



Giancarlo Butti - Alberto Piamonte

Governance del rischio

Dall'analisi al reporting e la sintesi
per la Direzione



Governance del rischio
Dall'analisi al reporting e la sintesi per la Direzione
di Giancarlo Butti e Alberto Piamonte

Governance del rischio

Dall'analisi al reporting e la sintesi per la Direzione

EDITORE

ITER Srl – Milano
Via A. Sacchini, 20
20131 Milano (MI)
www.iter.it

ISBN: 9788894441536

STAMPA

Digital Book s.r.l.
Via Karl Marx, 9
06012 Cerbara - Città di Castello (PG)

Prima edizione Settembre 2020

Copyright ITER Srl (www.iter.it)

Tutti i diritti sono riservati a norma di legge e a norma delle convenzioni internazionali.

Nessuna parte di questa pubblicazione può essere riprodotta con sistemi elettronici, meccanici o altri, senza l'autorizzazione scritta dell'editore.

Tutti i marchi citati sono registrati dai rispettivi proprietari.

Gli eventuali testi delle normative e di altri documenti riportati nel libro hanno solo finalità indicativa e non hanno alcun valore ufficiale.

Gli unici testi ufficiali delle normative sono quelli riportati sulle pubblicazioni ufficiali dei vari enti emittenti che prevalgono in caso di discordanza.

*Alle piccole Hope
e Spotty
Giancarlo*

Giancarlo Butti (*giancarlo.butti@promo.it*)

(LA BS 7799), (LA ISO IEC 27001), CRISC, CDPSE, ISM, DPO, DPO, CBCI, AMBCI

Master in Gestione aziendale e Sviluppo Organizzativo (MIP - Politecnico di Milano).

Si occupa di ICT, organizzazione e normativa dai primi anni 80:

- analista di organizzazione, project manager, security manager ed auditor presso gruppi bancari
- consulente in ambito documentale, sicurezza, privacy... presso aziende di diversi settori e dimensioni.

Come divulgatore ha all'attivo:

- oltre 800 articoli su 30 diverse testate
- 25 fra libri e white paper, alcuni dei quali utilizzati come testi universitari
- 15 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT sulla sicurezza ICT in Italia
- relatore in oltre 120 eventi presso ABI, ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, TECNA...
- docente in master e corsi di perfezionamento post-universitario in diversi atenei.

Socio di AIEA/ISACA (www.aiea.it – Associazione Italiana Information Systems Auditors), del CLUSIT (www.clusit.it – Associazione Italiana per la Sicurezza Informatica) e di BCI (Business Continuity Institute).

Partecipa ai gruppi di lavoro di ABI LAB, di ISACA-AIEA, di UNINFO, di Oracle Community for security...

Fra i coordinatori di www.blog.europrivacy.info.

Alberto Piamonte (*alberto.piamonte@alice.it*)

Alberto Piamonte, laureato nell'Università di Padova in Ingegneria Elettronica, fa attualmente parte del KeyMap Team, un gruppo di Consulenti ed Aziende che si occupa dello sviluppo di strumenti automatizzati e metodologie per attività di audit, l'analisi e gestione dei rischi, la certificazione conformità e la realizzazione di efficaci ed efficienti sistemi di controllo e di governo.

Oltre che svolgere in prima persona attività di consulenza si occupa attivamente dei problemi relativi al governo dei sistemi IT tenendo frequenti corsi e seminari su metodologie quali COBIT, ITIL e ISO27001 ed alla sensibilizzazione e diffusione delle relative tematiche, è stato Consigliere AIEA con il ruolo di Research Director.

Inizia la sua carriera come ricercatore IBM con permanenza più che decennale nei laboratori di ricerca e sviluppo (USA, Germania, Svezia ed Italia) occupandosi principalmente di comunicazioni (SNA) e relativi problemi di sicurezza.

Successivamente, come Direttore Responsabile del Marketing Olivetti per le Pubbliche Amministrazioni, è stato coinvolti nella gestione e realizzazione di grandi progetti.

Più recentemente come Direttore Software Europa di Amdahl Corporation si è occupato delle problematiche di gestione e sicurezza di grandi reti di utenti.

Socio di ISACA – Roma, COBIT5 Trainer, Assessor ed Implementor.

