Processo di gestione del rischio d'informazione finanziaria

Chiara Cornalba
Deltas S.p.A.

GRUPPO BANCARIO
Credito Valtellinese

"La comunicazione finanziaria"
Sondrio, 9 marzo 2010

Agenda

- Vincoli di conformità alla L. 262/20005
- Soluzioni operative
- Nuove sfide per il futuro

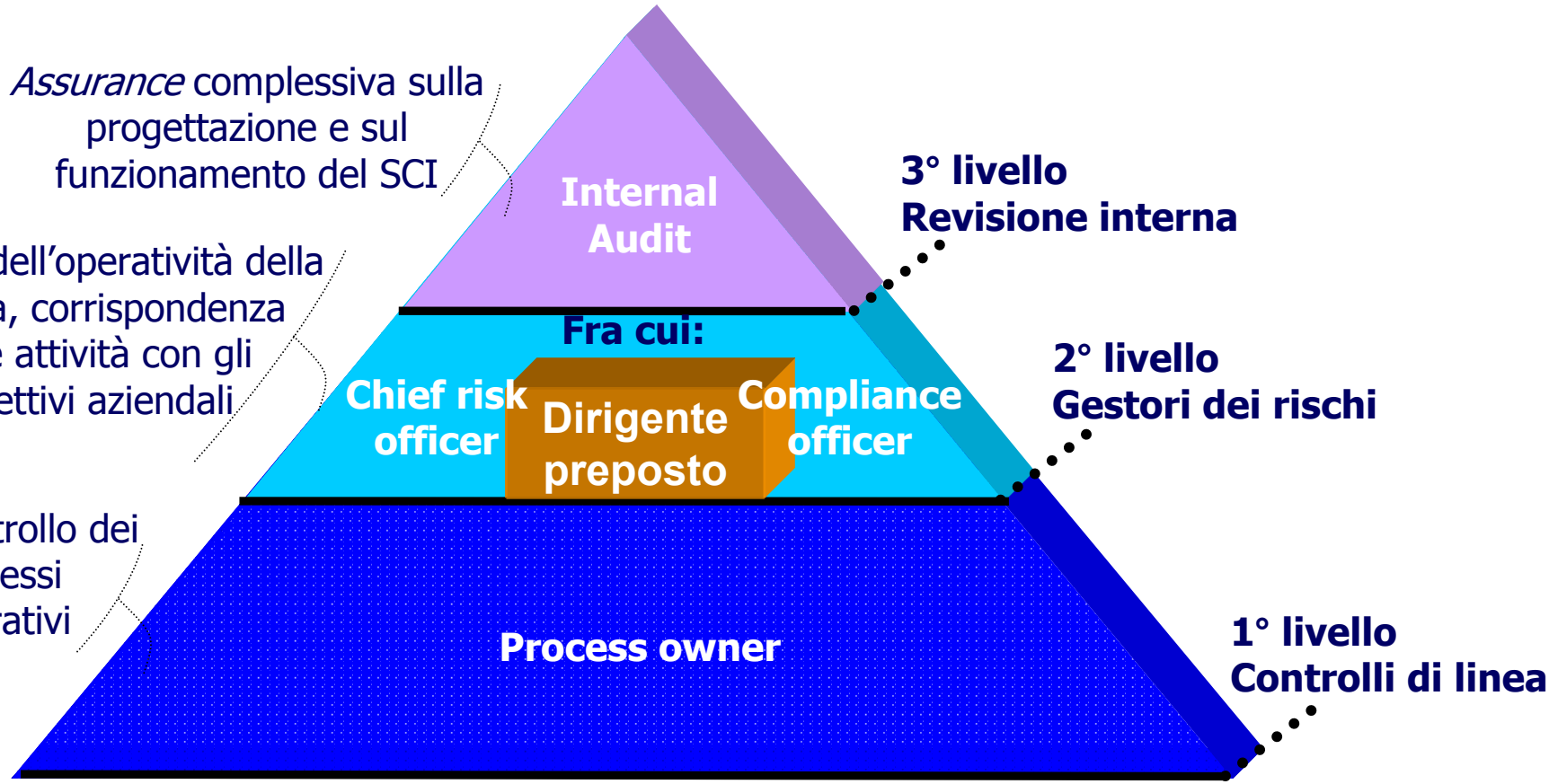
Rischio d'informazione finanziaria

Per gli emittenti quotati aventi l'Italia come Stato membro d'origine, l'articolo 154-bis del TUF impone un obiettivo di affidabilità e d'integrità dell'informazione finanziaria

Cambiamento culturale e organizzativo

Adeguatezza ed effettiva applicazione delle procedure amministrative e contabili per la formazione del bilancio	**Conformità dei documenti e loro corrispondenza alle risultanze dei libri e delle scritture contabili**	**Idoneità dei documenti a fornire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria**	**Attendibilità della relazione sulla gestione (andamento e risultato della gestione, descrizione dei principali rischi e incertezze)**

Sistema di controllo interno



Obiettivi | Soggetti | Funzione

Cfr. Banca d'Italia, *Istruzioni di Vigilanza per le banche*, Circolare n. 229, Tit. 9, p. 4, 1999 modificata e aggiornata da disposizioni successive

Rischio d'informazione finanziaria

E' il rischio attuale o prospettico d'incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie o danni reputazionali in conseguenza di violazioni di leggi, regolamenti o di autoregolamentazione riguardanti gli atti e le comunicazioni della società relativi all'informativa contabile.

