Il Sistema di Risk Management applicato ai Censimenti generali

Concetta Ferruzzi
Direzione generale

Daniele Frongia
Direzione centrale
metodologie e tecnologia

Istat

Indice

I livelli del sistema di controllo interno

Il sistema di controllo interno è un processo finalizzato al governo ed al controllo dell'organizzazione con l'obiettivo di coordinare i comportamenti e farli convergere verso gli obiettivi strategici.

I livello

Strumenti a supporto dello sviluppo ed il monitoraggio degli obiettivi in termini di efficacia ed efficienza:

- *STANDARD ORGANIZZATIVI*
  standard dei processi, delle procedure, delle carte dei servizi
- *SISTEMI OPERATIVI*
  pianificazione strategica, budget, sistema di programmazione annuale, sistema di valutazione delle performance, meccanismi di timely feedback and feed-forward, standardizzazione dei processi, soddisfazione degli utenti

II livello

Strumenti in grado di individuare, valutare e gestire i rischi

Risk Management

supportano la ***creazione di valore*** *mettendo la dirigenza, ai diversi livelli decisionali, in grado di affrontare gli eventi futuri che potenzialmente possono generare rischi consentendo di ridurre la probabilità di effetti negativi e migliorare le opportunità*

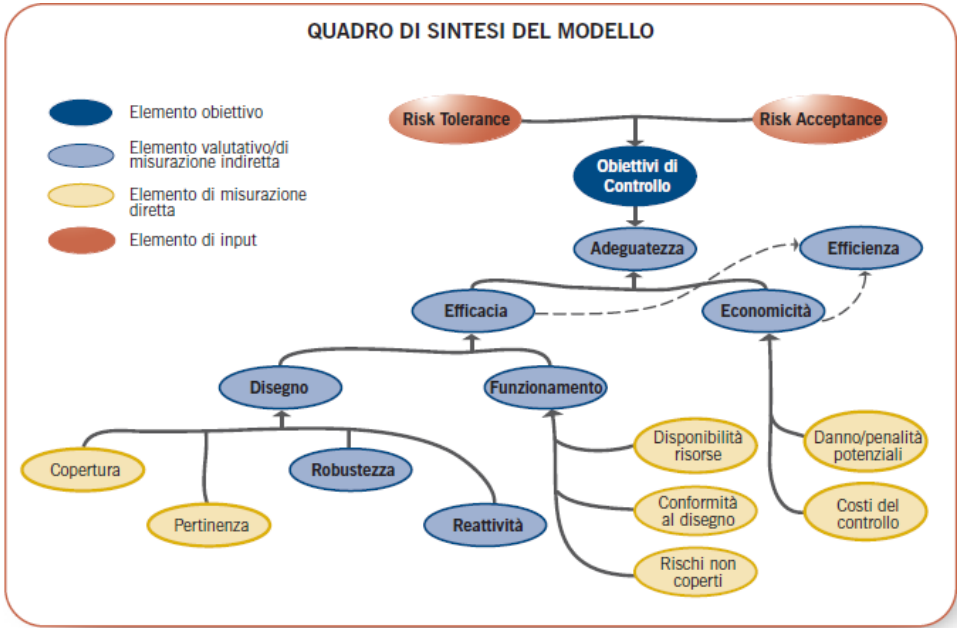
III livello

Strumenti per la valutazione dei processi, degli output e degli

- *TOTAL QUALITY MANAGEMENT (TQM)*
  sistemi in grado di garantire che il management e le statistiche prodotte siano di elevata qualità e rispondenti agli standard nazionali ed internazionali
- *INTERNAL AUDITING*
  processi in grado di fornire la ragionevole assicurazione del raggiungimento degli obiettivi, la corrispondenza alle regole ed alle procedure, la salvaguardia del patrimonio, la prevenzione delle frodi, la qualità delle informazioni per i processi di governance

Il sistema di controllo del rischio

Il Sistema di Controllo del Rischio può essere definito come "*l'insieme delle* ***regole****, delle* ***procedure*** *e delle* ***strutture organizzative*** *volte a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, una* ***conduzione dell'azienda (pubblica o provata) sana****, corretta e coerente con gli* ***obiettivi prefissati" .***



Fonte: Codice di Autodisciplina – Borsa Italiana S.p.A. Comitato per la Corporate Governance

ASSOCIAZIONE ITALIANA INTERNAL AUDITORS, Disegno e funzionamento del sistema di controllo interno, AIIA, 2008

Gli Obiettivi strategici del Risk Management in ISTAT

Il **Sistema di Risk Management** insiste sugli **obiettivi strategici** fissati dagli **Organi di Governo** dell'Istituto:

- del sostegno alla produzione statistica attraverso processi amministrativi e gestionali di qualità
- della "messa in sicurezza" di tutti i Sistemi dell'Istituto
- dello sviluppo del capitale umano e il miglioramento delle condizioni di lavoro del personale

La Direzione generale partecipa alla *"messa in sicurezza"* dell'Istituto con la definizione del Sistema di gestione dei Rischi, *progettato, sperimentato* e *applicato* dalla *Commissione tecnica* per l'introduzione in Istat di un Sistema di Risk Management

