ICT RISK MANAGEMENT

Società KAPPA

Introduzione

Carlo Guastone, Convegno AIEA – Analisi dei rischi, Verona 26 maggio 2006

APPROCCIO ALLA GESTIONE DEL RISCHIO

- Definizioni
- Metodologie per il Risk Management
- Master Plan per la Gestione dei Rischi

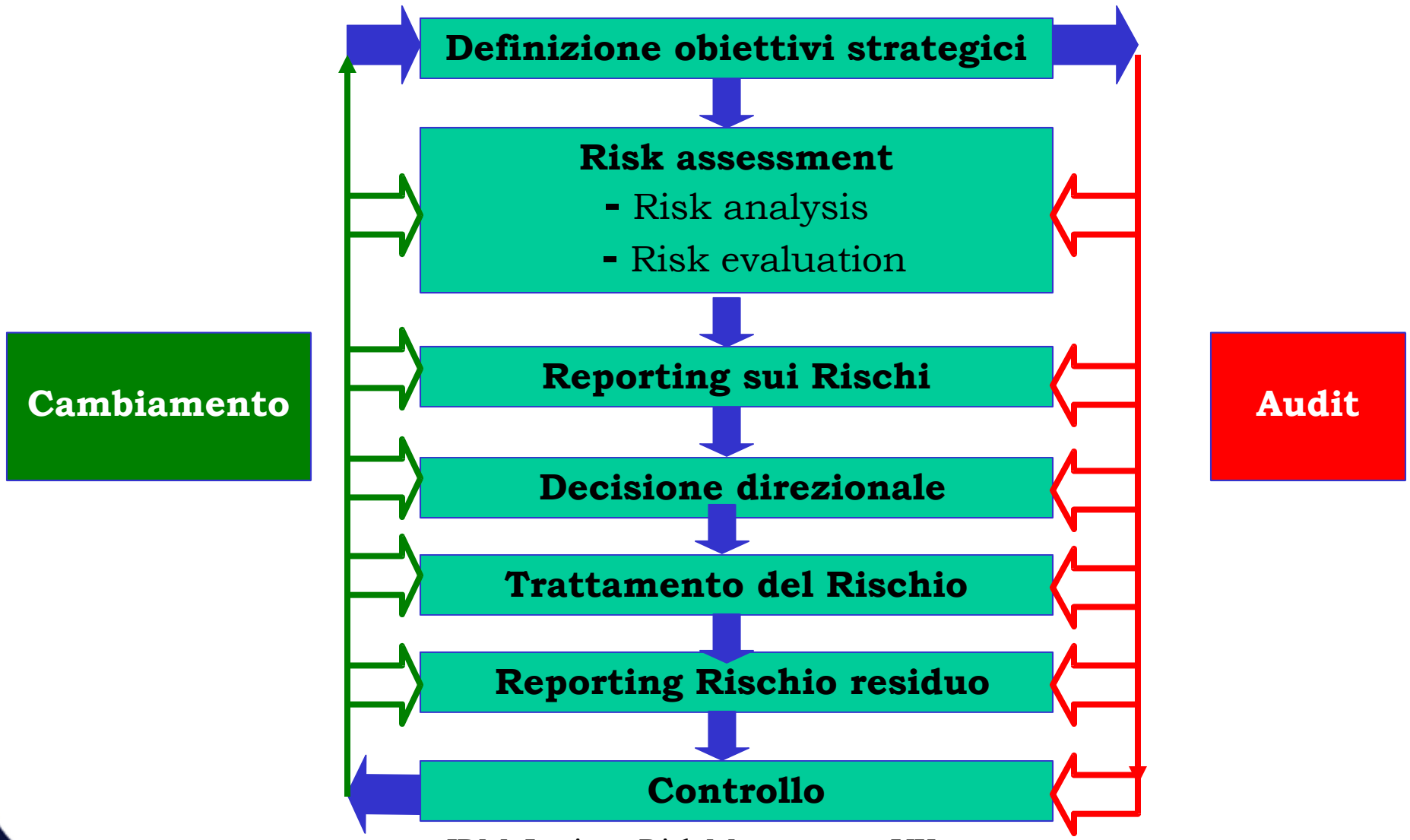
Cos'è il Risk Management

"**Il rischio può essere definito come la combinazione della probabilità di accadimento di un evento e delle sue conseguenze**"

ISO/IEC Guide 73 Risk Management, 2002

La Norma ISO/IEC 13335, considera, correttamente, oltre alle dimensioni **probabilità** e **danno**, **anche la vulnerabilità** a fronte delle possibili minacce

IRM - Processo di Risk Management



IRM: Institute Risk Management, UK

I punti chiave del Risk assessment

CONSAPEVOLEZZA

Metodo compreso e scelto dai responsabili aziendali.

