LA VALUTAZIONE DEL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI E IL REPORTING DELL'INTERNAL AUDIT

WORKSHOP PER I PROFESSIONISTI DEL SETTORE MANIFATTURIERO E SERVIZI

26 marzo 2014
Milano

Associazione Italiana Internal Auditors

LA VALUTAZIONE DEL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI E IL REPORTING DELL'INTERNAL AUDIT

RELATORI

***SIRO TASCA**, Chief Audit Executive – Falck Renewables S.p.A.*

***NICOLO' ZANGHI**, Associate Partner – KPMG Advisory S.p.A.*

***MAURO MAESTRINI**, Chief Audit Executive – Italcementi S.p.A.*

e coordinatore del Gruppo di Lavoro

Associazione Italiana Internal Auditors

AGENDA

Premessa

1. Il ruolo dell'Internal Audit
2. Il reporting periodico
3. La valutazione del SCIGR
   - 3.1. Principali riferimenti di leading practice in tema di valutazione del SCIGR
   - 3.2 Fattori da considerare nella valutazione SCIGR
   - 3.3. Documentazione di valutazione del SCIGR

Premessa (1/4)

Obiettivi e destinatari

- Fornire una guida pratica agli Internal Auditors, anche di piccole e medie imprese, relativamente a:
  - ✓ Reporting periodico dell'I.A. verso gli attori del SCIGR
  - ✓ Elementi sui quali basare la valutazione del SCIGR.

  nel rispetto degli Standards Internazionali per la pratica professionale dell'Internal Auditing e dalle Leading Practices.
- Non si tratta quindi di un "position paper" dell'Associazione Italiana Internal Auditors, ma del risultato dell'attività e delle esperienze di un Gruppo di Lavoro all'interno del Comitato Manifatturiero.

Premessa (2/4)

Perché la valutazione del Sistema di Controllo Interno e di Gestione dei Rischi

- Il **responsabile della funzione di Internal Audit** "verifica, sia in via continuativa sia in relazione a specifiche necessità e nel rispetto degli standard internazionali, l'operatività e l'idoneità del sistema di controllo interno e di gestione dei rischi […]. Le relazioni periodiche contengono una valutazione sull'idoneità del sistema di controllo interno e di gestione dei rischi" - *Codice di Autodisciplina*
- Il **Consiglio di Amministrazione**, previo parere del Comitato Controllo e Rischi, "valuta, con cadenza almeno annuale, l'adeguatezza del sistema di controllo interno e di gestione dei rischi rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto, nonché la sua efficacia […]" - *Codice di Autodisciplina*
- **Business Judgment Rule**: "A legal principle that makes officers, directors, managers, and other agents of a corporation immune from liability to the corporation for loss incurred in corporate transactions that are within their authority and power to make when sufficient evidence demonstrates that the transactions were made according to risk and control system"

Premessa (3/4)

Maurizio Sella

L'Internal Audit è coinvolto nella verifica in via continuativa e nella valutazione dell'idoneità dell'intero Sistema […] essendo l'unica funzione "sul campo" con competenze e accessi alle varie funzioni aziendali

Un ruolo centrale nel sistema di controllo endosocietario è affidato all'Internal Audit […] che non può essere confinato alla mera verifica della corretta applicazione delle procedure aziendali, ma deve poter indicare eventuali nuove aree di rischio e quindi svolgere anche una funzione propositiva.

Ferdinando Superti Furga

Premessa (4/4)

Gruppo di lavoro

Ferruccio Bellelli *(Saras S.p.A. – Responsabile Internal Audit)*

Alessandro De Michele (*Italcementi S.p.A. – Supervisor Internal* Auditor)

Marco Fabruzzo *(Buzzi Unicem S.p.A. – Responsabile Internal Audit)*

Mauro Maestrini (*Italcementi S.p.A. – Chief Audit Executive e Coordinatore gruppo di lavoro*)

Paolo Mantovano *(KPMG Advisory S.p.A. – Partner)*

Luca Preite *(Pirelli & C. S.p.A. – Supervisor Internal Auditor)*

Alessandra Ramorino *(Brembo S.p.A. – Internal Audit Director)*

Elena Riccardi *(KPMG Advisory S.p.A. - Senior Consultant)*

Siro Tasca *(Falck Renewables S.p.A. – Responsabile Internal Audit)*

Nicolò Zanghi *(KPMG Advisory S.p.A. – Associate Partner)*

1. Il ruolo dell'Internal Audit (1/2)

Gli elementi che caratterizzano il ruolo dell'Internal Audit sono:

- centralità e indipendenza nella supervisione del sistema di controllo e di gestione dei rischi:
  - comunicare il proprio ruolo;
- attività di verifica continuativa, organizzata attraverso un piano di audit, riportando periodicamente le risultanze di tale attività a diversi soggetti:
  - predisporre un reporting periodico della propria attività;
- valutazione di idoneità su un sistema integrato nel quale operano altre funzioni con responsabilità di controllo e monitoraggio del sistema medesimo:
  - effettuare una valutazione di idoneità del sistema.

1. Il ruolo dell'Internal Audit (2/2)

Comunicare il ruolo

- È necessario che l'organizzazione abbia compreso il ruolo e le responsabilità dell'I.A.
- L'I.A. deve farsi conoscere dalla Società (Mandato, partecipazione a riunioni, reporting)
- L'I.A. deve conoscere la Società (partecipazione a riunioni con il Management, coinvolgere il Management nella preparazione del piano di audit e nei singoli interventi)

Predisporre il reporting

- Comunicare il valore del proprio lavoro
- Comprendere le esigenze informative dei nostri interlocutori per:
  - ✓ Personalizzare il reporting e condividere i contenuti per i diversi interlocutori;
  - ✓ Ridurre l'expectation gap tra le aspettative degli stakeholders e gli obiettivi dell'I.A.;
  - ✓ Sintetizzare in un documento il risultato delle diverse attività che portano l'I.A. a formare i giudizi sull'idoneità del SCIGR.

