

Enterprise Risk:
identificare, governare e gestire
i rischi IT

**RISK IT
FRAMEWORK**

Bozza

Parte prima (traduzione dei capitoli 1, 2, 3 4 e 5)

Traduzione italiana, versione: **martedì 10 febbraio 2009**



LEADING THE IT GOVERNANCE COMMUNITY

v 0.1 revised 3Feb09

Pagina lasciata intenzionalmente in bianco

Prefazione alla traduzione italiana

La presente traduzione è stata realizzata da **Agatino Grillo**, CISA, CISSP, CISM.

Questo documento viene diffuso via web attraverso il sito <http://www.compliancenet.it/> in formato **pdf**, Microsoft **Word 97-2003** ed **Open Office 3.0** al fine di garantirne la massima diffusione.

Per contattare Agatino Grillo:

- agatino.grillo@gmail.com
- <http://www.agatinogrillo.it/>

La versione in lingua inglese (versione originale) di questo documento è liberamente scaricabile, previo registrazione gratuita, in formato **pdf**, dal sito di ISACA a questo link: <http://www.isaca.org/AMTemplate.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm&ContentID=47642>

Questa prima parte della traduzione comprende i primi cinque capitoli del documento.

IT Governance Institute®

L'IT Governance Institute (ITGI™) (<http://www.itgi.org/>) è un ente di ricerca, indipendente e no-profit, che fornisce linee guida per la comunità di business internazionale sui temi legati alla *governance* degli asset IT. ITGI è stato creato dall'associazione no-profit **ISACA** (<http://www.isaca.org/>) nel 1998 per aiutare l'alta direzione ed i professionisti IT nella gestione dei rischi connessi all'erogazione dei servizi informatici garantendo l'allineamento degli stessi con gli obiettivi dell'azienda, l'allocazione propria delle risorse IT e la misurazione delle performance. ITGI ha anche sviluppato i *Control Objectives for Information and related Technology* (COBIT®) e Val IT™, ed offre risorse in formato elettronico, ricerche originali e casi di studio sia per assistere il top management ed il Consiglio di Amministrazione nelle attività di IT Governance sia per aiutare i professionisti IT ad erogare servizi informatici ad alto valore aggiunto.

Disclaimer

ITGI ha ideato e realizzato questa pubblicazione, intitolata “*Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework Exposure Draft*” (la “pubblicazione”), principalmente come risorsa di tipo “educativo” per i Chief Information Officer (CIOs), il *senior management* ed il management IT. ITGI e gli autori di questa pubblicazione non forniscono nessuna assicurazione che l'uso di queste linee guida e degli strumenti indicati in questa pubblicazione possano garantire di per sé la conformità alle norme né il successo nei risultati. La pubblicazione non deve essere considerata come comprendente ogni informazione, procedura, test che ragionevolmente può portare allo stesso risultato. Nella determinazione della proprietà di ogni specifico controllo, procedura o test, coloro che si occupano di test e controlli devono applicare il proprio giudizio sulle specifiche circostanze di controllo presenti nell'ambiente dell'*Information Technology* (IT) sotto verifica.

Diritti

Copyright © 2009 IT Governance Institute. All rights reserved. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere usata, copiata, riprodotta, modificata, distribuita, visualizzata, memorizzata in un sistema elettronico o trasmessa in qualsiasi forma e con qualsiasi mezzo (elettronico, meccanico, per mezzo di fotocopie, registrato in maniera elettronica o in altro modo) senza l'autorizzazione scritta preliminare dell'IT Governance Institute.

La riproduzione di parte selezionate del documento per uso interno, non commerciale o accademico è permesso ma deve contenere l'attribuzione completa della fonte del materiale. Nessuna altro diritto, o permesso, è concesso rispetto a quest'opera.

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.660.5700
Fax: +1.847.253.1443
E-mail: info@itgi.org
Web site: <http://www.itgi.org>

Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework Exposure Draft
Printed in the United States of America

Ringraziamenti

IT Governance Institute desidera ringraziare:

Authors and Development Team

Dirk Steuperaert, CISA, IT in Balance BVBA, Belgium, Chair
Steven De Haes, University of Antwerp Management School, Belgium
Rachel Massa, CISSP, PricewaterhouseCoopers LLP, USA
Bart Peeters, PwC Advisory, Belgium
Steve Reznik, CISA, PricewaterhouseCoopers LLP, USA

IT Risk Task Force

Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland, Chair
Steven Babb, CGEIT, KPMG, UK
Brian Barnier, IBM, USA
Jack Jones, CISA, CISM, CISSP, Risk Management Insight LLC, USA
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Gladys Rouissi, CISA, Commonwealth Bank of Australia, Australia
Lisa Young, CISA, Carnegie Mellon University, USA

Expert Reviewers

Mark Adler, CISA, CISM, CISSP, CIA, Allstate Insurance Company, USA
Gary S. Baker, CA, Deloitte & Touche LLP, Canada
Dave H Barnett, CISM, CISSP, Applera Corporation, USA
Brian Barnier, IBM, USA
Laurence J. Best, PricewaterhouseCoopers LLP, US
Peter R. Bitterli, CISA, CISM, ITACS Training AG, Switzerland
Luis Blanco, CISA, UK
Adrian Bowles, Ph.D., Sustainability Insights Group (SIG411), USA
Dirk Bruyndonckx, CISA, CISM, MCA, KPMG Advisory, Belgium
Christophe Burtin, CISA, Burtin Corporation International, Luxembourg
Olivia Xardel-Burtin, Luxembourg

Rahul Chaurasia, Student, Indian Institute of Information Technology, Allahabad, India
Roger Debreceeny Ph.D., FCPA, University of Hawaii – Manoa, USA
Steven De Haes, University of Antwerpen Management School, Belgium
Philip De Picker, CISA, National Bank of Belgium, Belgium
Heidi L. Erchinger, CISA, CISSP, System Security Solutions Inc., USA
Robert Fabian, I.S.P., Robert Fabian Associates, Canada
Shawna Flanders, CISA, CISM, ACS, PSCU Financial Services, USA
John Garms, CISM, CISSP, ISSEP, Electric-Tronics Inc., USA
Dennis Gaughan, IBM Trivoli, USA
Yalcin Gerek, CISA, CGEIT, T.A.C. A.S., Turkey
Edson Gin, CISA, CFE, CIPP, SSCP, USA
Gary Hardy, CGEIT, IT Winners, South Africa
Winston Hayden, CISA, ITGS Consultants, South Africa
Jimmy Heschl, CISA, CISM, CGEIT, KPMG Austria
Monica Jain, CGEIT, CSSBB, CSQA, Covansys – A CSC Company, USA
Jack Jones, CISA, CISM, CISSP, Risk Management Insight LLC, USA
Dharmesh Joshi, CISA, CGEIT, CA, CIBC, Canada
Catherine I. Jourdan, PricewaterhouseCoopers LLP, USA
Kamal Khan, CISA, Saudi Aramco, Saudi Arabia
Marty King, CISA, CPA, Blue Cross Blue Shield NC, USA
Terry Kowalyk, Credit Union Deposit Guarantee Corporation, Canada
Denis Labhart, Swiss Life, Switzerland
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Philip Le Grand, Datum International Ltd, UK
Bjarne Lonberg, CISSP, A.P. Moller – Maersk, Denmark
Jo Lusk, CISA, Federal Housing Finance Board, USA
Charles Mansour, CISA, Charles Mansour Audit & Risk Services, UK
Mario Micallef, CGEIT, CPAA, FIA, Malta
Jack Musgrove, CGEIT, CMC, Aline, USA
Paul Phillips, Operational Risk, GRCB Technology, Barclays Bank Plc ???
Andre Pitkowski, CGEIT, OCTAVE, Grupo Pao de Acucar, Brazil
Jack M. Pullara, CISA, PricewaterhouseCoopers LLP, USA
Felix Ramirez, CISA, Riebeeck Associates, USA
Daniel L. Ruggles, CISM, CGEIT, CISSP, PMP, PM Kinetics LLC, USA
Stephen J. Russell, PricewaterhouseCoopers LLP, US
Deena Lavina Saldanha, CISA, UAE
Mark Scherling, USA
Gustavo Adolfo Solis Montes, CISA, CISM, Grupo Cynthus, Mexico
John Spangenberg, SeaQuation, The Netherlands
Robert E. Stroud, CA Inc., USA
John Thorp, CMC, I.S.P., The Thorp Network, Canada
Lance M. Turcato, CISA, CISM, CPA, CITP, City of Phoenix, USA
Kenneth Tyminski, Retired, USA
Erik P. van Heijningen, Ph.D., RA, Bank Mendes Gans MV, The Netherlands
Sylvain Viau, CISA, SVC, Canada
Greet Volders, CGEIT, Voquals NV, Belgium
Thomas M. Wagner, Marsh Risk Consulting, USA
Owen Watkins, ACA, MBCS, Siemens, UK
Clive E. Waugh, CISSP, Digital Insight, Inc., USA
Amanda Xu, CISA, CISM, PMP, Indymac Bank, USA