PRESENTAZIONE	1
INTRODUZIONE.....	2
I RISCHI.....	3
Il concetto di rischio	3
Tipologia di rischi.....	4
LA GESTIONE DEL RISCHIO	11
Standard per la gestione del rischio	11
Metodologie per la gestione del rischio	14
I ruoli nella gestione dei rischi	15
L'ANALISI DEI RISCHI	17
Un approccio all'analisi del rischio a più livelli	17
Terminologia dell'analisi dei rischi	20
Metodologie per l'analisi dei rischi.....	22
Aspetti trasversali nella analisi dei rischi.....	27
Fasi dell'analisi dei rischi.....	29
LA RACCOLTA DELLE INFORMAZIONI	31
Tecniche di raccolta dei dati	31
La verifica documentale.....	31
Le informazioni da raccogliere in ambito ICT	33
Fonti dati sulle risorse.....	33
LA MAPPATURA DEGLI ASSET	39
Gli asset dal punto di vista dell'azienda.....	39
La conoscenza	42
La classificazione delle informazioni.....	45
I documenti.....	48
I documenti elettronici	48
Il sistema informativo	49
Il ciclo di vita delle informazioni	50
I flussi documentali.....	51
Il capitale umano	54
Competenze/Conoscenze	54
Altri asset immateriali.....	58
La collocazione degli asset aziendali.....	58

Correlazione fra gli asset	58
Struttura gerarchica.....	60
Cataloghi di asset.....	64
I servizi.....	67
I processi.....	68
Cataloghi di processi.....	70
Le finalità di trattamento.....	73
Cataloghi delle finalità	73
MINACCE E VULNERABILITÀ	77
Gli eventi di minaccia.....	77
Classificazione delle fonti di minacce	81
Le Vulnerabilità.....	85
Cataloghi delle minacce e delle vulnerabilità	86
MISURE DI SICUREZZA.....	91
Classificazione delle Misure di Sicurezza	91
Ciclo di vita delle misure di sicurezza	92
Coerenza nelle contromisure	93
Differenza nelle contromisure	95
Cataloghi delle misure di sicurezza.....	95
Misure di sicurezza - Policy e Procedure	103
PROBABILITÀ E IMPATTI.....	109
Valutazione della probabilità.....	109
Valutazione degli impatti.....	116
Esempi di scale di impatto	121
Registro “Qualitativo” Minacce-Probabilità-Impatti	127
UN NUOVO APPROCCIO ALLA CYBERSECURITY	129
Evoluzione da qualitativo a quantitativo	129
Da IT Security a Cybersecurity: standard ISO/IEC 27032:2012	129
Misura del rischio Cybersecurity	131
Da Qualitativo a Quantitativo: sostituzione uno-a-uno.....	134
L’esperto come strumento della valutazione	135
Loss exceedance curve	139
Visualizzare il rischio.....	140
La tolleranza al rischio: come descriverla in termini statistici	140
Supporto alle decisioni: ROSI.....	141
Come migliorare le stime.....	141
La taratura delle stime di probabilità	142
Riduzione dell’incertezza con metodi statistici	143
Set di utility Excel personalizzate.....	144
AGGREGAZIONI E CORRELAZIONI DEI RISCHI.....	145
Somma dei rischi e Calcolo della rischiosità totale.....	145

Rischi indipendenti	146
Rischi correlati	146
Perché un approccio “rischio totale”	147
FACTOR ANALYSIS OF INFORMATION RISK (FAIR)	151
Posizionamento rispetto ad altri Standards / Frameworks	154
CONCETTI, FORMULE E STRUMENTI EXCEL.....	159
Definizione delle scale di misura	159
Le possibili scale di misura.....	159
Scale qualitative.....	162
Scale quantitative	163
RISCHIO QUANTITATIVO.....	167
ALE (Annualized Loss Expectancy)	167
Indice di Rischiosità normalizzato (rn).....	167
Somma o moltiplicazione?.....	169
Definizione delle scale logaritmiche, probabilità ed impatti	169
Indice di rischio normalizzato	172
IL TRATTAMENTO DEL RISCHIO.....	175
L’attivazione delle contromisure	177
Il trasferimento del rischio	179
Il ciclo dell’analisi del rischio.....	180
ALLEGATO A.....	181
ALLEGATO B.....	189
ALLEGATO C.....	195
Analisi dei Rischi dal punto di vista del GDPR.....	195
Determinazione analitica della valutazione di impatto	201
Altri rischi per i diritti e le libertà fondamentali delle persone fisiche.....	203
Confronto fra analisi del rischio dal punto di vista dell’azienda e del GDPR.....	204
Il trattamento del rischio dal punto di vista del GDPR	205
ALLEGATO D.....	207
ALLEGATO E	211
ALLEGATO F	213
INDICE ANALITICO	215