2. Il reporting periodico (1/2)

- Nel documento sono riportate alcune slide di dettaglio dei principali flussi informativi che si devono (e/o possono) instaurare verso gli organi di controllo.
- Informativa periodica
  - ✓ Piano di audit
  - ✓ Rapporti di audit
  - ✓ Follow-up
  - ✓ Rapporto periodico di attività
- Informativa su tematiche specifiche
  - ✓ Informativa dell'Organismo di Vigilanza ex D.Lgs. 231/01
  - ✓ Informativa sul rispetto delle procedure previste ai fini della 262/05

2. Il reporting periodico (2/2)

- Informativa ad hoc
  - ✓ Audit special
  - ✓ Modifiche della metodologia valutazione SCIGR
  - ✓ Formazione e certificazione Auditors
  - ✓ Quality Assurance Review

- Informativa agli organi di controllo sulle performance dell'Internal Audit attraverso un set predefinito di KPI (cfr. "KPI AUDIT – Come misurare le performance della funzione di auditing interno", AIIA)

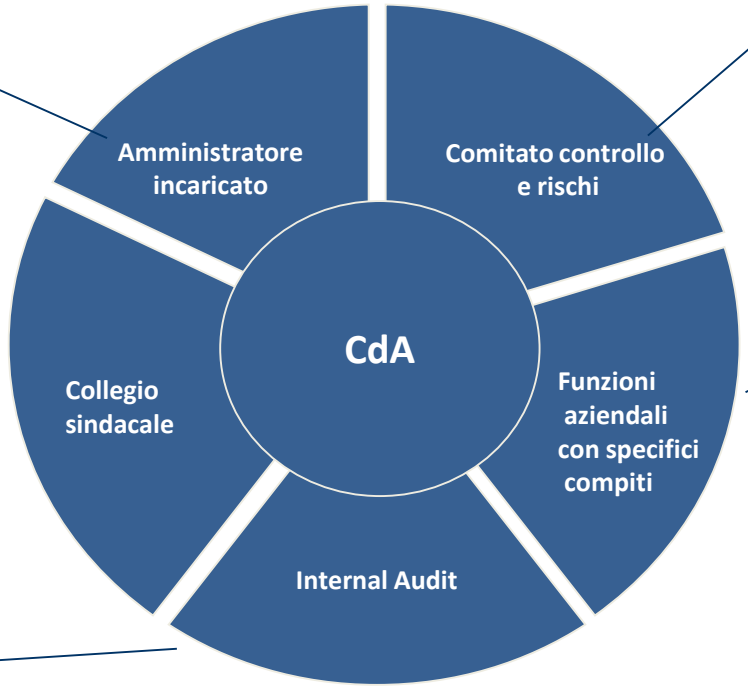
3.1. Principali riferimenti di leading practice in tema di valutazione del SCIGR (1/8)

Il codice di autodisciplina e i soggetti coinvolti

- I soggetti coinvolti nel SCIGR di un'organizzazione sono molteplici, ma la responsabilità ultima spetta al Consiglio di Amministrazione, il quale ha un ruolo centrale in materia di sistema di controllo interno e gestione dei rischi.

Implementa lo SCIGR, valutandone, nel continuo, adeguatezza ed efficacia

Esprime pareri al CdA, in generale, su temi legati al SCIGR e, in particolare, sulla valutazione di adeguatezza del SCIGR



Vigila su efficacia SCIGR

Specifici compiti in tema di controllo dei rischi; sono articolate in relazione a dimensioni, complessità e profilo di rischio dell'impresa

cd Funzioni di secondo livello, introdotte con riferimento alla definizione di **SCIGR strutturato su tre livelli**

Verifica operatività e idoneità SCIGR

Gli organi di governo, nell'ambito della conduzione e della supervisione dell'attività di impresa, devono garantire una buona governance del sistema integrato di gestione dei rischi e dei relativi controlli interni.

Associazione Italiana Internal Auditors

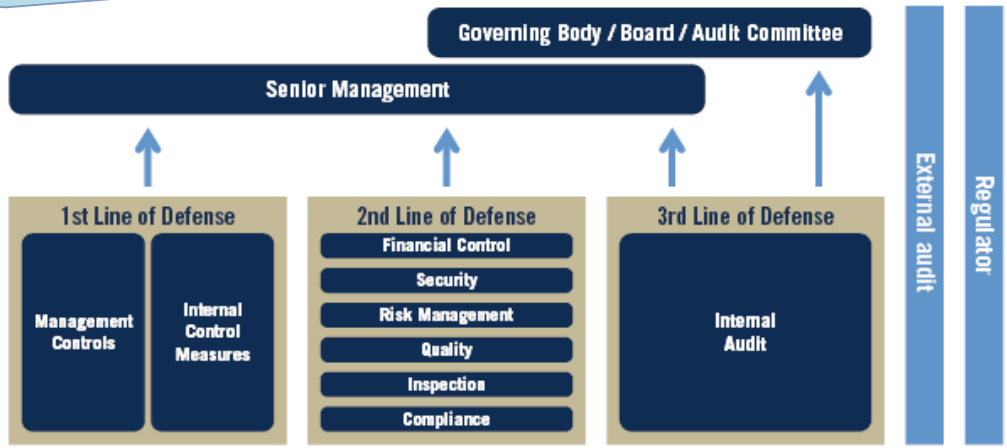
3.1. Principali riferimenti di leading practice in tema di valutazione del SCIGR (2/8)