Regole comuni per il governo dei rischi

Il processo di gestione del rischio d'informazione finanziaria segue le regole di un qualunque processo di *risk management*

- "ISO Risk management – Vocabulary", Guide n. 73, novembre 2009, Organizzazione internazionale per gli standard (Iso);
- "Iso 31000, Risk management – Principles and guidelines" (2009), Organizzazione internazionale per gli standard (Iso);
- "COSO Enterprise Risk management framework" (2004), Committee of Sponsoring Organizations della Treadway Commission;
- "Risk Management Standard" (2003), Federation of European Risk Management Associations;
- Standard di risk management (ad es. Australia, Nuova Zelanda);
- …

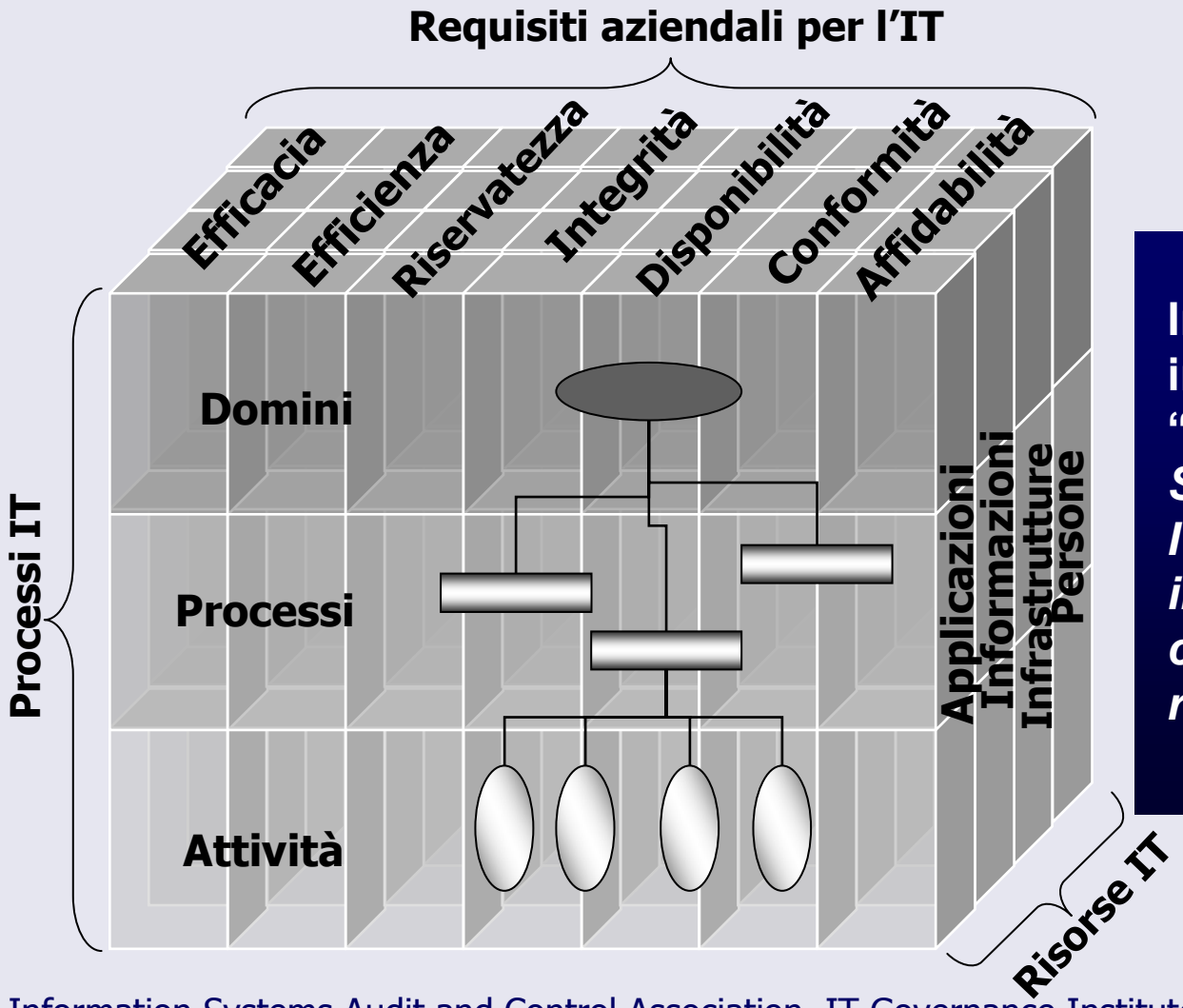
Framework di gestione del rischio

International Organization for Standardization, *Iso 31000, Risk management – Principles and guidelines*, novembre 2009

Il modello COSO

Committee of Sponsoring Organizations (Treadway Commission),
COSO Report - Internal Control. Integrated Framework, settembre 1992.