ITGI Board of Trustees

Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, KPMG LLP, UK, International President
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA, Belgium, Vice President
Yonosuke Harada, CISA, CISM, CAIS, InfoCom Research Inc., Japan, Vice President
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, CGEIT, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President
Robert E. Stroud, CA Inc., USA, Vice President

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President
Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, FHKIoD, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President

IT Governance Committee

Tony Hayes, FCPA, Queensland Government, Australia, Chair
Sushil Chatterji, Edutech Enterprises, Singapore
Kyung-Tae Hwang, CISA, Dongguk University, Korea
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Hugh Penri-Williams, CISA, CISM, CCSA, CIA, Accenture Technology Services, France
Gustavo Adolfo Solis Montes, CISA, CISM, Grupo Cynthus, Mexico
Robert E. Stroud, CA Inc., USA
John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp Management School, and IT Alignment and Governance Research Institute, Belgium

ITGI Affiliates and Sponsors

American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants Inc.
ISACA
ISACA chapters
ITGI Japan
Norwich University
Socitm Performance Management Group
Solvay Brussels School of Economics and Management
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
Analytix Holdings Pty. Ltd.
B Wise B.V.
CA Inc.
Consult2Comply
Hewlett-Packard
IBM
ITpreneurs Nederlands B.V.
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corp.
TruArx Inc.
Wolcott Group LLC
World Pass IT Solutions

INDICE

INDICE	V
INDICE DELLE FIGURE	VI
PREFAZIONE	1
1 RISK IT FRAMEWORK – SCOPO E AUDIENCE DI RIFERIMENTO	6
1.1 DEFINIZIONE DI RISCHIO IT	6
1.2 OBIETTIVI DEL RISK IT FRAMEWORK	6
1.3 AUDIENCE E STAKEHOLDER DI RIFERIMENTO	7
1.4 BENEFICI E RISULTATI	8
2 I PRINCIPI DI RISK IT	10
3 RESPONSABILITÀ E ACCOUNTABILITY PER GLI IT RISK	12
4 CONSAPEVOLEZZA E COMUNICAZIONE	15
4.1 BENEFICI DELLA CONSAPEVOLEZZA E COMUNICAZIONE	15
4.2 CONSAPEVOLEZZA – CULTURA DEL RISCHIO	15
4.3 COMUNICAZIONE DEL RISCHIO – COSA COMUNICARE?	16
4.4 COMUNICAZIONE DEL RISCHIO - STAKEHOLDER	18
5 RISPOSTA AI RISCHI INFORMATICI	20
5.1 SELEZIONE DELLE RISPOSTE AI RISCHI E SCELTA DELLA PRIORITÀ.....	21

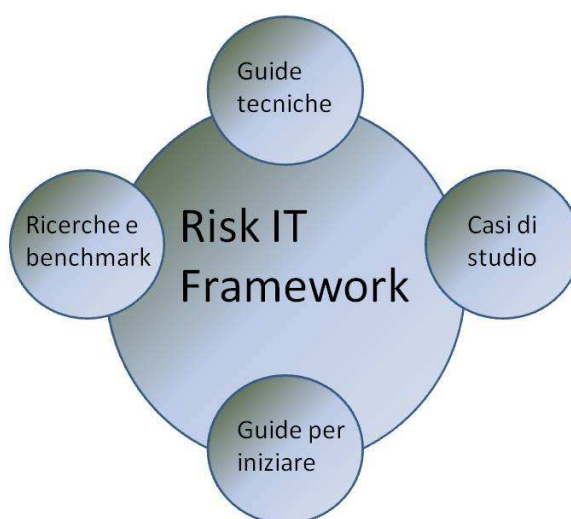
INDICE DELLE FIGURE

FIGURA 1 – EVOLUZIONE DELL’INIZIATIVA “RISK IT”	1
FIGURA 2 – TIPI DI RISCHIO	2
FIGURA 3 – AUDIENCE E BENEFICI	8
FIGURA 4 – RESPONSABILITÀ E ACCOUNTABILITY	13
FIGURA 5 – COMUNICAZIONE DEL RISCHIO	17
FIGURA 6 – FLUSSI DI COMUNICAZIONE DEL RISCHIO E RELATIVI STAKEHOLDER	18
FIGURA 7 – OPZIONI DI RISPOSTA AI RISCHI E PRIORITÀ	22

PREFAZIONE

Questo documento fa parte dell'iniziativa “**Risk IT**” (<http://www.isaca.org/riskit>) dell'*IT Governance Institute* (ITGI), iniziativa finalizzata ad aiutare le aziende nella gestione dei rischi collegati all'*Information Technology* (IT). Lo sviluppo del *Risk IT framework* si deve ad un team internazionale di esperti e professionisti che ha utilizzato prassi e metodologie diffuse e condivise per la gestione efficace dei rischi informatici. *Risk IT* è dunque un framework basato su un insieme di principi guida e processi caratteristici di business arricchito da linee guida di management conformi a tali principi. Via via che l'iniziativa Risk IT si svilupperà essa verrà integrata con i risultati delle attività di ricerca svolte da questo team, aggiornando le linee guida, inserendo nuovi *case study* e servizi ausiliari di supporto al framework di base (figura 1).

Figura 1 – Evoluzione dell'iniziativa “Risk IT”



Il Risk IT framework è complementare a **COBIT®**¹, anch'esso sviluppato da ITGI, che fornisce un approccio completo e coerente per il governo e la gestione di servizi di alta qualità basati sull'*Information Technology*. Ma mentre COBIT individua le “buone prassi” anche servendosi del *risk management*, il framework Risk IT si concentra sull'obiettivo di identificare, governare e gestire i rischi IT dell'impresa.

I rischi di business possono essere di vario tipo: di credito, strategico, di mercato, legati ai *competitor*, connessi all'*Information Technology*, eccetera.

Il rischio informatico (*IT risk*) è il rischio di business associato con l'uso, l'*ownership*, le procedure, il coinvolgimento, l'influenza e l'adozione dell'informatica in azienda. L'*IT risk* riguarda, dunque,

¹ IT Governance Institute, Control Objectives for Information and related Technology, COBIT® 4.1, 2008, www.itgi.org (versione italiana disponibile sul sito AIEA http://www.aiea.it/html/area_download.html)

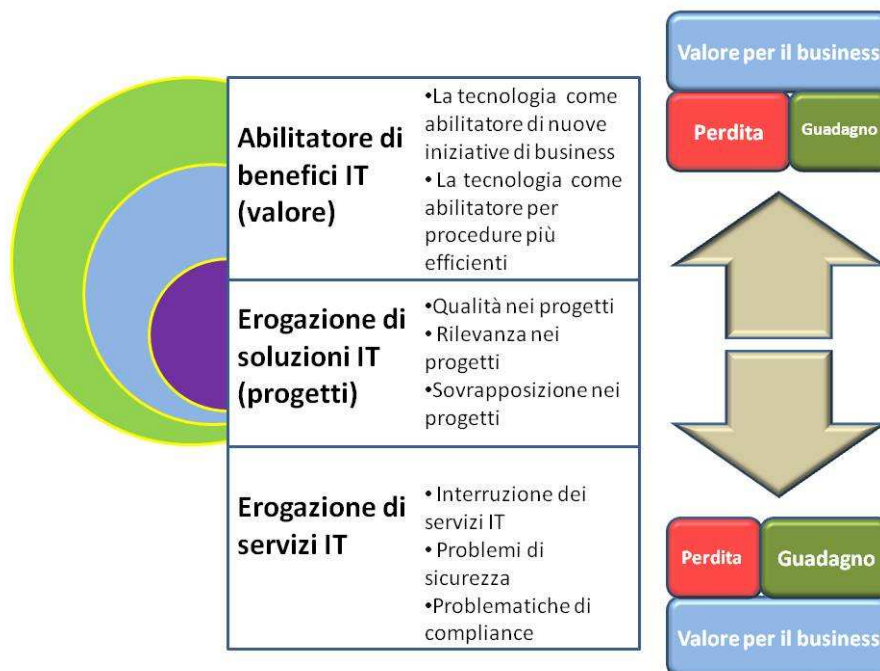
gli eventi connessi all'informatica che possono avere potenzialmente un impatto sul business. Esso prende in considerazione sia la **frequenza** degli eventi incerti sia la **gravità** del possibile impatto di tali eventi; l'IT risk, proprio per la sua natura legata all'incertezza, rappresenta una sfida per il raggiungimento degli obiettivi strategici dell'impresa e può diventare un ostacolo per il conseguimento degli obiettivi aziendali.