Il modello dei tre livelli di controllo

- I soggetti che concorrono alla valutazione del SCIGR sono identificati sui tre livelli di controllo

*"**As a first line of defense, operational management** has ownership, responsibility, and accountability for assessing, controlling, and mitigating risks together with maintaining effective internal controls.*
***As a second line of defense, the risk management function** facilitates and monitors the implementation of effective risk management practices by operational management and assists the risk owners in defining the target risk exposure and reporting adequate risk-related information through the organization…*
***As a third line of defense, the internal audit function** will, through a risk-based approach, provide assurance to the organization's board and senior management on how effectively the organization assesses and manages its risks, including the manner in which the first and second lines of defense operate."*

ECIIA e FERMA - 2010



The Institute of Internal Auditors, *IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control*, (2013)

***"Business-enabling functions,** such as risk, control, legal, and compliance provide the second line of defense as they clarify internal control requirements and evaluate adherence to defined standards "*
Internal Control - Integrated Framework, CoSO 2013

Associazione Italiana Internal Auditors

3.1. Principali riferimenti di leading practice in tema di valutazione del SCIGR (3/8)

Framework riferimento: il CoSO ERM

- Il "CoSO ERM", costituisce il modello di riferimento in tema di controllo interno e gestione dei rischi. Punto di forza del framework è l'estensione dell'ambito del controllo interno al tema della gestione del rischio aziendale, realizzando, così, un modello unico di riferimento del quale il sistema di controllo interno è parte integrante.

CoSO Enterprise Risk Management - Integrated Framework

"Monitoraggio": si concretizza in interventi continui, integrati nella normale attività operativa aziendale e/o in valutazioni separate, volti a valutare la presenza e il funzionamento continuo nel tempo di tutte le componenti di un sistema di Enterprise Risk Management.

Il processo di gestione del rischio aziendale è infatti soggetto a cambiamenti e il management è chiamato a verificarne l'efficacia nel tempo.

Il framework affronta solo parzialmente il tema della valutazione del sistema di controllo interno e di gestione dei rischi e non sviluppa uno strumento pratico di valutazione di immediata applicazione.

3.1. Principali riferimenti di leading practice in tema di valutazione del SCIGR (4/8)

Recenti sviluppi e approcci

- Di seguito sono illustrati i più recenti approcci per la valutazione del SCIGR: il "Key Principles Approach" e il "Maturity Model Approach". Entrambe le metodologie presentano vantaggi e svantaggi.

Key Principles Approach

- \+ Approccio semplice con logica on/off
- \+ Valutazione chiara e facilmente comprensibile sul sistema di controllo interno e gestione dei rischi
- \+ Parere puntuale in termini di compliance
- \- Lunga condivisione e approvazione degli esiti
- \- Difficile comprensione dei miglioramenti possibili da implementare in ottica di evoluzione del SCIGR
- \- Difficilmente applicabile laddove i processi siano complessi o indefiniti
- \- Complicata identificazione delle carenze di processo relative agli obiettivi operativi

Maturity Model Approach

- \+ Favorisce la discussione sull'evoluzione del SCIGR e sulle opzioni di miglioramento continuo
- \+ Più facile espressione delle aspettative di maturità dei singoli processi con riferimento agli obiettivi operativi
- \- Difficile individuazione del livello di maturità ritenuto accettabile e ottimale.
- \- In termini di compliance, qualsiasi elemento che non si collochi al più alto livello di maturità potrebbe essere oggetto di preoccupante attenzione

La scelta su quale dei due approcci utilizzare nella valutazione del SCIGR dovrebbe tenere in considerazione le possibili implicazioni dei due diversi approcci di valutazione.

3.1. Principali riferimenti di leading practice in tema di valutazione del SCIGR (5/8)

Recenti sviluppi e approcci: Key Principles Approach

- L'approccio per principi si basa sul concetto che qualsiasi processo di controllo interno e gestione dei rischi, per essere pienamente efficace, deve soddisfare un insieme minimo di principi caratteristiche. **Il management è chiamato ad individuare l'esistenza di componenti e principi sia nel disegno e implementazione del sistema di controllo interno ("present") sia nell'operatività e gestione del sistema stesso ("functioning")**

Approccio basato sui principi

Control environment	1. L'organizzazione dimostra impegno nell'integrità e valore etico 2. Il CDA è indipendente dal management ed esercita attività di monitoraggio per l'attività di sviluppo e di performance del sistema di controllo interno. 3. Nel rispetto degli obiettivi il management stabilisce struttura e sistema di deleghe e poteri. 4. L'organizzazione in linea con gli obiettivi persegue una strategia nella ricerca ,sviluppo e ritenzione di talenti. 5. L'organizzazione vigila sulle responsabilità degli attori del controllo interno nel perseguimento degli obiettivi
Risk Assessment	6. L'organizzazione specifica gli obiettivi con chiarezza in modo da individuare e valutare i rischi connessi. 7. L'organizzazione nel raggiungimento degli obiettivi identifica i rischi. E l'analisi del rischio è il punto di partenza nel determinare la più appropriata gestione dello stesso. 8. L'organizzazione considera il rischio di frode nel raggiungimento per il raggiungimento dei propri obiettivi 9. L'organizzazione identifica e valuta i cambiamenti che potrebbero significatamente impattare il sistema di controllo interno.
Control activities	10. L'organizzazione seleziona e sviluppa attività di controllo che contribuiscono alla mitigazione a un livello accettabile dei rischi di mancato raggiungimento degli obiettivi. 11. L'organizzazione seleziona e sviluppa attività di controllo sulla tecnologia a supporto del raggiungimento degli obiettivi. 12. L'organizzazione descrive le attività di controllo all'interno delle policy, che stabiliscono i risultati attesi, e nelle relative procedure che sviluppano tali policy.
Information and communication	13. L'organizzazione ottiene o genera e utilizza informazioni rilevanti e di qualità a supporto del funzionamento delle altre componenti del sistema di controllo interno. 14. L'organizzazione ha un processo di comunicazione interna, che include gli obiettivi e le responsabilità sui controlli interni, necessario a supportare il funzionamento delle altre componenti del sistema di controllo interno. 15. L'organizzazione comunica all'esterno i fatti rilevanti che hanno impatto sulle altre componenti del sistema di controllo interno.
Monitoring activities	16. L'organizzazione seleziona, sviluppa e svolge continue o specifiche valutazioni per verificare la presenza e il funzionamento delle componenti del sistema di controllo interno. 17. L'organizzazione valuta e comunica le carenze del sistema di controllo interno in modo tempestivo ai responsabile dell'adozione di azioni correttive, inclusa l'alta direzione e il consiglio di amministrazione, qualora necessario.

