

Carolyn Dittmeier
con la collaborazione di Elisabetta Fusi

BIBLIOTECA
L. PACIOLI

La governance dei rischi

Un riferimento per gli organi
e le funzioni di governo e controllo

Prefazione di
Massimo Menchini

Redazione e impaginazione: Tralerighe s.n.c., Milano

Per l'edizione in lingua italiana
Copyright © 2015 EGEA S.p.A.
Via Salasco, 5 - 20136 Milano
Tel. 02/5836.5751 - Fax 02/5836.5753
egea.edizioni@unibocconi.it - www.egeaonline.it

Tutti i diritti sono riservati, compresi la traduzione, l'adattamento totale o parziale, la riproduzione, la comunicazione al pubblico e la messa a disposizione con qualsiasi mezzo e/o su qualunque supporto (ivi compresi i microfilm, i film, le fotocopie, i supporti elettronici o digitali), nonché la memorizzazione elettronica e qualsiasi sistema di immagazzinamento e recupero di informazioni.
Per altre informazioni o richieste di riproduzione si veda il sito www.egeaonline.it/fotocopie.htm

Date le caratteristiche di Internet, l'Editore non è responsabile per eventuali variazioni di indirizzi e contenuti dei siti Internet menzionati.

Prima edizione: settembre 2015

ISBN 978-88-238-3426-2

Stampa: lalitotipo, Settimo M.se (MI)

Questo volume è stato stampato con inchiostri vegetali su carta approvata dal Forest Stewardship Council, non ottenuta dalla distruzione di foreste primarie.

Indice

Prefazione di Massimo Menchini

pag. IX

Introduzione

» XI

Ringraziamenti

» XV

1 Contesto regolamentare e di autodisciplina

» 1

1.1 Il quadro europeo regolamentare e autoregolamentare

» 4

1.2 I Principi OECD

» 17

1.3 L'esperienza del Regno Unito

» 25

1.4 Il King III Corporate Governance Code del Sud Africa

» 30

1.5 Il contesto statunitense

» 36

1.6 La normativa italiana e il Codice di Autodisciplina

» 44

1.6.1 La normativa societaria

» 44

1.6.2 L'attuazione della Direttiva europea 2006/43/CE:
il D.Lgs. 39/2010

» 46

1.6.3 Il D.Lgs. 231/2001: i rischi di reato per eventi illeciti

» 47

1.6.4 La legge sulla tutela del risparmio

» 49

(Legge 28 dicembre 2005, n. 262)

» 49

1.6.5 Il Codice di Autodisciplina

» 50

1.7 Le indicazioni per il settore finanziario

» 53

1.7.1 Framework for Internal Control Systems
in Banking Organisations

» 54

1.7.2 Basilea I, II, III

» 55

1.7.3 Internal Capital Adequacy Assessment Process
(ICAAP)

» 61

1.7.4 Risk Appetite Framework (RAF)

» 65

1.7.5 Corporate governance principles for banks

» 70

1.7.6 Settore assicurativo: EIOPA, Solvency II
e ORSA - Assessment of Own Risks

» 71

2	Principi, standard e modelli di riferimento di risk management	»	79
2.1	La definizione di rischio e di risk management d'impresa	»	80
2.2	Standard e modelli di riferimento e la loro evoluzione storica	»	88
2.2.1	Enterprise Risk Management (ERM) o CoSO II	»	96
2.2.2	ISO 31000	»	114
2.2.3	Comparazione tra ISO 31000 ed ERM	»	121
2.2.4	Il modello GRC (Governance, Risk and Compliance)	»	122
2.2.5	Altri riferimenti	»	127
2.3	Business Case: il Gruppo Italcementi	»	136
3	L'implementazione del modello e il processo di risk management	»	149
3.1	L'effettiva implementazione di un modello di gestione dei rischi	»	150
3.2	Il processo di risk management d'impresa	»	155
3.2.1	L'ambiente interno e lo sviluppo della cultura aziendale	»	158
3.2.2	L'esplicitazione degli obiettivi di business e di governance	»	161
3.2.3	Il risk assessment	»	164
3.2.4	Le strategie nella risposta al rischio	»	201
3.2.5	Monitoraggio dei rischi e utilizzo dei key risk indicator	»	204
3.2.6	Risk reporting e comunicazione	»	209
3.3	Il sistema di controllo interno nell'ambito del risk management	»	212
3.3.1	Gli obiettivi di controllo in relazione agli obiettivi di governo e di business	»	221
3.3.2	Valutazione del sistema di controllo interno, risk based	»	225
3.3.3	Criteri di adeguatezza del disegno dei controlli	»	231
3.3.4	Criteri per l'effettivo funzionamento dei controlli	»	233
3.4	Scale di maturità nell'implementazione di un modello di risk management	»	234
3.5	Un sistema aziendale integrato	»	240
3.5.1	Enterprise risk management e il modello organizzativo ex D.Lgs. 231/01	»	243
4	Risk governance e pianificazione strategica dell'impresa	»	247
4.1	Integrare risk management e pianificazione strategica	»	248
4.1.1	Analisi dei rischi nella definizione delle linee strategiche	»	251
4.2	I rischi strategici	»	252
4.2.1	Cyber security risks	»	254
4.3	Il risk appetite nell'ambito del piano strategico	»	256
4.4	Business Case: il Gruppo Autogrill	»	262

5	Risk governance in chiave organizzativa	»	275
5.1	Il ruolo del Consiglio di Amministrazione	»	282
5.2	Il risk oversight e il supporto del Comitato Controllo e Rischi	»	289
5.3	L'amministratore incaricato del sistema di controllo interno e di gestione dei rischi	»	296
5.4	Il ruolo del Collegio Sindacale	»	298
5.5	La funzione del Chief Risk Officer	»	301
5.5.1	Le scelte organizzative	»	301
5.5.2	Il ruolo "eclettico" del Chief Risk Officer	»	304
5.6	La funzione di Internal Auditing quale assurance	»	308
5.7	Policy e procedure di risk management	»	317
5.8	Le relazioni e i flussi informativi tra gli organi e le funzioni di controllo	»	322
	Bibliografia	»	333