Identificazione delle relazioni fra risorse, minacce e rischi

GESTIONE NEL TEMPO

Analisi aggiornabili agevolmente nel tempo in caso di modifiche

Analisi condotte in momenti diversi sullo stesso ambito, devono dare comparabili

RIPETIBILITÀ DEI RISULTATI

Valutazioni il più possibile oggettive (scale di valori specifiche o analisi quantitative)

Utilizzo di questionari con linee guida esplicative

SISTEMATICITÀ

Si deve garantire che vengano analizzate tutte le risorse, le minacce e le vulnerabilità relative all'ambito di analisi

Non sono accettabili analisi che considerano solo alcune minacce

da Seminario DNV Auditor ISO 27001, aprile 2006

Fasi Progettuali del Risk management

A) Mappatura dei rischi aziendali

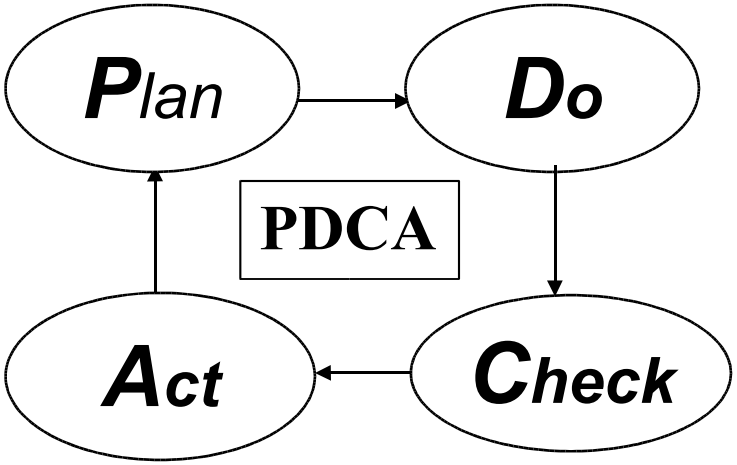
B) Valutazione dei rischi aziendali

C) Definizione del modello organizzativo
(Individuazione misure trattamento del rischio)

D) Attuazione misure di trattamento
(Attuazione delle misure di trattamento)

E) Monitoraggio

F) Miglioramento delle prestazioni



Metodologia ERMS Sernet spa

Fase B.3.1) Misurazione/Stima dei Rischi

- **Cause di minaccia reali (stima delle PROBABILITÀ)**
- **Effettive VULNERABILITÀ esistenti (considerando le protezioni in atto)**
- **DANNI potenziali diretti e indiretti**

RISCHIO = Danni x Probabilità x Vulnerabilità

Fase B.3.2) Tecniche di Misurazione/Stima

Qualitative	**scale tipo: Alto/Medio/Basso**
Semi-Qualitative	**scale di Punteggi (es.: da 1 a 10)**
Quantitative	**Valori Economici**

La scelta della Tecnica dipende dai costi/benefici delle alternative, e dalla incertezza/attendibilità delle informazioni da utilizzare

In certi casi, è consigliato fare una prima valutazione con una tecnica meno impegnativa (QUAL/SEMI-QUAL) e poi, sui rischi più importanti, migliorare la stima con una tecnica QUANTITATIVA

L'utilizzo della Tecnica Semi-Qualitativa (Risk Scoring) al posto di quella Qualitativa (Risk Rating) è preferibile quando, oltre a calcolare il Rischio su specifici obiettivi/attività, si vuole poi ottenere un Rischio "complessivo" (possibile aggregando i Punteggi)

Fase B.3.2a) Tecnica Qualitativa/Semi-Qualit.

	Probab. evento	Low			Medium			High		
	Vulner.	L	M	H	L	M	H	L	M	H
Impatto	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	↑	↑	↑	↑	↑	↑	↑	↑	↑
	4									
	5	4	5	6	5	6	7	6	7	8

RISCHIO

(Fonte ISO 13335)