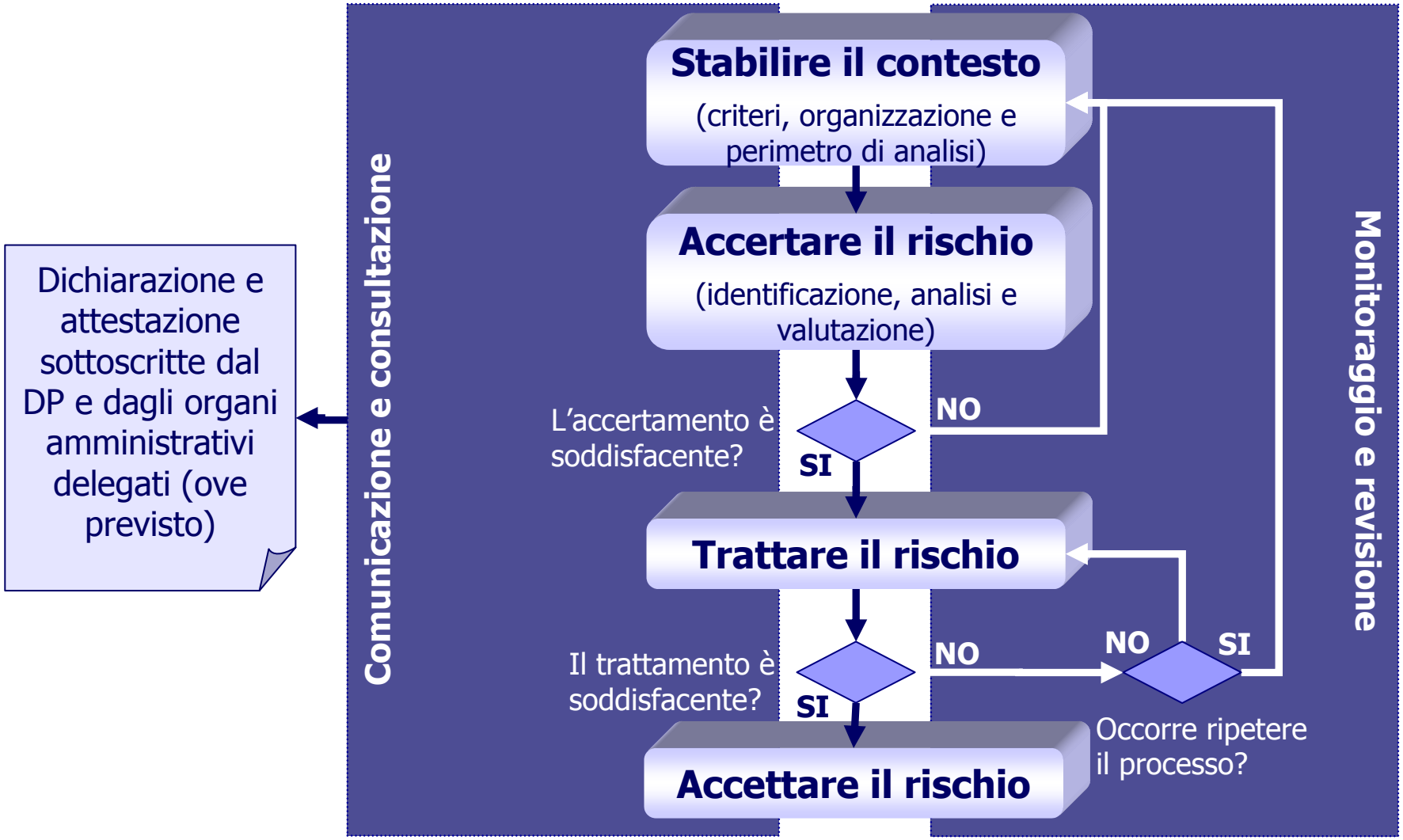
Il modello COBIT



Integrazione tra IT e informazione finanziaria: "*IT Control Objectives for Sarbanes-Oxley. The role of IT in the design and implementation of internal control over financial reporting*" (2004, 2006).

Information Systems Audit and Control Association, IT Governance Institute, *Control Objectives for Information and related Technology*, 1992.

Processo di gestione del rischio d'informazione finanziaria



Stabilire il contesto

Criteri di base

Avere almeno una visione generale sulle regole di:

- analisi,
- valutazione,
- accettazione dei rischi.

Regole di determinazione della magnitudo

Organizzazione

Stabilire se:

- i mezzi e i poteri messi del DP siano idonei;
- le risorse delle unità organizzative siano adeguate;
- esistono eventuali sovrapposizioni funzionali.

Perimetro di analisi

Identificare la sua composizione, considerando la natura del rischio e l'obiettivo del processo di gestione.