Il rischio IT può essere categorizzato in modi differenti (figura 2):

- *IT service delivery risk*, associato con la *performance* e la disponibilità dei servizi IT e che può portare alla distruzione o riduzione del valore d'impresa;
- *IT solution delivery/benefit realisation risk*, associato con il contributo dell'IT alle nuove o più avanzate soluzioni di business di solito nella forma di progetti o programmi;
- *IT benefit realisation risk*, associato con le opportunità (perdute) di usare la tecnologia per migliorare l'efficienza e l'efficacia dei processi di business o per usare la tecnologia come "abilitatore" per le nuove iniziative di business.

Si noti che il rischio IT esiste sempre anche se esso non viene individuato o riconosciuto dall'azienda.

Figura 2 – Tipi di rischio



La figura 2 mostra che per tutte le categorie di IT risk c'è sempre un equivalente "rovesciato". Per esempio:

- *service delivery* – se le prassi per il *service delivery* sono rafforzate l'azienda può ottenere dei benefici ad esempio essere pronta a conquistare ulteriori volumi di transazioni o quote di mercato;
- *project delivery* – il delivery di progetti di successo porta a nuove funzionalità di business.

È importante comprendere e avere costantemente in mente la dualità rischio/opportunità quando si effettuano le decisioni relative al rischio. A volte la decisione può riguardare l'esposizione relativa ad un rischio non gestito rispetto al beneficio potenziale che ne può derivare oppure il potenziale vantaggio che si può ottenere se le opportunità sono colte rispetto ai vantaggi persi se esse non sono colte.

Il Risk IT framework si rivolge ad una vasta *audience* in quanto il *risk management* è un requisito strategico e pervasivo in qualsiasi azienda.

L'*audience* di riferimento comprende:

- alta direzione e componenti del consiglio di amministrazione che hanno la necessità di definire la direzione e monitorare i rischi a livello d'impresa;
- manager dei dipartimenti IT e delle funzioni di business che hanno bisogno di definire i processi di gestione dei rischi;
- professionisti del *risk management* che necessitano di specifiche linee guida per i rischi IT;
- *stakeholder* esterni.

Il *Risk IT framework* completo si rivolge a manager e professionisti che giocano un ruolo nella gestione dei rischi IT. Linee guida aggiuntive sono disponibili nelle "*Risk IT techniques guide*" (qui sintetizzate: una pubblicazione più dettagliata sarà disponibile a breve in forma separata) che comprende esempi pratici, metodologie ed i riferimenti dettagliati di *Risk IT*, rispetto a COBIT e Val IT.

Il framework si basa su principi di standard e framework generalmente riconosciuti per l'*enterprise risk management* quali COSO, ERM² e AS/NZS 4360³ e fornisce le linee guida su come applicare tali principi all'IT.

Risk IT si differenzia dagli attuali documenti e linee guida sull'IT risk che si focalizzano solamente sulla sicurezza informatica; al contrario Risk IT copre tutti gli aspetti dei rischi informatici.

I principi del Risk IT framework sono:

- *governance* d'impresa efficace dei rischi informatici:
 - collegare in continuo i rischi agli obiettivi di business,
 - allineare la gestione dei rischi di business connessi all'IT con l'*enterprise risk management* aziendale,
 - bilanciare i costi ed i benefici nella gestione dei rischi;
- gestione efficace dei rischi informatici:
 - facilitare una comunicazione aperta e onesta sui rischi informatici,
 - definire un "giusto tono" del vertice aziendale nella definizione e valorizzazione delle responsabilità (*accountability*) del personale,

² Committee of Sponsoring Organisations of the Treadway Commission, *Enterprise Risk Management - Integrated Framework*, 2004, www.coso.org

³ Standards Australia, Risk Management, 2004, www.saiglobal.com

- operare all'interno di livelli di tolleranza di rischio accettabili e ben definiti,
- stabilire un processo continuo che rientra nelle attività quotidiane.

Sulla base di tali principi i **blocchi chiave** per la costituzione di una buona gestione del rischio sono:

- definizione delle responsabilità per la gestione dei rischi informatici;
- definizione degli obiettivi e della tolleranza e predisposizione al rischio (*risk appetite*);
- identificazione, analisi e descrizione dei rischi;
- monitoraggio dell'esposizione al rischio;
- gestione dei rischi informatici;
- collegamento e coerenza con le linee guida già esistenti di gestione del rischio.

Intorno a questi “*building blocks*” è stato definito un modello di processo per i rischi informatici che apparirà familiare a chi già conosce COBIT e Val IT⁴: sono infatti fornite linee guida complete e coerenti sulle attività chiave per ciascun processo, per le responsabilità in ogni processo, per i flussi informativi tra i processi e per la gestione della *performance* di ogni processo. I processi sono divisi in tre domini - **Risk Governance**, **Risk Evaluation** e **Risk response** – ciascuno dei quali contiene a sua volta tre processi:

- **Risk Governance:**
 - stabilire e mantenere una visione comune del rischio,
 - integrazione con l'*Enterprise Risk Management*,
 - prendere decisioni di business avendo coscienza dei rischi implicati;
- **Risk Evaluation:**
 - raccogliere i dati,
 - analizzare i rischi,
 - gestire i profili di rischio;
- **Risk Response:**
 - suddividere, articolare il rischio,
 - gestire il rischio,
 - rispondere agli eventi.

Applicando le “buone prassi” dell'IT risk management così come sono descritte in Risk IT permette di fornire benefici tangibili al business come ad esempio minori “sorprese” e “fallimenti” nelle procedure informatiche, maggiore qualità delle informazioni, maggiore fiducia da parte degli *stakeholder* e riduzione delle criticità legate alla *compliance* normativa.

Il Risk IT framework è parte del portfolio dei prodotti di ITGI sull'**IT governance**. Anche se questo framework può essere letto come un documento *standalone*, esso tuttavia prevede riferimenti a COBIT. La guida tecnica rilasciata a supporto di questo framework utilizza in maniera estesa riferimenti a COBIT e Val IT così i manager e i professionisti sono invitati a familiarizzarsi con i principi ed i contenuti più importanti di questi due framework⁵.

⁴ IT Governance Institute, *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, 2008, www.itgi.org. In Italiano è disponibile: Val IT 2.0 - FAQ in italiano <http://www.agatinogrillo.it/content/val-it-20-faq-italiano>

⁵ Vedi www.isaca.org/cobitcampus per la formazione su COBIT

Come COBIT e Val IT, Risk IT è un framework, non uno standard. Ciò significa che le aziende possono e devono personalizzare le componenti fornite nel framework per adattarle alle caratteristiche proprie della loro organizzazione e del loro contesto.

1 RISK IT FRAMEWORK – SCOPO E AUDIENCE DI RIFERIMENTO

1.1 DEFINIZIONE DI RISCHIO IT

Il rischio informatico (*IT risk*) è il rischio di business associato con l'uso, l'*ownership*, le procedure, il coinvolgimento, l'influenza e l'adozione dell'informatica in azienda. L'*IT risk* riguarda, dunque, gli eventi connessi all'informatica che possono avere potenzialmente un impatto sul business. Esso prende in considerazione sia la frequenza degli eventi incerti sia la "gravità" del possibile impatto di tali eventi; l'*IT risk*, proprio per la sua natura legata all'incertezza, rappresenta una sfida per il raggiungimento degli obiettivi strategici dell'impresa e può diventare un ostacolo per il conseguimento degli obiettivi aziendali.