Fase B.3.2b) Tecnica Quantitativa

Variabile aleatoria = **UTILE**

RISCHIO

Utile U

Prob.(/Vuln.) P

Utile atteso Ua = Σ (U*P)
= **50.000 €**

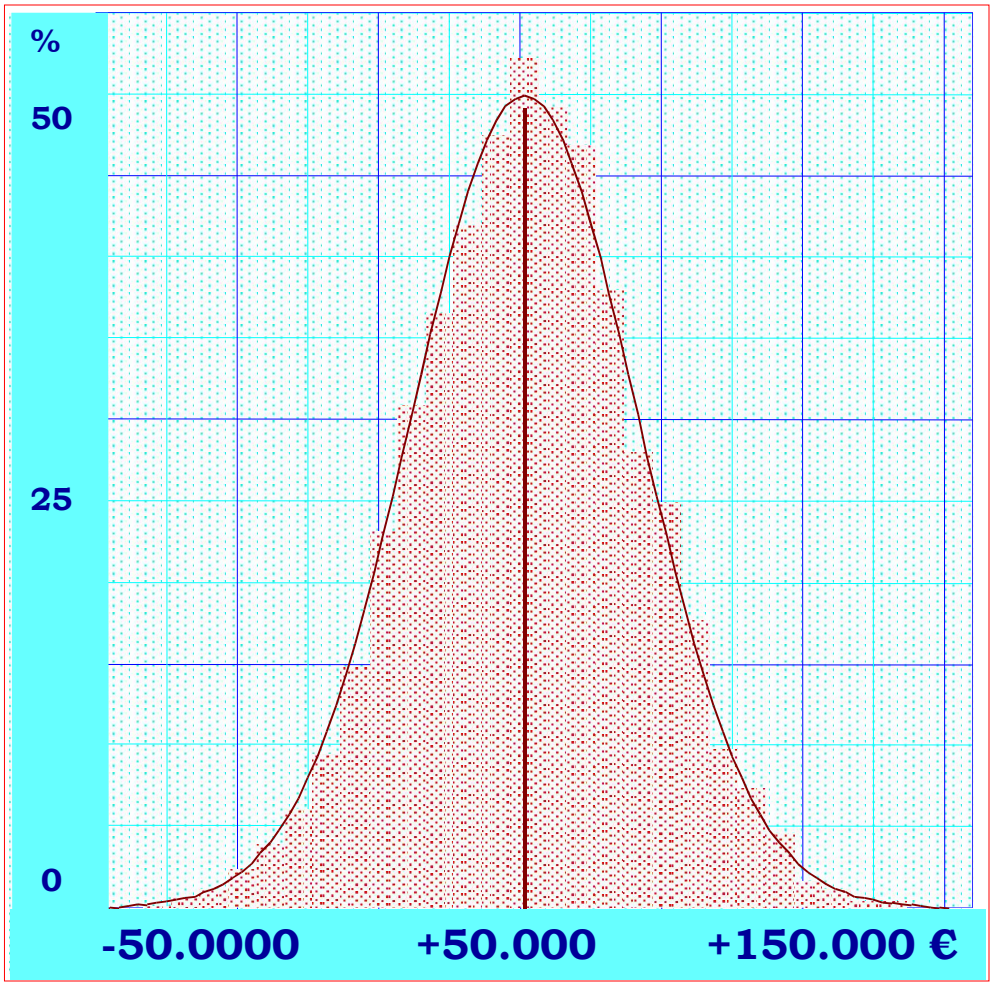
Scarto S = U - Ua

Scarto Q.m. б = $\sqrt{\Sigma (s^2*P)}$

Perdita MAX potenziale

PMP 99,9% = Ua - 3,09*б
= **- 23.000 €**

PMP 99,0% = Ua - 2,33*б
= - **5.000 €**



sernet

a company of ABM NETWORK

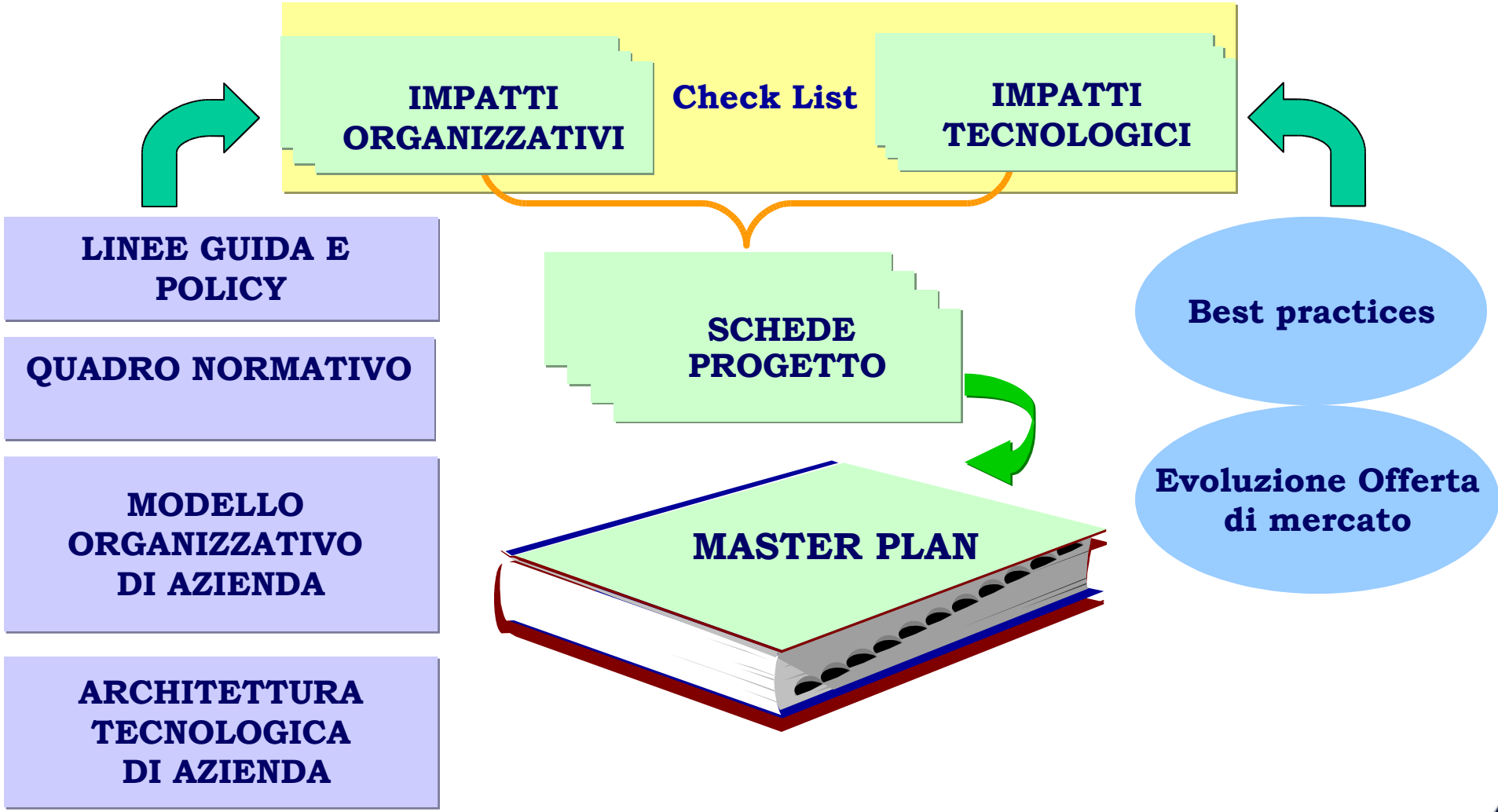
Fase D.3) Individuazione dei Trattamenti