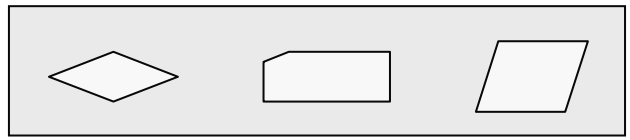
Onere operativo, principi di coerenza e proporzionalità.

Accertamento del rischio

Identificazione del rischio

- Selezione del perimetro di analisi
- Formalizzazione dei processi rilevanti
- Identificazione dei rischi
- Analisi del rischio
- Valutazione del rischio

Ambiente aziendale
Information Technology
Processi amministrativi e contabili

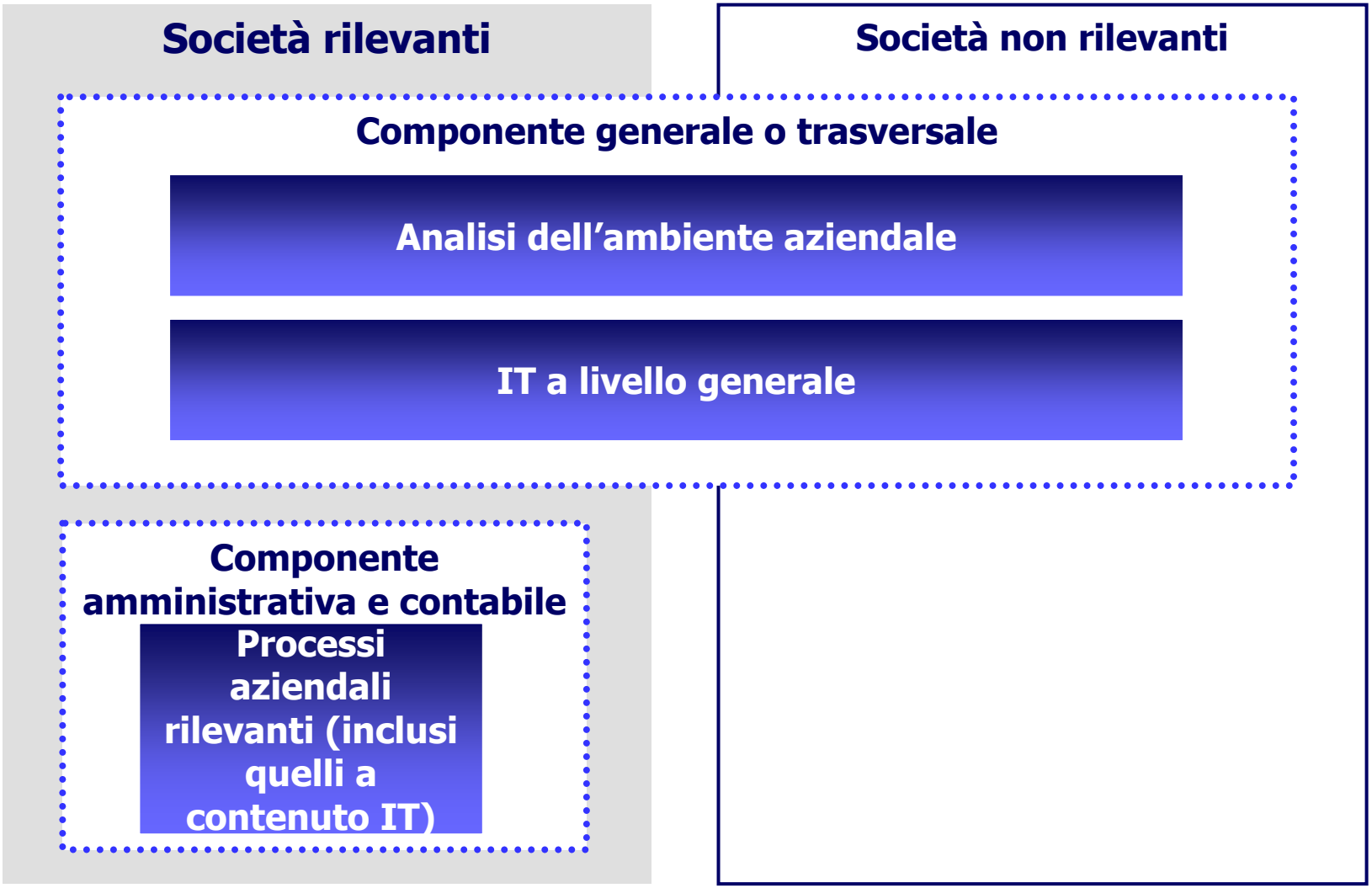


Rischio 1
Rischio 2
Rischio 3
Rischio 4

E	D	C
D	C	B
C	B	A

Priorità d'intervento
E – rischio
D - rischio
D - rischio

Modello di selezione del perimetro d'analisi del RIF



Selezione del perimetro di analisi

Aree che possono incidere sul RIF

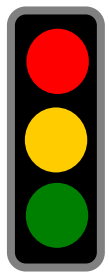
Società nei gruppi d'imprese

Processi amministrativi e contabili

Information Technology

Ambiente aziendale

PE
RIM
TE
RO



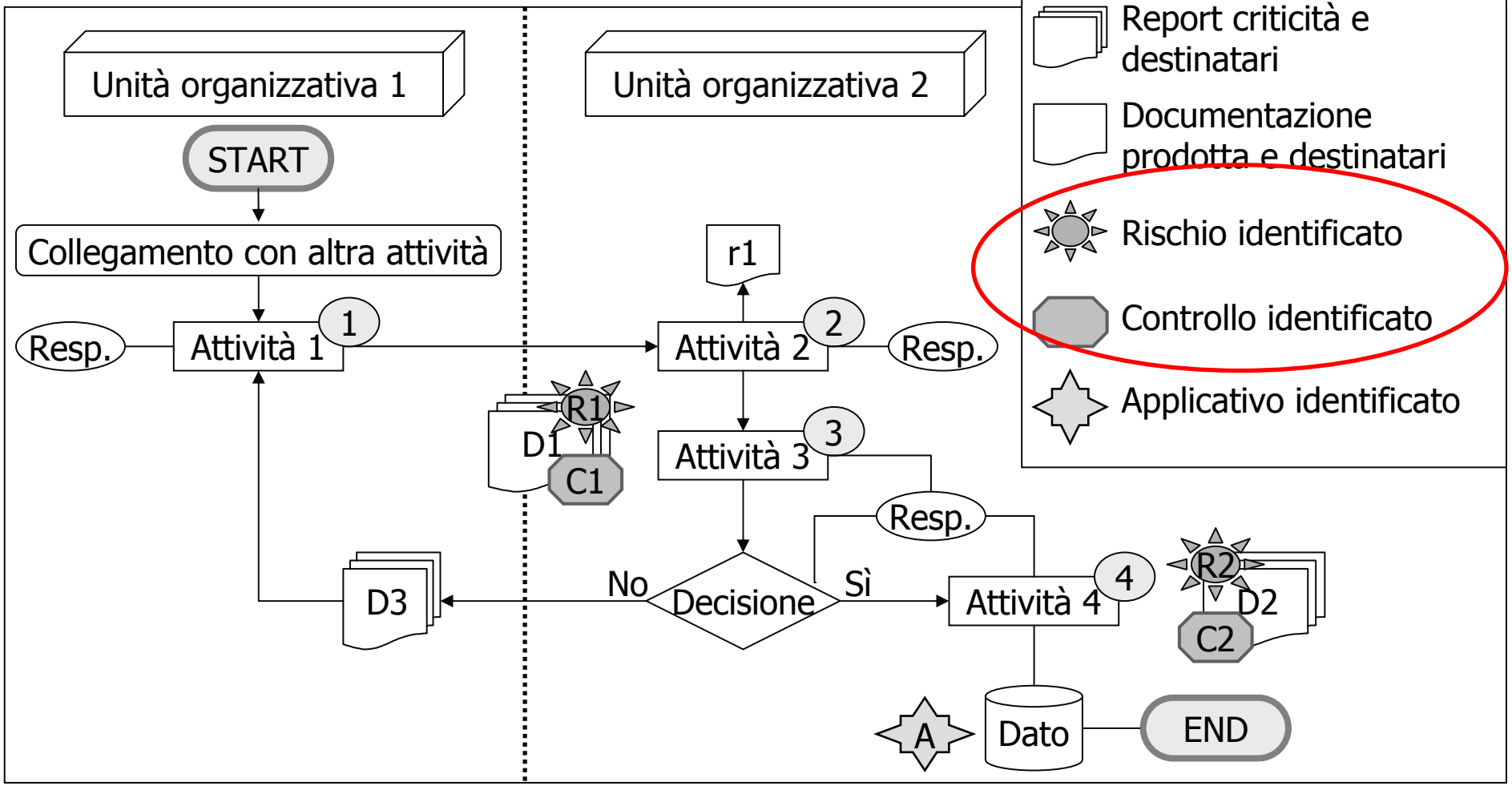
Soglie d'infrazione e criterio di rilevanza basato sul concetto di materialità

Granularità del filtro: principio di prudenza e costi

Priorità d'analisi: accertamento dei rischi e formalizzazione dei processi aziendali

Es. società quotata o con domanda di quotazione, che opera con paesi non trasparenti
Saldo contabile con valori stimati

Formalizzazione del processo aziendale



Identificazione dei rischi

Il processo di scoperta, elencazione e descrizione degli elementi (fonte, eventi, cause e conseguenze) di un rischio.

Analizzare ciò che può causare potenzialmente un danno, i controlli esistenti e gli elementi di debolezza aziendali che se correlati a cause generano un evento avverso.

Insieme di eventi o accadimenti che possono causare sanzioni, perdite finanziarie o danni di reputazione in conseguenza di violazioni di leggi, regolamenti o di autoregolamentazione riguardante gli atti e le comunicazioni della società relativi all'informativa contabile (es. errori, incongruenze, non correttezze e attività mancanti).