Il rischio IT può essere categorizzato in modi differenti (figura 2):

- *IT service delivery risk*, associato con la *performance* e la disponibilità dei servizi IT e che può portare alla distruzione o riduzione del valore d'impresa;
- *IT solution delivery/benefit realisation risk*, associato con il contributo dell'IT alle nuove o più avanzate soluzioni di business di solito nella forma di progetti o programmi;
- *IT benefit realisation risk*, associato con le opportunità (perdute) di usare la tecnologia per migliorare l'efficienza e l'efficacia dei processi di business o per usare la tecnologia come "abilitatore" per le nuove iniziative di business.

Si noti che il rischio IT esiste sempre anche se esso non viene individuato o riconosciuto dall'azienda.

1.2 OBIETTIVI DEL RISK IT FRAMEWORK

La gestione del *business risk* è una componente essenziale della amministrazione responsabile di qualsiasi impresa. Quasi ogni decisione di business richiede alla direzione generale o ai manager di bilanciare rischi e opportunità.

L'uso pervasivo dell'*Information Technology* (IT) può portare rilevanti vantaggi all'impresa ma anche introdurre dei rischi. Data l'importanza dell'IT sul business generale dell'azienda l'*IT risk* deve essere gestito come qualsiasi altro business risk chiave, come il rischio di mercato, il rischio di credito, e gli altri rischi operativi; tutti questi rischi ricadono sotto una categoria o "ombrello" di rischi più alta: "il fallimento nel raggiungere e garantire gli obiettivi strategici." Ma mentre tutti questi altri rischi da tempo sono entrati nel processo di *decision-making* dell'azienda ancora oggi troppi dirigenti tendono a relegare gli *IT risk* agli specialisti tecnologici al di fuori delle vere "sale di comando".

Il Risk IT framework aiuta nella comprensione dei rischi informatici e "abilita" gli utilizzatori a:

- integrare la gestione dell'*IT risk* nella più ampia gestione dei rischi aziendali;
- effettuare decisioni sulla base di informazioni più complete sull'estensione di rischi, sulla predisposizione a correre rischi e sulla tolleranza accettabile ai rischi dell'azienda;

- migliorare la comprensione sulle possibili azioni di risposta ai rischi.

In breve questo framework permette all'azienda di prendere le appropriate decisioni "basandosi sui rischi".

La realtà e la prassi hanno mostrato che il rischio IT è spesso sottovalutato e non compreso dagli *stakeholder* chiave dell'impresa, compresi i componenti del consiglio di amministrazione e l'alta direzione: in azienda c'è spesso gente in grado di identificare, misurare, monitorare e tenere sotto controllo ogni tipo di rischio aziendale; tuttavia senza una chiara comprensione del rischio IT, il top management e gli *executive* non possono avere un quadro di riferimento completo per fare le giuste scelte sulle priorità e sulla gestione dell'*enterprise risk*.

L'IT risk non è una problematica solamente tecnologica. Sebbene si tratti di una tematica tecnica e sia dunque necessario il coinvolgimento degli esperti IT per la gestione di tale rischio, tuttavia la componente di "business management" è quella più importante. I business manager determinano quali risorse IT siano necessarie per supportare il proprio business, determinano i target di riferimento per l'IT e, di conseguenza, sono i veri "responsabili" (*accountable*) per la gestione dei rischi associati all'IT.

Il Risk IT framework colma il gap tra i framework generici di risk management come COSO ERM e AS/NZS 4360 (ed il suo equivalente britannico ARMS)⁶ ed i framework IT più dettagliati (e principalmente orientati solo alla sicurezza informatica). Risk IT fornisce una visione completa, *end-to-end* ed approfondita di tutti i rischi connessi all'uso dell'IT e spazia dal "tono" e dall'approccio culturale richiesto dal top management fino alle problematiche operative.

In sintesi il framework rende capaci le imprese di comprendere e gestire i vari tipi di rischio IT superando un approccio meramente legato alla sicurezza informatica, considerando invece tutti gli aspetti della gestione dell'IT risk.

Il framework fornisce:

- un insieme di prassi e metodiche di *governance* specifiche per il risk management;
- un framework di processo *end-to-end* per gestire, con successo, l'IT risk;
- una lista generale degli eventi potenzialmente avversi legati all'IT che possono avere un impatto sugli obiettivi di business;
- tool e tecniche per individuare i veri rischi alle procedure IT più importanti senza utilizzare *check-list* generiche di controllo dei requisiti di *compliance*.

1.3 AUDIENCE E STAKEHOLDER DI RIFERIMENTO

L'audience di riferimento per il Risk IT framework è assai ampio in quanto numerosi sono sia i motivi per usare il framework sia i benefici che ciascun gruppo può trovarvi (vedi figura 3). Tutte le "posizioni" indicate nella figura 3 possono essere considerati "*stakeholder*" della gestione dell'IT risk.

⁶ AIRMIC, ALARM, IRM, *A Risk Management Standard*, 2002, www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

Figura 3 – Audience e benefici

Ruolo	Benefici / motivi per usare il Risk IT Framework
Consiglio di amministrazione ed Alta Direzione	Migliore comprensione delle proprie responsabilità e dei ruoli in relazione all'IT risk management
Corporate risk manager (per l' <i>enterprise risk management</i>)	Assistenza a coloro che gestiscono il rischio IT in conformità con in principi dell' <i>enterprise risk management</i> generalmente accettati
Operational risk manager	Collegamento del loro framework a Risk IT; identificazione delle perdite operative o sviluppo degli indicatori chiave di rischio
IT management	Migliore comprensione su come identificare e gestire i rischi IT e su come comunicare l'IT risk a coloro che prendono le decisioni di business
IT service manager	Miglioramento della loro visione dei rischi IT connessi alle procedure informatiche, visione che deve esser integrata nel più ampio <i>IT risk management framework</i>
Business continuity manager	Allineamento con l' <i>enterprise risk management</i> (dato che l' <i>assessment</i> dei rischi è un aspetto chiave delle loro responsabilità)
IT security manager	Posizionamento dei <i>security risk</i> in relazione alle altre categorie di IT risk
Chief financial officer (CFO)	Ottenimento di una visione migliore dei rischi IT e delle loro implicazioni economico finanziarie.
Enterprise governance officer	Assistenza, mediante la loro review ed il loro monitoraggio delle responsabilità di <i>governance</i> , degli altri ruoli di <i>governance</i>
Business manager	Comprensione e gestione del rischio IT – un tra i molti business risk – in relazione alla necessità che tutti i rischi siano allineati
IT auditor	Migliore analisi dei rischi in supporto ai piani di audit e ai relativi report
Regulator	Supporto ai loro <i>assessment</i> sull'approccio aziendale all'IT risk management
Auditor esterni	Linee guida aggiuntive sui livelli di rischio legati all'IT quando si redige una <i>opinion</i> sulla qualità dei controlli interni
Assicuratori	Supporto nello stabilire una copertura assicurativa adeguata per l'IT e nel trovare un accordo sui livelli di rischio accettabili
Agenzie di rating	In collaborazione con gli assicuratori; un riferimento per valutare in modo più obiettivo e dare un rating su come l'azienda gestisce i propri IT risk

1.4 BENEFICI E RISULTATI

Il Risk IT framework gestisce molte problematiche che oggi sono di grande attualità:

1. fornisce una visione accurata sia dei rischi IT correnti e di quelli prevedibili in un prossimo futuro che riguardano l'azienda (inteso in senso esteso) sia delle soluzioni di cui le aziende possono avvalersi;
2. linee guida di dettaglio (*end-to-end*) su come gestire i rischi IT superando la mera visione tecnologica e di sicurezza;
3. comprensione di come “capitalizzare” gli investimenti effettuati sul sistema di controlli IT già in essere per gestire i rischi IT;
4. quando si valutano e gestiscono i rischi IT, l'integrazione con il più ampio sistema di *compliance* aziendale;
5. un framework / linguaggio comune per aiutare a gestire le relazioni tra gli “*executive decision maker*” (consiglio di amministrazione/senior management), il Chief Information Officer (CIO) e l'*enterprise risk management*, o anche tra auditor e management;
6. promozione delle responsabilità sui rischi e la sua accettazione / condivisione in tutta l'azienda;
7. profilo di rischio completo per meglio comprendere le minacce e di conseguenza meglio utilizzare le risorse aziendali.