- **trasferibilità del rischio (es. assicurazioni, outsourcing)**
- **azioni tecnico-organizzative per riportare il rischio a livello di accettabilità (progetti)**
- **accettazione o eliminazione del rischio**

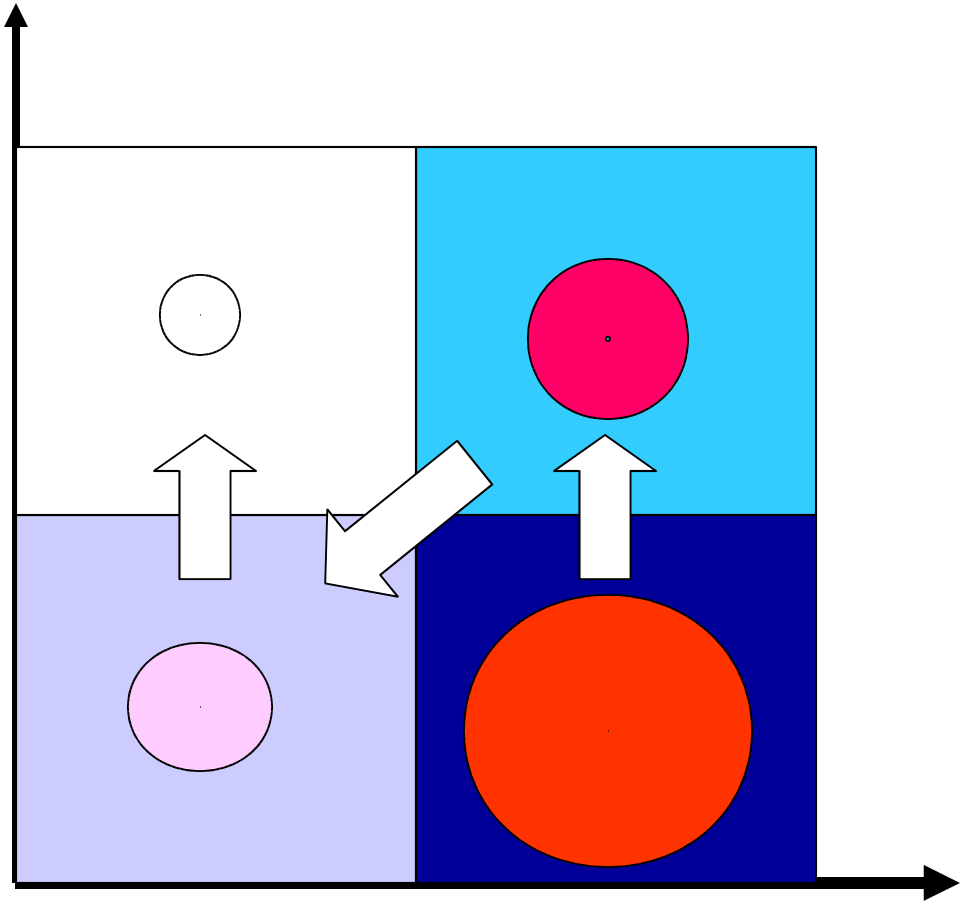
Il Master Plan dei Rischi

Documento, e relativa Sintesi Direzionale, in cui sono raccolti i risultati dell'analisi svolta, gli obiettivi ed il piano di intervento complessivo, con l'indicazione dei progetti, delle priorità, delle responsabilità, dei costi e dei tempi di attuazione