Identificazione dei rischi

- **E' possibile utilizzare diversi metodi, anche combinati tra loro:**
  - *brainstorming* tra gruppi di risorse appositamente costituiti ed eventualmente distinti per le aree identificate nel perimetro d'analisi;
  - interviste o somministrazione di questionari a risposta aperta/chiusa con i *process owner* ed esperti operanti nel perimetro d'analisi;
  - analisi di scenario e "*what-if*": per aree d'interesse meno tangibili, come l'ambiente aziendale;
  - *check-list* dei potenziali eventi avversi: quando risorse economiche, personale o tempi per realizzare il processo di *risk management* siano limitati;
  - studio dei *work-flow* di processo schematizzati mediante *flow-chart*: se l'effetto atteso al verificarsi di un evento avverso sia elevato.
- **La scelta dipende dal contesto, dalle conseguenze attese dal verificarsi di un evento avverso e dalle risorse disponibili (economiche e umane).**

Identificazione dei rischi

IT

Argomenti	Domande
Processi IT, organizzazione e relazioni	I sistemi e le basi di dati più importanti sono state censite e ne sono stati identificati gli *owner*?
	I ruoli e le responsabilità dell'organizzazione IT sono definite, documentate e ben comprese?

RISCHI

Ambiente aziendale

Mancata comunicazione del codice di condotta/etico a parte o tutta l'organizzazione

Inesistenza di/carenza del sistema di formazione del personale

Processi amministrativi e contabili

Stime non corrette derivanti da errate interpretazioni dei fatti

Alimentazione "matricini" non completa

IT

Inesistenza del sistema di archiviazione dei dati

Mancato censimento dei sistemi e delle basi di dati più importanti

Scheda del rischio

Descrizione

Società

Business unit

Soggetto rilevante

Soggetto responsabile della gestione

Rischio

Nome: ---

Codice: ---

Categoria: informazione finanziaria ---

Dettaglio

Tecnica utilizzata per rilevare il rischio: ---

Motivo per cui si è proceduto alla fase d'identificazione: ---

Fonti informative utilizzate: ---

Descrizione del rischio: agisce a livello di gruppo, singola impresa o processo, correlazione con altri rischi, modalità con cui si manifesta, effetti generati ---

Collocazione del rischio all'interno del processo: indicare anche un riferimento incrociato con il work-flow di processo ---

Misurazione

Holding period

In assenza di controlli

Frequenza/probabilità di accadimento: ---

Misura della dimensione dell'impatto: precisare se diverso da quello economico ---

In presenza di controlli

Frequenza/probabilità di accadimento: ---

Misura della dimensione dell'impatto: precisare se diverso da quello economico ---

Note

Livelli di propensione, accettazione e tolleranza al rischio: ---

Descrizione delle tecniche adottate per il trattamento: rif. Scheda sui controlli (*) ---

Eventuali attività già programmate per il trattamento, mediante suo controllo: descrivere l'effetto atteso ---

Annotazione del rischio: indicare il riferimento ---

(*) Nel caso d'intervento sul rischio, solitamente le tecniche prescelte considerano anche i presidi predisposti la cui descrizione è contenuta in una specifica scheda cui è opportuno rimandare per praticità operativa.

Identificazione dei controlli

La stima e la valutazione del livello del rischio dipendono dalle caratteristiche dei controlli che operano nel perimetro d'analisi.

Se mal progettati o non funzionanti in modo adeguato, vi possono essere delle vulnerabilità.

In presenza di duplicazioni, ci possono essere inefficienze.

ESEMPI

Ambiente aziendale

Policy e ogni altra regola che chiarisca in modo esplicito come costruire, mantenere e sviluppare un idoneo ambiente aziendale

Processi amministrativi e contabili

Controlli contabili e di ragioneria generale

Controlli amministrativi

IT

Ambiente tecnologico, procedure informatiche, accesso ai programmi e ai dati, sviluppo e gestione di modifiche ai programmi software e loro manutenzione

Scheda del controllo

Descrizione

Società

Business unit

Soggetto rilevante

Responsabile del controllo

Controllo

Nome: ---

Codice: ---

Dettaglio

Tipo, descrizione e obiettivo del controllo: es. abilitazione delle operazioni ---

Agisce a livello di gruppo, singola impresa o processo: ---

Collocazione dell'attività all'interno del processo: per creare un riferimento incrociato con il work-flow di processo ---

Natura

Controllo specifico per il rischio d'informazione finanziaria: sì/no

Utilità del controllo per scopi diversi dalla conformità all'art. 154-bis TUF: es. D.Lgs. 231/2001

Controllo: preventivo, concomitante o successivo --- di linea o direzionale ---

manuale, automatico o semi-automatico ---

frequenza di esercizio: es. giornaliero, settimanale, mensile, trimestrale ---

Modalità d'azione

Agisce sull'asserzione di bilancio: esistenza sì/no --- completezza sì/no ---

diritti ed obblighi sì/no --- valutazione sì/no ---

manifestazione sì/no --- misurazione sì/no ---

presentazione e informativa sì/no ---

Agisce su una policy di gruppo: specificare, Circ. n. XX "Titolo" del GG.MM.AAAA ---