2 I PRINCIPI DI RISK IT

Risk IT definisce e si fonda su un certo numero di principi guida per la gestione efficace del rischio IT. Tali principi, a loro volta, sono mutuati dai principi “generalmente accetati” dell’*enterprise risk management* applicati al dominio dell’IT. Il Risk IT *process model* è disegnato e strutturato per favorire le imprese nell’applicare tali principi in pratica e per fare confronti e *benchmarking* delle loro performance.

Il Risk IT framework si focalizza sul rischio IT – in altre parole sui *business risk* connessi all’uso dell’IT. La connessione al business è ben illustrata dai principi sui quali il framework è costruito:

- *governance* d’impresa efficace dei rischi informatici:
 - collegare in continuo i rischi agli obiettivi di business,
 - allineare la gestione dei rischi di business connessi all’IT con l’*enterprise risk management* aziendale,
 - bilanciare i costi ed i benefici nella gestione dei rischi;
- gestione efficace dei rischi informatici:
 - facilitare una comunicazione aperta e onesta sui rischi informatici,
 - definire un “giusto tono” dal vertice aziendale nella definizione e valorizzazione delle responsabilità (*accountability*) del personale,
 - operare all’interno di livelli di tolleranza al rischio accettabili e ben definiti,
 - stabilire un processo continuo che rientra nelle attività quotidiane.

I paragrafi che seguono esaminano in dettaglio ciascuno di questi principi.

Governance d’impresa efficace dei rischi informatici e collegamento continuo dei rischi agli obiettivi di business:

- l’IT risk è trattato come un *business risk*, non come un tipo di rischio da questo separato, e l’approccio è completo, coerente e plurifunzionale (*cross-functional*);
- il focus è sui risultati di business; l’IT supporta il raggiungimento degli obiettivi di business e gli IT risk sono espressi nei termini dell’impatto che essi possono avere sul raggiungimento degli obiettivi di business e della strategia;
- ogni analisi dell’IT risk comprende una “analisi di dipendenza” (*dependency analysis*) di come la funzione di business dipenda da tutti gli “strati” che compongono l’infrastruttura IT;
- l’IT risk management è un “abilitatore del business” non un inibitore; l’*IT-related business risk* è analizzato da entrambi i punti di vista: la protezione contro la distruzione del valore ed il contributo alla generazione del valore.

Governance d’impresa efficace dei rischi informatici e allineamento della gestione dei rischi di business connessi all’IT con l’*enterprise risk management* aziendale:

- gli obiettivi di business e la “quantità” di rischio che l’azienda è preparata ad assumersi devono essere chiaramente definiti;

- il processo aziendale di *decision-making* deve considerare l'ampio spettro di conseguenze potenziali ed opportunità che nascono dai rischi informatici;
- la predisposizione (*appetite*) al rischio a livello di entità funzionale riflette la sua filosofia di *risk management* ed influenza la cultura e lo stile operativo (come indicato nel COSO *Enterprise Risk Management - Integrated Framework*);
- le problematiche sul rischio sono integrate per ogni unità di business, cioè la visione sul rischio è comune e consolidata per tutta l'azienda;
- è prevista una "attestazione" o validazione dell'ambiente di controllo.

Governance d'impresa efficace dei rischi informatici e bilanciamento dei costi e dei benefici nella gestione dei rischi:

- il rischio è valutato secondo le priorità e gestito in modo coerente con la predisposizione (*appetite*) e la tolleranza ammesse;
- i controlli sono implementati sulla base di valutazioni ragionevoli e condivisibili; in altre parole: i controlli non sono implementati semplicemente per il gusto di farlo;
- i controlli esistenti sono tenuti in considerazione per gestire i rischi multipli o per garantire maggiore efficienza.

Gestione efficace dei rischi informatici e facilitazione della comunicazione aperta e onesta sui rischi informatici:

- sono scambiate informazioni aperte, chiare, accurate, tempestive e trasparenti sul rischio e tali informazioni sono la base per le decisioni su come gestire i rischi;
- problematiche sui rischi, principi, e metodo di *risk management* sono comuni e coerenti in tutta l'azienda;
- gli aspetti tecnologici sono tradotti in un linguaggio *business-oriented* comprensibile al management.

Gestione efficace dei rischi informatici e definizione di un "giusto tono" dal vertice aziendale nella definizione e valorizzazione delle responsabilità (*accountability*) del personale per operare all'interno di livelli di tolleranza al rischio accettabili e ben definiti:

- le persone "chiave" cioè coloro che sono in grado di influenzare i *business owner* ed i componenti del Consiglio di Amministrazione sono attivamente coinvolti nell'*IT risk management*;
- esiste una chiara assegnazione (ed accettazione) della *risk ownership*: ciò implica una responsabile assunzione dell'*accountability*, la possibilità di effettuare misurazione delle performance e l'integrazione del *risk management* nei sistemi generali di performance; tale impostazione è avallata dalla direzione e dal top management per mezzo di politiche e procedure al corretto livello di responsabilità;
- è promossa una cultura aziendale sensibilizzata al rischio a cominciare dai vertici aziendali; ciò aiuta ad assicurare che coloro che sono coinvolti con la gestione dei rischi operativi si muovono in coerenza con le assunzioni di base del rischio;
- le decisioni relative al rischio sono effettuate dal personale autorizzato a ciò con un focus sul business management, aspetto che gioca un ruolo chiave anche nella gestione dei rischi IT

anche tenendo in conto le decisioni sugli investimenti IT, le attività di ricerca fondi per i progetti, i principali cambiamenti legati agli ambienti IT, i *risk assessment* ed il monitoraggio ed il test dei controlli.

Gestione efficace dei rischi informatici è stabilire un processo continuo che rientra nelle attività quotidiane:

- a causa della natura dinamica e mutevole del rischio, la gestione dell'IT risk è un processo continuo, iterativo, costante; ogni cambiamento produce un rischio e/o una opportunità e l'azienda deve essere preparata a tutto ciò; occorrono piani preventivi, ove possibile, per gestire il cambiamento nella compagine aziendale (*merger ed acquisition*), nella compliance regolatoria, nell'IT, nel business, eccetera ...
- grande attenzione deve essere data all'uso di metodologie coerenti di *risk assessment*, ai ruoli e alle responsabilità, ai tool, alle tecniche, ai criteri in uso in azienda e in modo speciale:
 - all'identificazione dei processi chiave e dei relativi rischi (assegnando le corrette priorità e responsabilità anche in relazione ai profili di rischio),
 - alla comprensione dei possibili impatti sul raggiungimento degli obiettivi,
 - all'identificazione di indicatori e *trigger* che possono indicare se è richiesto un aggiornamento del framework o delle componenti del framework;
- le "*risk management practice*" sono state prioritizzate in modo appropriato ed incluse nei processi aziendali di *decisionmaking*;
- le "*risk management practice*" sono semplici e facili da utilizzare e contengono prassi per intercettare le minacce ed i rischi potenziali così come per prevenirli e mitigarli.

3 RESPONSABILITÀ E ACCOUNTABILITY PER GLI IT RISK

La tabella nella figura 4 definisce un certo numero di ruoli per il *risk management* ed indica dove questi ruoli assumono responsabilità o *accountability* per una o più attività all'interno di un processo. La **responsabilità** si riferisce a coloro che devono assicurare che le attività siano completate con successo. L'*accountability* si riferisce a coloro che hanno la "proprietà" delle risorse richieste e l'autorità di approvare l'esecuzione e/o l'accettazione dei risultati di un'attività all'interno di specifici processi di "Risk IT". Questa tabella è una sintesi delle tabelle di dettaglio contenute nel *process model*.