CoSO Internal Control - Integrated Framework

L'approccio per principi rende più agevole la definizione delle componenti del SCIGR e conseguentemente identifica chiaramente i criteri di riferimento ai fini della valutazione della sua adeguatezza.

Associazione Italiana Internal Auditors

3.1. Principali riferimenti di leading practice in tema di valutazione del SCIGR (6/8)

Recenti sviluppi e approcci: Maturity Model Approach

- Le scale di maturità della governance costituiscono, per il Comitato Controllo e Rischi ed il Consiglio di Amministrazione, uno strumento di riferimento per la valutazione del livello di efficacia e del grado di ottimizzazione della governance, dei presidi di risk management e dei controlli aziendali.

MEASURE	NONE	VERY LITTLE	SOME	GOOD	COMPLETE
Meaning	Very little or no compliance with the requirement in any way.	Only limited compliance with the requirement. Management supports the intent, but compliance in practice is poor.	Limited compliance with element state-ment. Certainly agree with the intent, but limited compliance in practice.	Management completely subscribes to the intent, but there is partially complete compliance in practice.	Absolute compliance with the element statement — in intent and in practice — at all times and in all places.

Esistono diversi modelli per valutare la scala di maturità del SCIGR che possono prendere in considerazione e analizzare elementi differenti ed essere sviluppati su più livelli.

Elemento del modello	BASE *Rispetto della compliance*	MATURO *Processo di gestione*	AVANZATO *Strumento strategico*
Risk governance	Politica di risk management centrale a supporto delle necessità esterne	Struttura di risk management con responsabilità definite a supporto degli obiettivi di risk management	Responsabilità in materia di risk management integrata con la gestione della performance
Valutazione dei rischi	Valutazione dei rischi effettuata a cadenza annuale con un'analisi e un'interpretazione limitata	Valutazione dei rischi frequente in linea con il normale reporting gestionale, analisi inclusa	Attività di rischio e controllo radicate nei processi aziendali
Quantificazione e aggregazione dei rischi	Quantificazione dei rischi selezionati	Quantificazione del rischio operativo; quantificazione elevata dei rischi selezionati	Aggregazione a livello di entità di tutte le aree di rischio
Monitoraggio e reporting sui rischi	Reporting dei rischi aziendali improntato al sostegno delle necessità esterne	Reporting esauriente nei confronti del Consiglio di amministrazione dell'Audit committee sui livelli di rischio attuali e sui rischi futuri	Allineamento del reporting sul rischio al fine di fornire un punto di vista unico sul rischio
Miglioramento di rischi e controlli	Poche sorprese grazie alla gestione dei rischi principali	Maggiore fiducia da parte degli stakeholder e migliori strategie di attenuazione del rischio	Strategia basata sui rischi, valutazione della performance e attribuzione del capitale

Sulla base dei risultati emersi dalla valutazione del sistema in essere, l'organizzazione può decidere il livello di maturità che intende raggiungere e sviluppare quindi un master plan di iniziative da intraprendere per indirizzare il percorso evolutivo del processo di Enterprise Risk Management.

3.1. Principali riferimenti di leading practice in tema di valutazione del SCIGR (7/8)

Sviluppi normativi in ambito UE: Punti di attenzione nei sistemi di corporate governance

- La nuova legislazione europea, emanata al fine di rafforzare la regolamentazione del settore bancario, evidenzia alcuni punti di attenzione nei sistemi di corporate governance.

- La natura non vincolante della maggior parte dei principi di corporate governance, ha contribuito alla mancanza dell'effettivo rispetto di tali principi, lasciando l'implementazione per lo più all'auto regolamentazione e al controllo esterno da parte degli azionisti.

European Commission

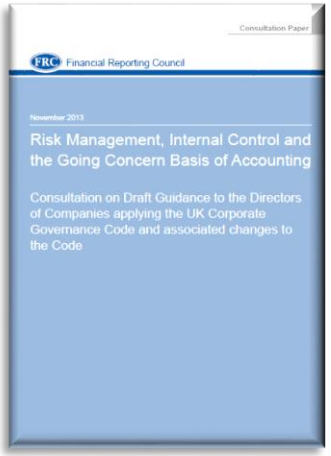
- L'autodisciplina ha avuto rilevanti effetti positivi sull'assetto complessivo della regolazione delle società quotate italiane.
- Relativamente all'effettiva applicazione delle raccomandazioni, alle quali le società dichiarano di volere aderire, in Italia e negli altri ordinamenti europei, emerge che i rimedi siano rimessi essenzialmente all'iniziativa privata (cosiddetto private enforcement) e ai meccanismi di controllo endo-societari.