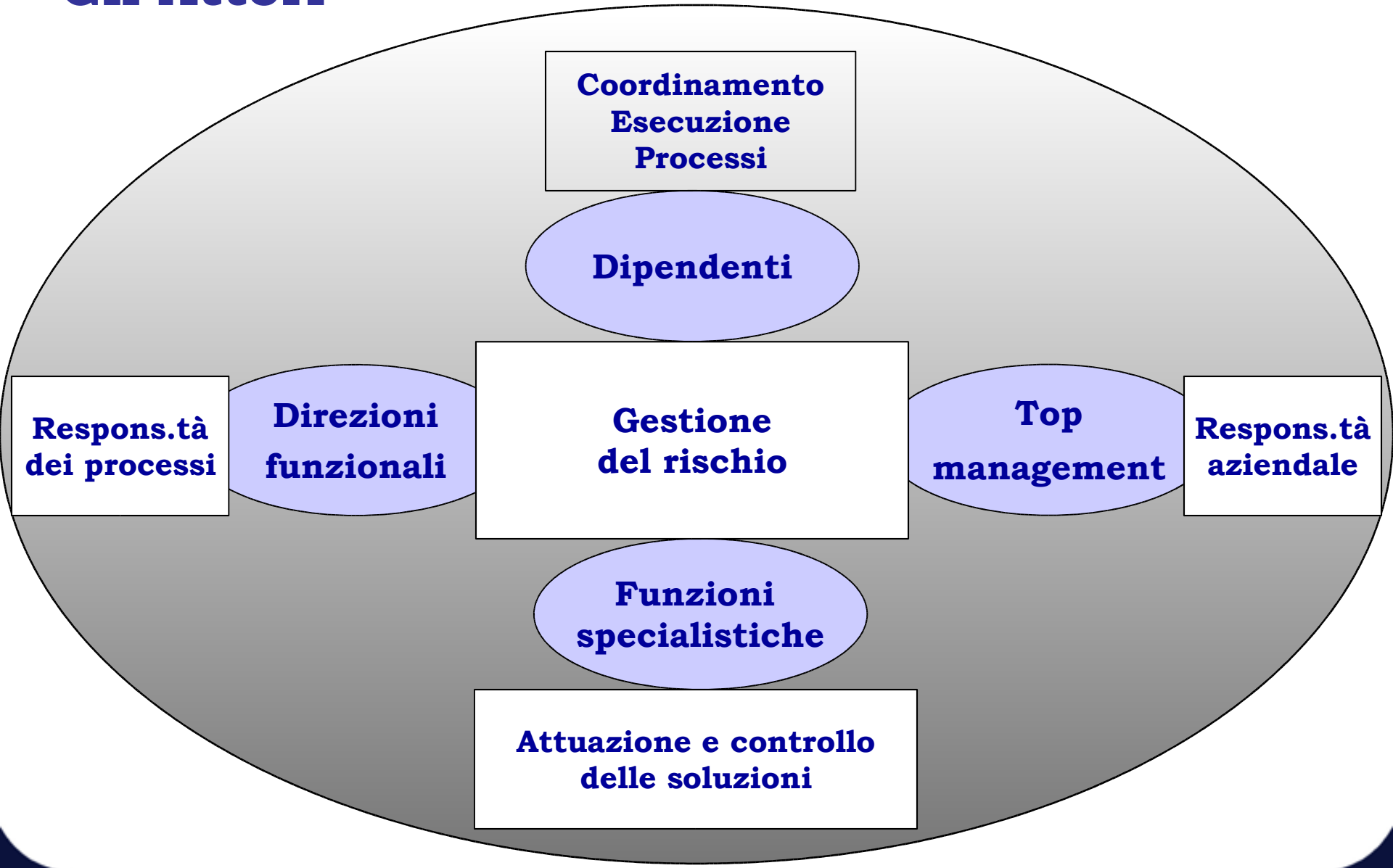
La Struttura del Master Plan



Le Priorità


Costo misure protettive
Alto
Basso
Basso
Alto
Livello di Rischio

Gli Attori



Il Team

- Esperienze in settori/progetti dell'area di indagine
- Conoscenza dei processi e dell'organizzazione aziendale
- Disponibilità di tempo e di adeguate informazioni

- Visibilità direzionale
- Coinvolgimento di Process Owner e "clienti interni" dei servizi
- Trasparenza dei criteri di valutazione e documentazione dei risultati

- Formazione
- Coaching
- Benchmarking

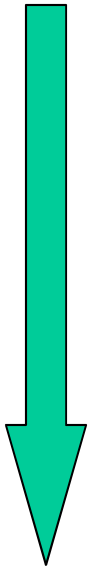
Società KAPPA

Progetto di ICT Risk Management 2006

(Fase di ICT Risk Assessment)

La Realtà Aziendale

- Azienda di servizi
- Oltre 3000 dipendenti, 4 Sedi principali
- Funzione Sistemi Informativi con una ventina di dipendenti
- Soluzioni ERP e software verticale specializzato



- Realizzato il Check-up delle soluzioni di ICT Security verso la Norma BS 7799 (ISO 27001)
- Realizzata una Soluzione di Disaster Recovery
- Nuova Policy di sicurezza ICT basata su ISO 27001
- Comitato direzionale sicurezza informazioni
- Responsabile aziendale di sicurezza ICT

- Aggiornamento Istruttoria periodica di ICT Risk Management

Il Progetto di ICT Risk Management

- In coerenza con la Nuova Policy di sicurezza ICT, svolgere una **istruttoria periodica di valutazione e gestione dei rischi ICT**
- Il risultato dell'istruttoria di valutazione (**Risk Assessment**) è presentato al Comitato direzionale sicurezza informazioni per approvazione
- Approvato il risultato della valutazione, si individuano e pianificano i progetti di intervento
- Si inizia, poi, la fase di realizzazione dei Progetti approvati dal Comitato Sicurezza Informazioni (**ICT Risk Management**)

Le Attività

Start up del Progetto

Definizione del perimetro e criteri di accettabilità dei rischi

Identificazione del Perimetro (4 aree di indagine: Centro di calcolo e Rete, 3 applicazioni aziendali critiche)