Figura 4 – Responsabilità e accountability

Definizione del ruolo		Governance del rischio			Valutazione del rischio			Risposta al rischio		
Ruolo	Definizione del ruolo	Visione comune del rischio	Integrazione con ERM	Decisioni sulla base del rischio	Raccolta dei dati	Analisi del rischio	Mantenimento del profilo di rischio	Articolazione del rischio	Gestione del rischio	Reazione agli eventi
Consiglio di Amministrazione	Coloro (con ruolo esecutivo o meno) che sono <i>accountable</i> per la <i>governance</i> aziendale ed hanno il pieno controllo delle sue risorse	A	A							
Chief executive officer (CEO)	La persona di più alto grado che ha la responsabilità della gestione complessiva dell'impresa (Direttore Generale)	A/R	A/R						A	
Chief risk officer (CRO)	Coloro che supervisionano tutti gli aspetti di <i>risk management</i> in azienda. Può essere costituita una funzione di <i>IT risk officer</i> per supervisionare i rischi relativi all'IT.	A/R	R	A/R	A/R	A/R	A	A/R	A/R	A/R
Chief information officer (CIO)	La persona con ruolo più alto (<i>the most senior official</i>) in azienda che è <i>accountable</i> per gli aspetti IT, per l'allineamento dell'IT alla strategia di business, per la pianificazione, la gestione delle risorse e l'erogazione dei servizi IT e delle informazioni, il <i>deployment</i> delle relative risorse umane. Il CIO di solito conduce il <i>governance council</i> che gestisce il portfolio.	R	A/R	A/R	R	A/R	A/R	R	R	R
Chief financial officer (CFO)	La persona con ruolo più alto (<i>the most senior official</i>) in azienda che è <i>accountable</i> per la pianificazione finanziaria, le registrazioni contabili, le relazioni con gli investitori ed i rischi finanziari.	R								
Comitato gestione rischi	Coloro che sono <i>accountable</i> a livello aziendale per la collaborazione e gli accordi consensuali per garantire le attività e le decisioni di <i>enterprise risk management</i> . Può essere costituito un comitato rischi IT (<i>IT risk council</i>) per analizzare più in dettaglio i rischi IT e dare consigli a riguardo al comitato gestione rischi.	R		A/R		R		A		

Enterprise Risk: identificare, governare e gestire i rischi IT, Risk IT Framework – bozza

Business management	Coloro che gestiscono le linee di business con un ruolo formale in relazione alla conduzione dei relativi programmi.	A/R	R	A		A/R	A/R	A	R	R
Owner dei processi di business	Coloro che sono responsabili per l'identificazione dei requisiti di processo, per l'approvazione del disegno del processo e per la gestione delle performance del processo. In generale un <i>business process owner</i> deve avere un ruolo anche formale adeguato e la conseguente autorità per assegnare risorse alle attività specifiche per la gestione dei rischi del processo.	R	R	R	R	R	A/R	R	R	A
Funzioni di controllo del rischio	Le funzioni responsabili, in azienda, per la gestione dei domini specifici di rischio (cioè <i>chief information security officer, business continuity plan – disaster recovery, supply chain, project management office</i>)	R	R	R	R	R	R	R	R	R
Human Resource (HR)	La persona con ruolo più alto (<i>the most senior official</i>) in azienda che è <i>accountable</i> per la pianificazione e le politiche del personale	R								
Compliance e Audit	Le funzioni aziendali responsabili per la compliance e l'audit	R								R

4 CONSAPEVOLEZZA E COMUNICAZIONE

4.1 BENEFICI DELLA CONSAPEVOLEZZA E COMUNICAZIONE

La comunicazione è una componente chiave del *risk management*. I benefici di una comunicazione “aperta” comprendono:

- comprensione da parte dell’*executive management* della reale esposizione ai rischi informatici con la possibilità della definizione di risposte ai rischi appropriate ed informate;
- consapevolezza tra tutti gli *stakeholder* interni dell’importanza dell’integrazione dei rischi e delle opportunità nelle loro incombenze giornaliere;
- trasparenza nei confronti dei *stakeholder* esterni sul livello reale del rischio e sui processi di *risk management* in uso.

Le conseguenze di una comunicazione “povera” comprendono:

- un falso senso di fiducia nel vertice aziendale sul livello della reale esposizione rispetto all’IT e perdita di una direzione unica condivisa per il *risk management*;
- sovra comunicazione sui rischi nei confronti del mondo esterno specialmente se il rischio è elevato o appena sopra un livello accettabile. Questo può impaurire clienti potenziali o investitori o generare ispezioni non necessarie da parte delle autorità di controllo;
- la percezione che l’azienda sta cercando di nascondere rischi noti agli *stakeholder*.

4.2 CONSAPEVOLEZZA – CULTURA DEL RISCHIO

La “consapevolezza del rischio” (*risk awareness*) riguarda la consapevole accettazione che il rischio è parte integrante del business. Ciò non implica che tutti i rischi devono essere evitati o eliminati ma piuttosto che i rischi IT devono essere ben compresi ed analizzati, che le problematiche connesse a tali rischi sono state identificate ed analizzate e che l’azienda conosce ed utilizza i mezzi per gestire i rischi IT.

Una cultura “sensibile al rischio” (*risk-aware*) di solito offre un scenario nel quale le componenti del rischio sono apertamente discusse e c’è una chiara comprensione e condivisione del livello di rischio accettabile. Una cultura *risk-aware* inizia dal vertice aziendale con i dirigenti che definiscono la direzione, comunicano le decisioni prese in relazione ai rischi e ricompensano i comportamenti legati ad una gestione del rischio efficace.

La consapevolezza dei rischi implica anche che tutti i livelli all’interno della azienda sono sensibilizzati su come e perché reagire agli eventi avversi.

Una “cultura dell’accusa” (*blame culture*) deve essere evitata con tutti i mezzi in quanto potrebbe trasformarsi in un potente inibitore della comunicazione. In una cultura dell’accusa le business unit tendono a puntare il dito contro l’IT quando i progetti non sono rilasciati in tempo o non soddisfano i requisiti. Nel far ciò non si riesce a realizzare un vero coinvolgimento delle business unit per ottenere il successo di un progetto. Nei casi più estremi le business unit danno la colpa del fallimento per nascondere di non aver saputo comunicare in modo chiaro. Il “gioco della colpa” ha

il solo risultato di impedire una comunicazione reale ed efficace tra i dipartimenti dell'azienda contribuendo ad ulteriori ritardi.

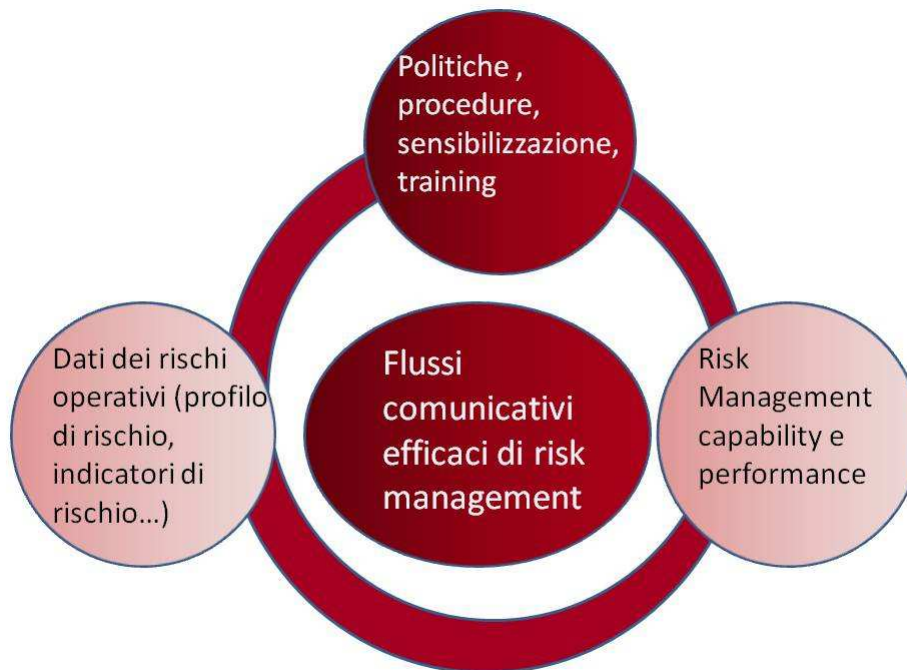
I dirigenti devono essere in grado di identificare e controllare in modo rapido una cultura basata sull'accusa se vogliono che la collaborazione cresca in tutta l'azienda.

4.3 COMUNICAZIONE DEL RISCHIO – COSA COMUNICARE?

La comunicazione sui rischi IT riguarda un vasto spettro di flussi informativi. Risk IT distingue i seguenti principali raggruppamenti di flussi informativi (figura 5):

1. politiche, procedure, consapevolezza, training, continuo rafforzamento da parte del vertice dei principi, eccetera; queste sono le componenti fondamentali della comunicazione globale della strategia dell'azienda per l'IT risk che guida tutte le azioni successive di risk management;
2. risk management *capability* e performance – questo tipo di informazioni permette di tenere sotto controllo il “motore di risk management” aziendale e evidenzia gli indicatori chiave di performance per un risk management efficace; questo tipo di informazioni ha un valore predittivo su come l'azienda è capace di gestire il rischio e ridurre l'esposizione;
3. dati relativi al *risk management* operativo quali:
 - profilo di rischio dell'azienda cioè il portfolio generale dei rischi (identificati) ai quali l'azienda è esposta,
 - cause di fondo per gli eventi di perdita,
 - soglia per i rischi,
 - opzioni (costi e benefici) per mitigare i rischi,
 - dati sugli eventi di perdita,
 - *Key Risk Indicator* (KRIs) di supporto al *management reporting* sui rischi.