Associazione Italiana Internal Auditors

3.1. Principali riferimenti di leading practice in tema di valutazione del SCIGR (8/8)

Sviluppi attesi: Financial Reporting Counsil

- A novembre 2013 il Financial Reporting Counsil ha pubblicato in consultazione la guida **"Risk Management, Internal Control and the Going Concern Basis of Accounting - Consultation on Draft Guidance to the Directors of Companies applying the UK Corporate Governance Code and associated changes to the Code"** che andrà a sostituire la "Internal Control: Guidance for Directors (2005)" e la "Going Concern and Liquidity Risk: Guidance for Directors (2009)". La versione definitiva, secondo le previsioni, sarà pubblicata nella prima metà del 2014 e diventerà operativa insieme agli aggiornamenti del Codice proposti.



Tra le principali proposte di revisione del UK Corporate Governance Code (in particolare (C.2. Risk Management and Internal Control): "C.2.2 **The board should monitor the company's risk management and internal control** and**, at least annually**, carry out **a review of their effectiveness**, and **report to shareholders** that they have done so. The monitoring and review should cover all material controls, including financial, operational and compliance controls"

Al board è richiesto un **on-going scrutiny** e un **annual assessment** che prenda in considerazione principalmente:

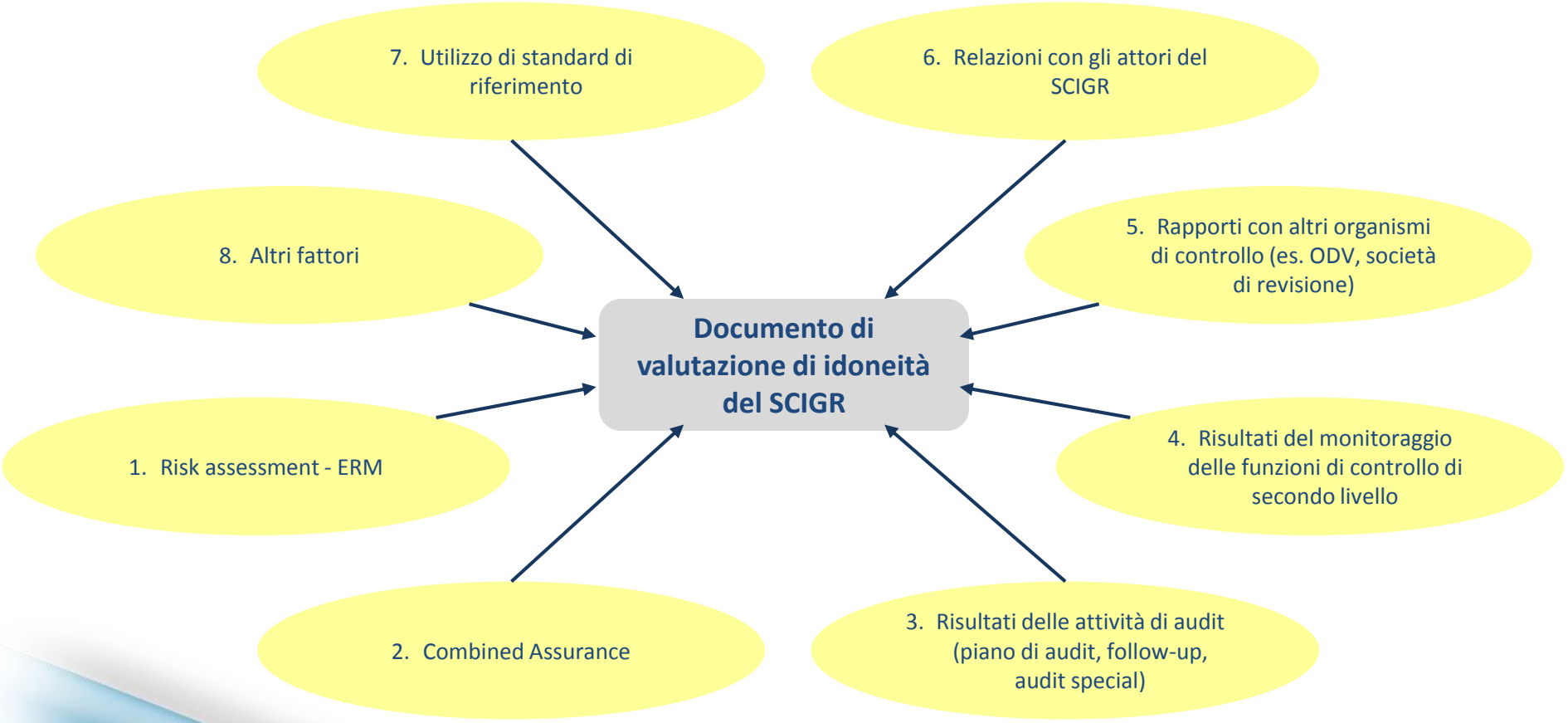
- the company's willingness to take on risk (its **risk appetite**);
- the **culture** of the company;
- the **integration of risk management** with considerations of **strategy and capital**, and with **business planning processes**;
- the **changes** in the nature and extent of principal risks;
- the **scope and quality of management's on-going monitoring** and the work of internal audit function and other sources of assurance;
- the **extent, frequency and quality of the communication of the results of the monitoring** to the board (or board committees);
- **issues** dealt with in reports reviewed by the board during the year with a material **impact on the company's performance or reputation;**
- the **effectiveness of the company's public reporting processes**.

