gestione proattiva di tutte le variabili considerate. I sistemi di gestione e controllo aziendale orientati al valore rappresentano inoltre un fattore competitivo di crescente importanza.

Applicazione esemplificativa (1)

1



1. Analisi dei processi rilevati ed eventuali integrazioni

Esempio

- Analisi della documentazione relativa ai processi in scope.
- Individuazione di rischi e controlli del processo ed apporto di eventuali integrazioni sulla base di interviste con gli utenti.

2

RISK

(7)	(8)	(9)	(10)	(11)	(12)	(13)						
						Obiettivi di Controllo						
						Financial Assertion					Altri	
DESCRIZIONE DEL RISCHIO	CODICE DI RISCHIO	CLASSE DI RISCHIO	RISCHIO: POTENZIALITA'	RISCHIO: GRAVITA'	RISCHIO: ESPOSIZIONE	E&O	C	V&A	R&O	P&D	Aut_Trn	SoA
Errata definizione rettifiche Rischio di errata definizione delle rettifiche da contabilizzare.	R_0019	Errata predisposizione dei dati mediante spreadsheet	Ridotta	Strategico	6-Medio Alto		1	1				

CONTROL VALUATION

(26)							(27)	(28)	(29)
Controllo									
Financial Assertion					Altri				
E&O	C	V&A	R&O	P&D	Aut_Trn	SoA	ToD	VALUTAZIONE DELL'EVIDENZA DI CONTROLLO	CONTROLLO CHIAVE?
	1	1					Non effettivo	Non adeguata	Si

2. Costruzione Risk & Control Matrix e Valutazione Rischi e Controlli

- Popolamento della Risk & Control Matrix (inserimento caratteristiche dei controlli)
- Classificazione dei rischi individuati
- Valutazione rischi (impatto/frequenza)
- Valutazione efficacia disegno del controllo (copertura Financial Assertion)
- Individuazione dei controlli Chiave / Non Chiave.

Applicazione esemplificativa (2)

Esempio

3	CONTROL VALUATION		
	(30)	(31)	(32)
	GAP	DESCRIZIONE DEL GAP	CONTROLLO EFFETTIVO?
	Check evidence inadeguata	Inadeguata formalizzazione e archiviazione delle evidenze di controllo da parte dell'addetto dell'Unità Organizzativa.	No

3. Identificazione carenze

- Descrizione della carenza riscontrata
- Il gap può essere dovuto ad un non adeguato disegno del controllo o ad un difetto di formalizzazione/ esecuzione dello stesso.

4	ACTION PLAN			
(33)	(34)	(35)	(36)	(37)
CODICE ACTION PLAN	DESCRIZIONE ACTION PLAN	ACTION PLAN OWNER	PRIORITA'	SCADENZA
TBD	E' necessario razionalizzare l'attività di review da parte di un soggetto diverso dall'esecutore dell'attività, avendo cura di formalizzare la produzione delle evidenze di controllo (spunta e sigla da parte dell'esecutore del controllo e idonea archiviazione presso la cartella contenente la documentazione prodotta a supporto del Bilancio).	Addetto Bilancio e Consolidato	Bassa	TBD

4. Proposta di remediation (Action plan) in caso di rilevazione di una carenza

- Definizione azione correttiva a fronte della carenza individuata
- Determinazione dell'owner dell'azione correttiva
- Definizione della priorità
- Individuazione della scadenza.

LA COSTRUZIONE DI UN SISTEMA DI CONTROLLO INTERNO (IL CASO DELLE COMPAGNIE DI ASSICURAZIONE)

Dott. Werther Montanari
Direttore Audit di Gruppo
Società Cattolica di Assicurazione Soc. Coop.

Verona, 9 dicembre 2009