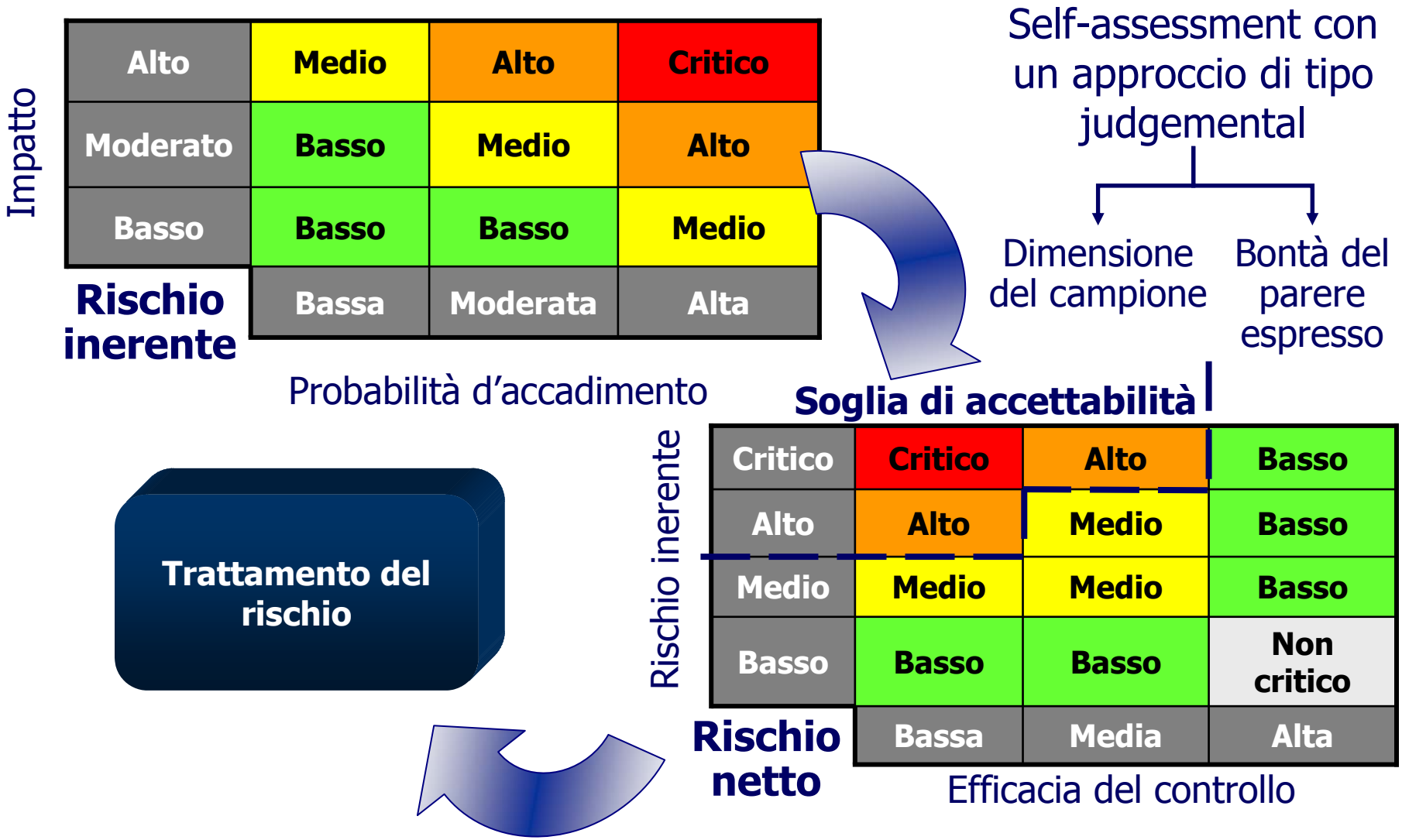
Agisce su elementi di natura IT: specificare, es. piano "IT security" approvato il GG.MM.AAAA ---

Agisce su uno o più rischi identificati: specificare l'insieme di rischi correlati utile per determinare i cd. key control ---