Statement on risk management and internal control

In order to comply with Provision C.2.2 of the UK Corporate Governance Code, the **board should report on its review of the effectiveness of the company's risk management and internal control systems.**

Associazione Italiana Internal Auditors

3.2. Fattori da considerare per la valutazione del SCIGR (1/11)



Associazione Italiana Internal Auditors

3.2.Fattori da considerare per la valutazione del SCIGR (2/11)

1. Risk assessment - ERM

- Codice di autodisciplina: ”ogni emittente si dota di un sistema di controllo interno e di gestione dei rischi costituito dall’insieme delle regole, delle procedure e delle strutture organizzative volte a consentire l’identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi”.
- Esiste un processo che porta a conoscere i rischi aziendali per poterli misurare, gestire e monitorare ?
  - ✓ ERM: consente una gestione integrata e di governo dei rischi
  - ✓ Attività di Risk Management
  - ✓ Piano di Audit come unico documento in cui si formalizza un’analisi dei rischi
- Documento: “ERM – Guidance per Internal Auditors del settore Manifatturiero”.

3.2.Fattori da considerare per la valutazione del SCIGR (3/11)

2. Combined assurance

- Standard 2050: “il responsabile internal auditing dovrebbe condividere le informazioni e coordinare le diverse attività con i diversi prestatori, esterni ed interni, di servizi di assurance e consulenza, al fine di assicurare un’adeguata copertura e di minimizzare le possibili duplicazioni”.
- Combined assurance map: evidenza i top risks e l’assurance fornita da diversi assurance providers al fine di fornire informazioni utili al Board per esercitare al meglio il suo ruolo di oversight.
- Chiarire i 3 livelli di controllo e i rispettivi ruoli e responsabilità.
- Combined assurance report.

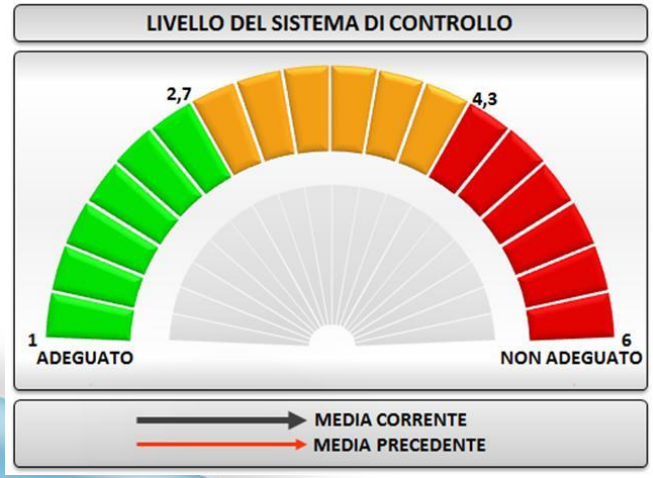
Risks	Three lines of defense											
	Management				Corporate Functions				Third-Party Assurance			
	Reviews	Sign-offs	Self-assessment	KPIs	Finance	HR	IT	Operation	Auditors	Specialist	Internal Audit	Quality Audit
Fraud and Theft												
Competition risks												
IT system failure												
...												

3.2.Fattori da considerare per la valutazione del SCIGR (4/11)

3. Risultati delle attività di audit

3.1. Risultati di interventi effettuati sulla base del piano di audit

- Risultati dei singoli report presentati nel corso dell'anno
- Necessità di riassumere i risultati in un documento sintetico (tabella, matrice, ecc.)



	Vendite	Acquisti	Finanza	Tecnica	Risorse Umane	.....
AREA 1	C ↘	A ⇔	B ↗	C ↗	D ↗	C ⇔
AREA 2	E ⇔	C ↘	B ↗	B ↘	D ↘	B ↗
AREA 3	C ↗	D ↗	A ⇔	E ⇔	C ↗	C ↘
AREA 4	A ⇔	C ↗	B ↗	C ↗	D ↗	C ↗
AREA 5	C ↗	A ⇔	C ↗	E ⇔	C ↗	D ↗
.....	C ↗	B ↗	C ⇔	B ↗	C ⇔	D ⇔

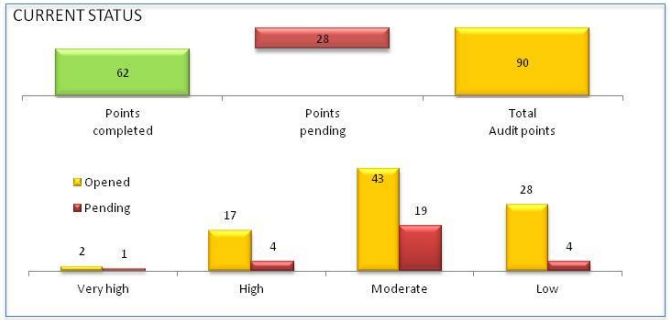
3.2.Fattori da considerare per la valutazione del SCIGR (5/11)

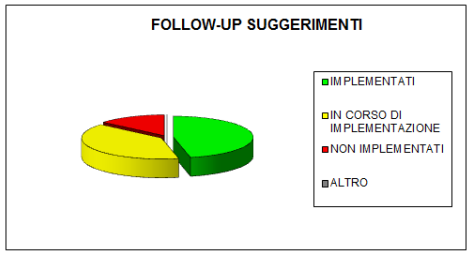
3. Risultati delle attività di audit

3.2. Risultati del processo di follow-up

- Un SCIGR per essere adeguato, oltre a riconoscere i propri punti di debolezza e i conseguenti rischi, deve essere in grado di attivare un percorso per ricondurre il rischio ad un livello accettabile.
- Reportistica per sintetizzare lo status delle azioni correttive concordate con il management a seguito delle raccomandazioni contenute nei rapporti di audit.