Figura 5 – Comunicazione del rischio



Per essere efficace il flusso informativo all'interno di queste categorie deve sempre essere:

- chiaro;
- conciso – l'informazione o la comunicazione non deve travolgere il ricevente; tutte le ben note regole di base della "buona comunicazione" si applicano infatti anche alla comunicazione sui rischi;
- utile – ogni comunicazione sui rischi deve essere rilevante; le informazioni tecniche troppo dettagliate o che sono inviate ad interlocutori inappropriati creano confusione ed ostacoli invece di favorire una chiara visione dei rischi;
- tempestivo – per ogni rischio esistono dei momenti critici tra il momento della sua origine ed il momento del manifestarsi dei suoi possibili effetti sul business; per esempio un rischio può originarsi quando è definita una organizzazione IT non adeguata con la conseguente inefficienza nell'IT service *delivery*; in un altro esempio il punto di origine può scaturire dal fallimento di un progetto e le conseguenze ripercuotersi sulle iniziative di business; la comunicazione è tempestiva quando permette di intraprendere azioni nei momenti appropriati per identificare e gestire il rischio; viceversa non ha nessuna utilità comunicare il ritardo di un progetto una settimana prima della data di conclusione prevista;
- rivolto alla corretta audience di riferimento – l'informazione deve essere comunicata al giusto livello di aggregazione, adattata all'audience di riferimento ed "abilitante" per prendere le giuste decisioni; per esempio un *security officer* può aver bisogno di informazioni tecniche sulle intrusioni e sui virus prima di fare il *deploy* delle soluzioni; un *IT steering committee* non ha bisogno di queste informazioni con lo stesso dettaglio mentre necessita di informazioni aggregate per decidere sui cambiamenti nelle politiche o per approvare budget aggiuntivi per gestire lo stesso tipo di rischio.

4.4 COMUNICAZIONE DEL RISCHIO - STAKEHOLDER

La tabella in figura 6 fornisce una vista d'insieme dei canali informativi più importanti per la comunicazione efficace ed efficiente sul *risk management*. Si tratta semplicemente di una sintesi che non vuole ovviamente rappresentare tutti i flussi comunicativi tra i processi di risk management (il dettaglio è fornito nella descrizione dettagliata dei processi del *process framework*). Lo scopo della tabella è di fornire una *overview* in “una pagina” dei principali flussi comunicativi sull'IT risk che devono esistere in una forma o nell'altra in qualsiasi azienda.

La tabella non include la fonte e la destinazione delle informazioni; esse possono essere trovate nel *process model* dettagliato. Questa tabella si focalizza sulle informazioni più importanti di cui ogni *stakeholder* ha bisogno nei propri processi.

La lista degli stakeholder è differente da quella usata nella figura 4. Alcuni dei ruoli inclusi nella figura 6 sono importanti ma non rappresentano *key player* nel processo generale di *risk management* dell'azienda come mostrato nella figura 4.

Figura 6 – flussi di comunicazione del rischio e relativi stakeholder

Comunicazione dagli altri agli stakeholder	Stakeholder	Comunicazione dagli stakeholder agli altri
<ul style="list-style-type: none"> · Executive summary risk report · Current risk exposure/profile · KRI 	Executive management e consiglio di amministrazione	<ul style="list-style-type: none"> · Predisposizione (<i>appetite</i>) aziendale al rischio · Obiettivi chiave di performance · IT risk RACI chart · Politiche del rischio, tolleranza al rischio definita dal management · Aspettativa sulla consapevolezza del rischio · Cultura del rischio
<ul style="list-style-type: none"> · Ambito e pianificazione dell'IT risk management · Registro dell'IT risk · Risultati della risk analysis · Executive summary risk reports · Integrated/aggregated risk report · KRI 	CRO ed enterprise risk committee	<ul style="list-style-type: none"> · Predisposizione (<i>appetite</i>) aziendale al rischio · Esposizione residua del rischio · Esposizione residua del rischio informativo ed operativo
<ul style="list-style-type: none"> · Predisposizione (<i>appetite</i>) aziendale al rischio · Ambito e pianificazione dell'IT risk management · Obiettivi chiave di performance · IT risk RACI chart · Richiesta di <i>enterprise IT risk assessment</i> · IT risk framework e metodologia di <i>scoring</i> · Registro dell'IT risk · Obiettivi chiave di performance 	CIO CFO	<ul style="list-style-type: none"> · Esposizione residua del rischio · Esposizione residua del rischio informativo ed operativo · Impatto sul business dei rischi IT e business unit impattate · Cambiamenti nel continuo ai fattori di rischio (minacce)

Comunicazione dagli altri agli stakeholder	Stakeholder	Comunicazione dagli stakeholder agli altri
<ul style="list-style-type: none"> · Ambito dell'IT risk management · Piani per il business ordinario e la comunicazione sull'IT risk · Cultura del rischio · Impatto sul business dei rischi IT e business unit impattate · Cambiamenti nel continuo ai fattori di rischio (minacce) · Obiettivi chiave di performance · pianificazione dell'IT risk management · Richiesta di <i>enterprise IT risk assessment</i> · Registro dell'IT risk · Cultura del rischio · Obiettivi chiave di performance · Esposizione residua del rischio · Obiettivi chiave di performance · IT risk RACI chart · pianificazione dell'IT risk management · Monitoraggio della compliance e del controllo 	<p>Business management ed owner dei processi di business</p> <p>IT management (inclusa la sicurezza e la gestione dei servizi)</p> <p>Compliance ed audit</p> <p>HR</p> <p>Compliance ed audit</p> <p>Auditor esterni</p>	<ul style="list-style-type: none"> · Monitoraggio dei controlli e della compliance · Esposizione residua del rischio · Esposizione residua del rischio
<ul style="list-style-type: none"> · <i>Public opinion</i>, legislazione · Executive summary risk report · Tutte le comunicazioni, in generale, rivolte al Consiglio di Amministrazione e all'Alta Direzione 	Regulator	<ul style="list-style-type: none"> · Requisiti per i controlli ed il <i>reporting</i>
<ul style="list-style-type: none"> · Executive summary risk report 	Investitori	<ul style="list-style-type: none"> · Tolleranza al rischio per il loro portfolio di investimenti
<ul style="list-style-type: none"> · Summary risk report, compreso il rischio residuale, il rischio agli asset chiave, i controlli sui livelli di maturità, i risultati di audit · Aspettativa sulla consapevolezza del rischio · Cultura del rischio 	<p>Assicuratori</p> <p>Staff</p>	<ul style="list-style-type: none"> · Copertura assicurativa (proprietà, interruzione del business, D & O) · Problemi potenziali legati all'IT risk

5 RISPOSTA AI RISCHI INFORMATICI

Lo scopo di definire una “risposta al rischio” (*risk response*) è di riportare il rischio residuale (attuale) in linea con il livello di tolleranza al rischio definito dall’azienda. Non si tratta di un compito da svolgere “una volta per tutte” quanto piuttosto di una attività periodica da includere nel ciclo del processo di *risk management*. Per i rischi significativi l’azienda (o l’unità organizzativa) di solito prende in considerazione diversi tipi di risposta ed opzioni. Ciò può provocare dei cambiamenti nello *status quo*.

Le “risposte al rischio” possono essere classificate come segue.

1. Evitare il rischio (*risk avoidance*)

Evitare il rischio significa cancellare le attività da cui nasce il rischio. La “*risk avoidance*” viene applicata quando nessun’altra risposta al rischio appare adeguata cioè quando nessuna altra risposta ha successo nel ridurre la frequenza e l’impatto fino alla soglia definita secondo il *risk appetite*, oppure se il rischio non può essere condiviso o se, in definitiva, il rischio è considerato inaccettabile dal management. Alcuni esempi in ambito IT di *risk avoidance* includono la rilocalizzazione del *data centre* lontano da posizioni che presentano significativi rischi in termini di fenomeni naturali avversi o la decisione di rinunciare a progetti i cui *business case* rivelano una elevata possibilità di fallire..