Costituzione del team di valutazione (ICT, Key User, Consulenza)

Formazione e sensibilizzazione del Team

Svolgimento della fase di valutazione

Omogeneizzazione dei risultati

Classificazione dei rischi e sintesi direzionale

Identificazione e valutazione dei progetti di intervento

Audit

Approvazione e realizzazione Progetti di intervento

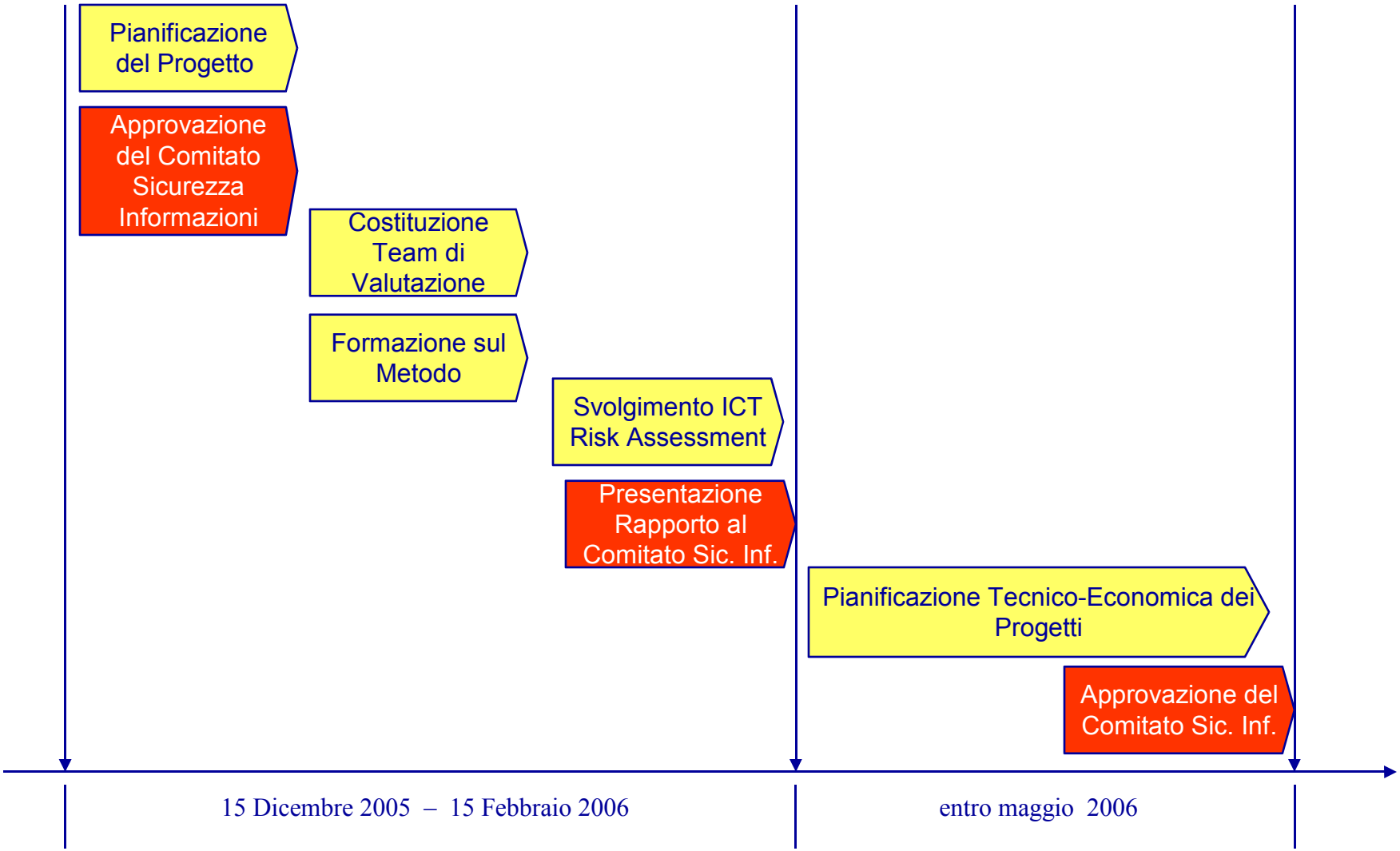
Comitato Sicurezza Informazioni

- presieduto da un membro del Comitato di direzione
- composto da Responsabili Internal Audit, Sicurezza ICT, Security, Sistemi Informativi
- promuove l'indagine
- definisce il perimetro e i limiti di accettabilità dei rischi
- approva la costituzione del team di valutazione
- valuta i risultati della fase di risk assessment
- approva i progetti di miglioramento
- propone eventuali aggiornamenti del budget
- valuta i risultati dei progetti di miglioramento

Team di valutazione

- Coordinamento a cura del Responsabile di Sicurezza ICT
- Riunioni dedicate alle 4 Aree di indagine
- Partecipazione di 2-3 key users per Area
- Partecipazione di 4 Responsabili (esercizio-tecnologia e 3 aree applicative) e 6 capi-progetto / sistemisti ICT
- Partecipazione del Team di Consulenza Sernet