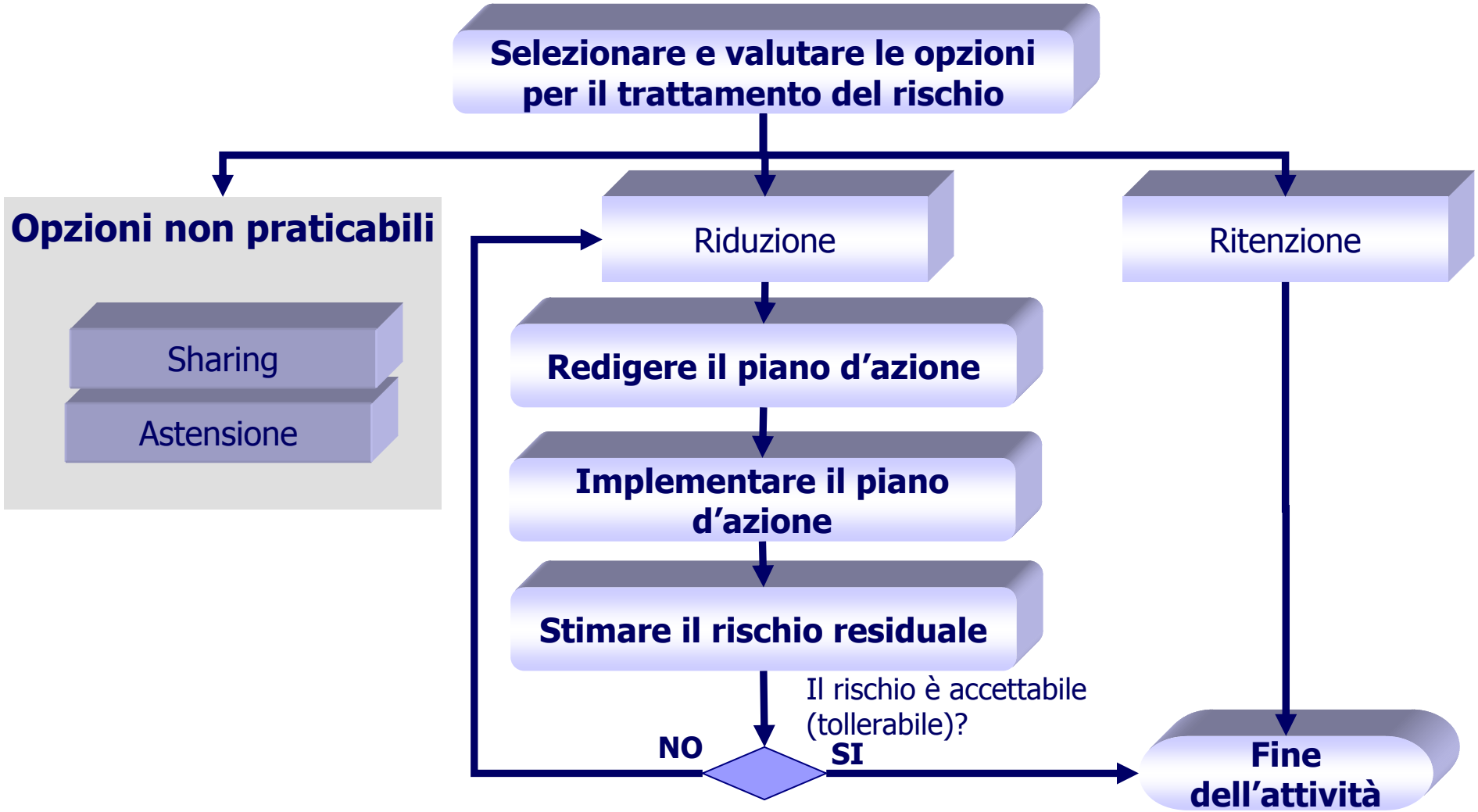
Note

Eventuali attività già programmate per il suo miglioramento: riferimento al piano d'attività e descrivere l'effetto atteso ---

Stima e valutazione dei rischi



Trattamento del rischio



Trattamento del rischio

Trattamento

Di diverso tipo:

- prevenzione di altri eventi avversi,
- riduzione dell'impatto,
- aumento della consapevolezza del rischio.

Esempi:

• introdurre una specifica procedura;

• impostare una password di identificazione per accedere a dati sensibili.

Piano d'azione

Un insieme articolato di azioni da implementate.

Ad ogni piano è associato un ordine di priorità per la sua realizzazione. Dipende dalla dimensione della gravità della carenza riscontrata.

Rischio residuale

Definire se il nuovo livello di rischio stimato sia accettabile o, al contrario, occorre predisporre un altro piano di trattamento.

Monitoraggio, revisione, comunicazione e consultazione

Monitoraggio e revisione

La messa a regime del sistema di gestione del rischio non è sufficiente per l'adempimento normativo nel tempo.
Occorre predisporre un'attività di manutenzione continuativa nel tempo e di revisione periodica del rischio residuale.

Comunicazione e consultazione

Report contenenti gli elementi necessari e utili alla formalizzazione dei documenti che contengono lo svolgimento e la realizzazione di ciascuna fase operativa

Attestazione e dichiarazione

Il modello ERM (COSO II)

Committee of Sponsoring Organizations, *Enterprise Risk Management – Integrated Framework*, settembre 2004

Il modello COSO III

***Internal Control over Financial Reporting – Guidance for Smaller Public Companies*, 2006:**

- predisposto per le imprese di piccole dimensioni;
- specifico per il *financial reporting*.

E' per la Treadway Commission e gli operatori di settore una raccolta di raccomandazioni a valenza generale, indipendenti dalle dimensioni aziendali.

Componenti di controllo

Monitoraggio
Informazioni e comunicazione
Attività di controllo
Valutazione del rischio
Ambiente di controllo

Venti principi