STATUS DELLE RACCOMANDAZIONI					
Anno	*Rischio*	*Attuate*	*Aperte*	*In ritardo*	TOTALE
2012	Molto Alto	6	0	0	6
	Alto	18	2	2	22
	Medio	80	12	11	103
	Basso	55	15	15	85
	Totale	159	29	28	216
2013	Molto Alto	9	2	0	11
	Alto	22	8	3	33
	Medio	70	26	9	105
	Basso	48	33	9	90
	Totale	149	69	21	239





Associazione Italiana Internal Auditors

3.2.Fattori da considerare per la valutazione del SCIGR (6/11)

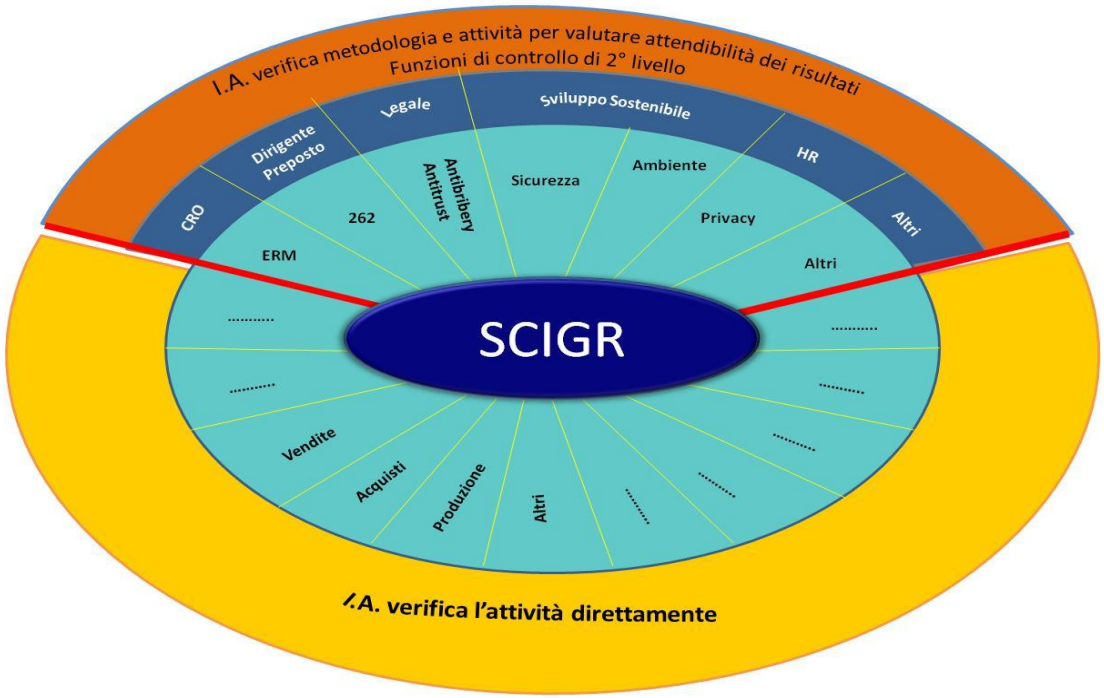
3. Risultati delle attività di audit

3.3. Risultati degli audit special

- Gli interventi di audit special, generalmente effettuati a seguito di richieste degli attori del SCIGR o del top management o su segnalazioni di whistleblower, sono una spia rilevante del funzionamento del SCIGR.
- Da una parte richieste e segnalazioni testimoniano che il canale per identificare le falle nel sistema funzionano, dall'altra sono anche evidenza di situazioni patologiche del SCIGR che si sono verificate a causa della sua imperfezione.

3.2.Fattori da considerare per la valutazione del SCIGR (7/11)

4. Risultati del monitoraggio delle funzioni di controllo di 2° livello



- L'Internal Audit deve quindi accertarsi che le attività di audit/monitoraggio delle altre funzioni siano state effettuate seguendo una metodologia tale per cui i risultati siano attendibili e utilizzabili dall'Internal Audit stesso.

Associazione Italiana Internal Auditors

3.2.Fattori da considerare per la valutazione del SCIGR (8/11)

5. Rapporti con altri Organismi di Controllo

- Esistono altri Enti/Organismi che effettuano attività di audit all'interno dell'organizzazione:
  - ✓ Auditor esterni
  - ✓ Organismo di Vigilanza
  - ✓ Certificatori esterni (qualità, ambiente, sicurezza, ecc..).
- Indipendenza più marcata rispetto alle funzioni di controllo di 2° livello.
- Maggiori difficoltà nel verificare/concordare la metodologia di lavoro.
- Ottenere le relazioni e organizzare incontri per lo scambio di informazioni.

3.2.Fattori da considerare per la valutazione del SCIGR (9/11)

6. Relazioni con gli attori del SCIGR

- Il Responsabile Internal Audit nello svolgimento delle attività a lui assegnate in tema di sistema di controllo interno e gestione dei rischi, interagisce con numerosi soggetti, che sono in un certo senso i nostri clienti:
  - ✓ Consiglio di Amministrazione
  - ✓ Amministratore incaricato del SCIGR
  - ✓ Comitato Controllo e Rischi
  - ✓ Collegio Sindacale.
- E' necessario, accertarsi che la società preveda modalità di coordinamento tra vari i vari soggetti sopra elencati al fine di massimizzare l'efficienza del SCIGR e di minimizzare le duplicazioni di attività.
- Un continuo flusso informativo e incontri periodici sono indispensabili al fine di evitare un "expectation gap" tra le loro aspettative e quanto l'Internal Audit per missione, mandato o risorse è in grado di garantire.