Il Gantt di Progetto (Risk assessment e Pianificazione Progetti di intervento)

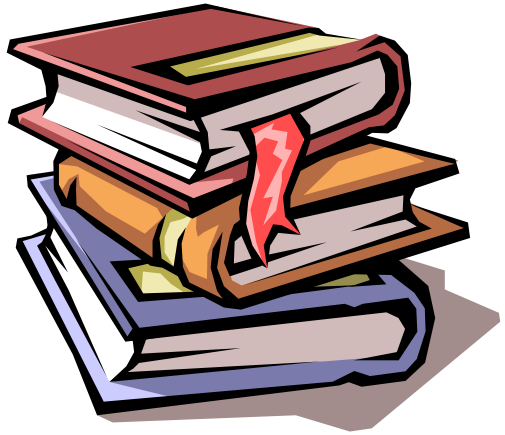


I Risultati intermedi

Redazione del documento “Progetto ICT Risk Management – Fase di Valutazione dei Rischi (ICT Risk Assessment)”

Per i perimetri:

- CED e rete
- Sistema SAP,
- Sistema Personale,
- Sistema Gestionale



Misura dei Rischi ICT

Individuazione dei Rischi Prioritari e dei Progetti di miglioramento

Prassi operativa per la valutazione dei rischi ICT

Calcolo del Rischio

Il **RISCHIO** è stato calcolato considerando il valore del potenziale **DANNO** (diretto o indiretto) a fronte delle minacce, moltiplicato per la **PROBABILITÀ** di accadimento e tenuto conto delle misure di protezione in atto (grado di **VULNERABILITÀ**).

RISCHIO = Danno X Probabilità X Vulnerabilità

Per la misurazione/stima del **RISCHIO** è stata utilizzata una tecnica semi-qualitativa, con una scala di punteggi da 0 a 1000 (ottenuta dal prodotto delle tre valutazioni dei tre fattori **D**, **P**, **V**).

Le minacce considerate sono derivate dall'elenco dei Controlli presenti nello Standard Gestionale sulla Sicurezza ICT BS 7799-2 (ISO 27001)

Valutazione degli Impatti (DANNO)

La misurazione dell'**IMPATTO** viene effettuata per ogni minaccia attraverso una tecnica semi-qualitativa che considera una scala numerica tra 0 e 10.

Il valore dell'**IMPATTO** viene assegnato nell'ipotesi di accadimento della minaccia, senza considerare la Probabilità e la Vulnerabilità.

Per ottenere maggiore omogeneità nelle valutazioni, il Team adotta uno schema condiviso ("Tabella Impatti") in cui, per ciascuna tipologia di Impatto, vengono espressi dei valori convenzionali per i diversi livelli di gravità.

TABELLA IMPATTI (esempio)

Tipologia/Valore	Valore Alto Punteggio: 8	Valore medio Punteggio: 5	Valore basso Punteggio: 3
Danni economici ed operativi	Alterazione dati gestionali con impatto sul Bilancio	Alterazione dati operativi non rilevanti	Alterazione dati gestionali non critici
Violazioni di norme e/o leggi	Violazione con sanzioni penali o con sanzioni amministrative superiori ad euro.....	Violazione con sanzioni amministrative inferiori ad euro....	Comportamenti non conformi a Norme interne senza particolari conseguenze
Danni di immagine	Perdita della fiducia dei clienti e/o dei patner	Deterioramento significativo del livello di servizio siti web	Errore occasionale di una comunicazione a fornitori

Valutazione della Probabilità

La misurazione della **PROBABILITÀ** viene effettuata per ogni minaccia attraverso una tecnica semi-qualitativa che considera una scala numerica tra 0 e 10.

Il valore della **PROBABILITÀ** viene assegnata nell'ipotesi di accadimento della minaccia, senza considerare la Vulnerabilità.

Per ottenere maggiore omogeneità nelle valutazioni, il Team adotta uno schema condiviso ("Tabella Probabilità") in cui, per ciascuna variabile di Probabilità, vengono espressi dei valori convenzionali per i diversi livelli di gravità.

TABELLA PROBABILITÀ (esempio)

Variabili/Valore	Valore Alto Punteggio: 8	Valore medio Punteggio: 5	Valore basso Punteggio: 3
Numerosità utenti potenziali portatori di minacce	Tutti gli utenti interni e consulenti ICT esterni	Gruppi di utenti interni e consulenti ICT esterni	Alcuni utenti interni
Frequenza stimata nell'anno	Una volta ogni mese	Una volta ogni anno	Inferiore ad una volta l'anno

Valutazione della Vulnerabilità

La **VULNERABILITÀ** è un valore che esprime il livello di protezione dalle minacce.

Per ogni controllo e per ogni fattore che influenza la protezione dalle minacce, si assegna un punteggio secondo i criteri riportati nella Tabella Vulnerabilità (dal valore 0=protezione totale, al valore 10=nessuna protezione).