2. Riduzione mitigazione del rischio (*risk reduction/mitigation*)

Riduzione del rischio significa effettuare una azione che riduce la frequenza o l’impatto del rischio o entrambi. Il modo più comune di rispondere al rischio è di introdurre un certo numero di misure di controllo volte a ridurre sia la frequenza di un evento avverso che potrebbe accadere e/o l’impatto sul business nel caso l’evento effettivamente accadesse.

3. Trasferimento condivisione del rischio (*risk sharing/transfer*)

Condividere il rischio significa ridurre la frequenza del rischio o l’impatto trasferendo o condividendo una parte del rischio stesso. Tecniche comuni comprendono assicurazioni ed *outsourcing*. Esempi comprendono la stipula di una copertura assicurativa in relazione agli incidenti IT, *outsourcing* di parte delle attività IT o condivisione del rischio sui progetti IT con il fornitore per mezzo di accordi sulle tariffe o accordi su investimenti comuni.

4. Accettazione del rischio (*risk acceptance*)

Accettazione significa che non è intrapresa nessuna azione in relazione ad un particolare rischio e che la relativa perdita è accettata nel caso essa occorra. Ciò è differente dall’ignorare il rischio in quanto l’accettazione del rischio presuppone che il rischio è ben conosciuto e che a riguardo venga presa una decisione “informata” da parte del management. Se una azienda adotta la scelta di accettare il rischio occorre considerare con cura chi ha l’autorità di accettare il rischio e ciò tanto più quando si parla di rischio informatico. L’IT risk dovrebbe essere “accettato” solo dal business management (e dall’owner del processo di business) con la collaborazione ed il supporto dell’IT, e tale “accettazione” dovrebbe essere comunicata al senior management ed al Consiglio di Amministrazione.

Ad esempio ci potrebbe essere un rischio che un certo progetto non sia erogato con le funzionalità di business richieste alla data pianificata per il *delivery*. Il management può decidere di accettare il rischio e di andare avanti con il progetto.

L'auto assicurazione (*self-insurance*) è un'altra forma di accettazione del rischio.

Le "Guide tecniche di Risk IT" comprendono vari esempi di "risposte al rischio" e forniscono linee guida più dettagliate su come scegliere e dare priorità alle possibili "risposte". In relazione alla "*risk reduction*" sia COBIT sia Val IT comprendono un set completo e coerente di misure di controllo e le guide tecniche Risk IT offrono linee guida su come i diversi rischi possono essere ridotti usando questi due *framework*.

5.1 SELEZIONE DELLE RISPOSTE AI RISCHI E SCELTA DELLA PRIORITÀ

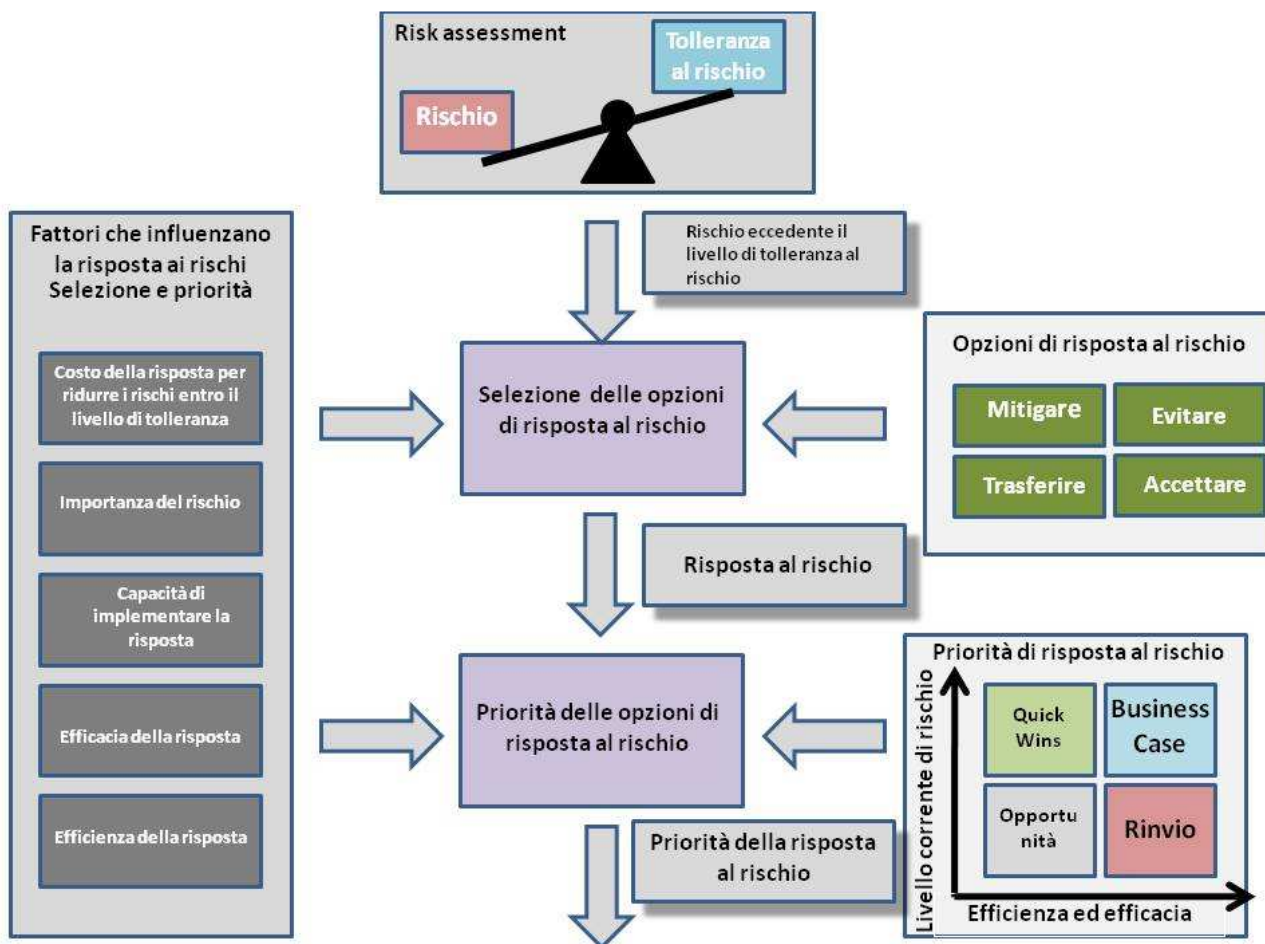
Quando le aziende analizzano il *risk portfolio* ed aggregano i costi e gli sforzi pianificati per le "risposte ai rischi" che sono state pianificate possono trovarsi di fronte alla situazione che la somma totale richiesta ecceda le risorse disponibili. Per questa ragione le aziende devono selezionare e dare una priorità alle "risposte" ai rischi usando i seguenti criteri:

- efficacia della risposta cioè l'estensione alla quale la risposta ridurrà l'impatto e la frequenza degli eventi avversi;
- capacità reale dell'azienda di implementare la risposta;
- importanza del rischio gestito dalla risposta cioè il suo posizionamento nella mappa dei rischi (che riflette la combinazione dei valori dell'impatto e della frequenza)
- efficienza della risposta cioè i benefici relativi forniti dalla risposta in confronto a:
 - altri investimenti relativi all'IT (gli investimenti nella risposta ai rischi implicano sempre misure che sono in competizione con altri investimenti IT o non IT),
 - altre risposte (una risposta può risolvere più rischi mentre un'altra potrebbe non farlo);
- costo della risposta cioè nel caso di trasferimento del rischio il costo del premio assicurativo; nel caso della mitigazione del rischio il costo (spese di capitale, salari, consulenza) per implementare le misure di controllo.

La figure 7 illustra le tipiche risposte ai rischi. Si noti che la decisione sulla priorità della risposta di solito produce più di un risultato:

- vincita veloce (*quick wins*) – risposte molto efficienti ed efficaci ai rischi alti;
- opportunità quando possibile – risposte efficienti ed efficaci per rischi più bassi;
- realizzazione di *business case* – risposte più costose o difficoltose per rischi alti;
- rinvio (*deferral*) – risposte costose a rischi più bassi.

Figura 7 – Opzioni di risposta ai rischi e priorità



Fine della traduzione della prima parte (capitoli 1, 2, 3, 4 e 5)

Roma 10 febbraio 2009