3.2.Fattori da considerare per la valutazione del SCIGR (10/11)

7. Utilizzo standard di riferimento

- L'utilizzo di modelli di riferimento per valutare il SCIGR e dei relativi strumenti metodologici applicabili, quali template, check list ecc.., è necessario al fine di accertarsi che tutte le componenti e i principi fondamentali del SCIGR siano presenti e funzionanti in modo integrato.
- Qualsiasi sia il modello di riferimento scelto, è necessario che il lavoro di valutazione sia debitamente documentato.
  - ✓ Key Principles Approach (COSO 2013, ISO 31000)
  - ✓ Maturity Model Approach (Ned Community e altri).

3.2.Fattori da considerare per la valutazione del SCIGR (11/11)

8. Altri fattori

- In funzione dell'organizzazione della società, della sua complessità e del grado di maturità del SCIGR, vi sono altri aspetti da considerare e da citare nella relazione di sintesi:
  - ✓ Evoluzione impianto procedurale
  - ✓ Aggiornamento del Modello di Organizzazione, Gestione e Controllo
  - ✓ Evoluzione delle politiche e linea guida di governance.
  - ✓ ……

3.3. Documento di valutazione

- Documento che sintetizza le conclusioni dell'Internal Audit sull'adeguatezza del SCIGR e che possa essere presentato e discusso in modo autonomo.
  1. Riferimento ai documenti di supporto sui quali si basa la valutazione.
  2. Richiamo alle principali deficiencies, se esistenti, e al relativo piano di implementazione delle azioni correttive.
  3. Riferimento alle limitazioni.

- La non idoneità è un'ipotesi da considerare astrattamente. Nel caso in cui si riscontrino "major deficiency" tali da compromettere il SCIGR nel suo complesso, l'Internal Audit informa tempestivamente gli attori del SCIGR sulla sua impossibilità a rilasciare il giudizio di idoneità.

Relazione periodica del resp. dell'Internal Audit (esempio)

Con riferimento ai principi condivisi con gli attori del SCIGR, il responsabile della funzione *Internal Audit*, nel rispetto degli standards internazionali della pratica professionale dell'*Internal Auditing* e sulla base dei seguenti elementi:

- Esiti delle attività di Risk Management
- La Combined Assurance per i xx rischi ritenuti più rilevanti
- Risultati delle attività di audit ed in particolare:
  - risultati dei XX interventi effettuati sulla base del piano di audit, approvato dal Consiglio di Amministrazione e basato su un processo strutturato di analisi e prioritizzazione dei principali rischi. Si allega un prospetto riassuntivo dei rating assegnati alle diverse aree
  - risultati dell'attività di follow-up al fine di verificare la messa in atto dei piani di azione concordati con le diverse Direzione a fronte dei rilievi emersi durante l'attività di audit. Si allega un prospetto sintetico dei risultati del follow-up
  - risultati degli audit special derivanti da segnalazioni di whistleblower o richieste del top management con particolare riferimento alle eventuali lacune del SCIGR o circostanze che hanno consentito il perpetrarsi dell'illecito o della situazione anomala
- Esame dell'attività e dei risultati del monitoraggio delle funzioni di controllo di secondo livello, con particolare riguardo al Dirigente Preposto e ai responsabili delle funzioni HSE, Affari Legali, Risorse Umane, Risk Management
- Scambi di informativa con il revisore esterno sull'informativa finanziaria
- Scambi di informativa con l'Organismo di Vigilanza sull'idoneità del Modello di Organizzazione, Gestione e Controllo
- Indirizzi ricevuti dal Consiglio di Amministrazione ed esame delle informazioni condivise con gli altri attori del SCIGR (Amm.incaricato del SCIGR, Comitato Controllo e Rischi, Collegio Sindacale)

Valuta idoneo il sistema di controllo interno e gestione dei rischi

Il SCIGR presenta ancora tuttavia alcune aree di miglioramento per le quali la società ha già posto in essere delle azioni correttive:

- Area di miglioramento 1
- Area di miglioramento 2
- Area di miglioramento 3

Si sottolinea come anche un SCIGR efficace, per quanto ben concepito, presenta alcuni limiti intrinseci, quali la possibilità che i controlli vengano vanificati fraudolentemente o per errori, per cui si può garantire solo con ragionevole certezza, e non in modo assoluto, il raggiungimento degli obiettivi di controllo e di gestione dei rischi.

LA VALUTAZIONE DEL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI E IL REPORTING DELL'INTERNAL AUDIT

WORKSHOP PER I PROFESSIONISTI DEL SETTORE MANIFATTURIERO E SERVIZI

26 marzo 2014
Milano

Associazione Italiana Internal Auditors

TAVOLA ROTONDA

L'INTERNAL AUDIT COME CATALIZZATORE DELLE FONTI DI ASSURANCE A SUPPORTO DEGLI ORGANI SOsocietari

INTERVENGONO

FERRUCCIO BELLELLI, *Responsabile Internal Audit – Saras S.p.A.*

MASSIMO MANENTE, *rappresentante del Comitato Manifatturiero – AIIA e collaboratore - Crowe Horwath*

PAOLO MANTOVANO*, Partner – KPMG Advisory S.p.A.*

MODERA

FRANCESCO ALBIERI, *Head of Gorup Internal Audit – Parmalat S.p.A. e coordinatore Comitato Manifatturiero - AIIA*

Associazione Italiana Internal Auditors

LA VALUTAZIONE DEL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI E IL REPORTING DELL'INTERNAL AUDIT

WORKSHOP PER I PROFESSIONISTI DEL SETTORE MANIFATTURIERO E SERVIZI

26 marzo 2014
Milano

Associazione Italiana Internal Auditors