TABELLA VULNERABILITÀ (esempio)

Variabili/Valore	Valore Alto Punteggio: 8	Valore medio Punteggio: 5	Valore basso Punteggio: 3
Necessità competenze tecniche	Limitata	Skill ICT	Sofisticati sistemi di attacco
Livello di conoscenze dell'ambiente tecnologico	Limitato	Architettura tecnologica e applicativa	Soluzioni tecnologiche di dettaglio
Livello di complessità dell'attacco	Basso	Tecnica di attacco semplice	Tecnica di attacco complessa
Presenza strumenti di controllo	Carenza di strumenti tecnico-organizzativi	Strumenti tecnico-organizzativi parziali	Strumenti tecnico-organizzativi efficaci

Matrice per il calcolo del Rischio

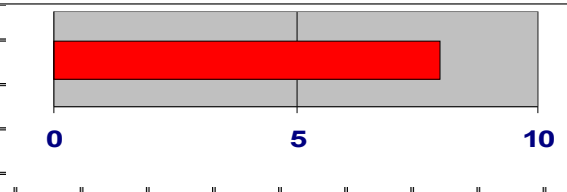
Una volta che siano stati valutati IMPATTI, PROBABILITÀ, VULNERABILITÀ, viene effettuato il calcolo del **RISCHIO** per ciascuna *minaccia* (le minacce sono derivate dall'elenco dei Controlli presenti nello Standard Gestionale sulla Sicurezza ICT BS 7799-2 (ISO 27001).

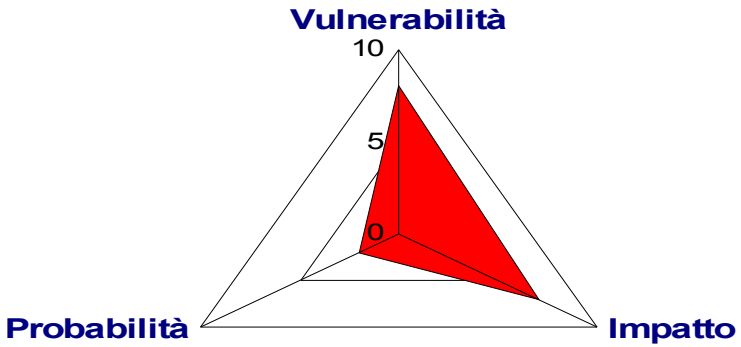
Descrizione Controllo BS7799-2	Rif. Norma	Impatto (valore tra 0-10)	Probabilità (valore tra 0-10)	Vulnerabilità (valore tra 0-10)	RISCHIO (valore tra 0-1000)
Documento di politica aziendale di base sulla sicurezza	A.3				
Definizione struttura organizzativa	A.4.1				
Copertura dei rischi verso i consulenti	A.4.2				

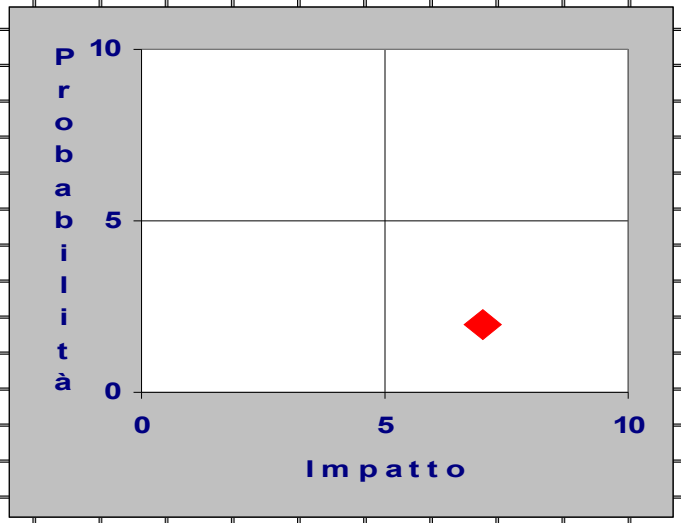
Le Valutazioni della minaccia (esempio)

Rischio = impatto x probabilità x vulnerabilità = 8 x 7 x 2 = 112

Vulnerabilità	8
Impatto	7
Probabilità	2







La classificazione dei risultati (esempio)

Punteggi fittizi assegnati solo a scopo didattico

Rif **BS7799**	**Minacce**	**Punteggio rischio**
P23	Distribuzione non autorizzata di informazioni riservate, per assenza di Policies sul grado di riservatezza	510
P37	Nuove applicazioni con carenti misure di sicurezza, per mancanza di Studi di fattibilità preventivi	440
P8	Errori operativi per carenze di addestramento del Personale	370
P11	Black out elettrico	260
P14	Ritardi nelle Elaborazioni batch critiche	220
P42	Errori applicativi per carenza Procedure di Change management	180
P44	Blocco dei servizi ICT per disastri ambientali o prolungate anomalie tecniche	170

Soglia convenzionale di accettazione del RISCHIO

Soglia = 250

Progetti di miglioramento suggeriti

- Sviluppo Policy specifica su riservatezza Informazioni
- Pubblicazione Linea Guida Change management (con Requisiti di Sicurezza)
- Attivazione ciclo di addestramento supplementare Sistema Gestionale
- Accelerazione installazione Gruppo elettrogeno di continuità
- Potenziamento Server applicazioni critiche
- Modifica SLA Sistema Disaster recovery (attivazione entro 12 ore)

Grazie per l'attenzione