Il Progetto Risk Management ISTAT

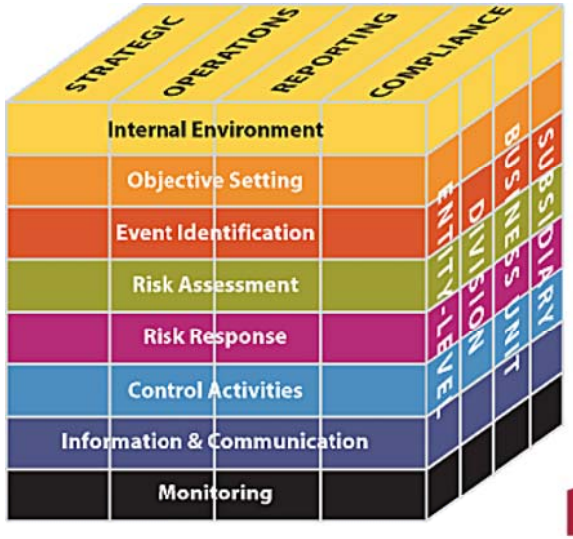
Il Progetto muove lungo 3 dimensioni:

- l'organizzazione, con la proposta di articolazione delle competenze e delle interconnessioni tra i Sistemi gestionali
- il Processo di ERM, con lo sviluppo delle fasi di analisi e trattamento dei rischi organizzativi
- la formazione e la diffusione, con la crescita della cultura organizzativa della gestione del rischio: risk.istat.it
- Il framework metodologico di riferimento

Il COSO Report prevede per ciascuno step del processo :

1. adeguata identificazione:
- rischio potenziale,
- impatto,
- probabilità di verificarsi,
- azioni di risposta

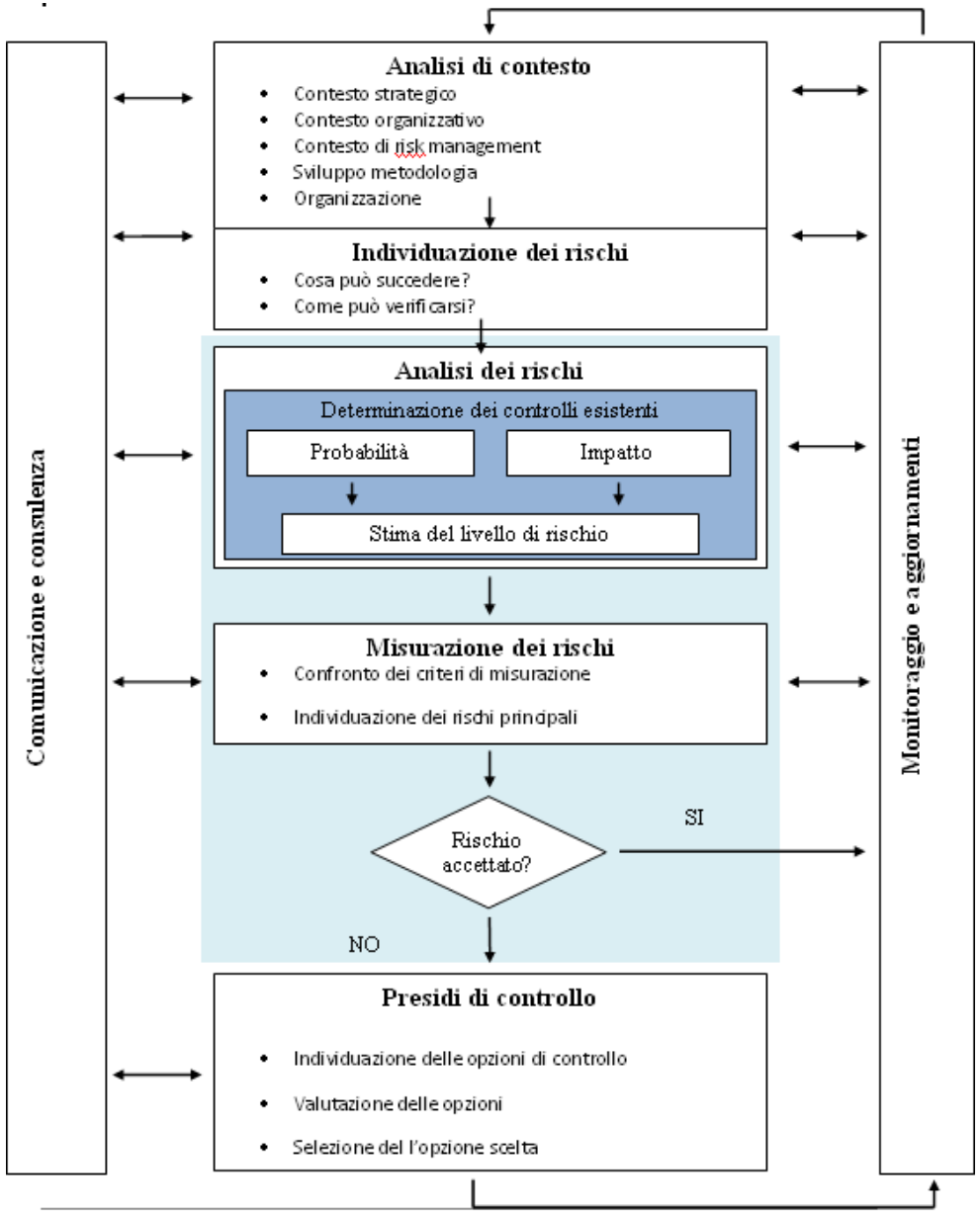
2. chiara assegnazione delle responsabilità coinvolte



2011 FORUM PA

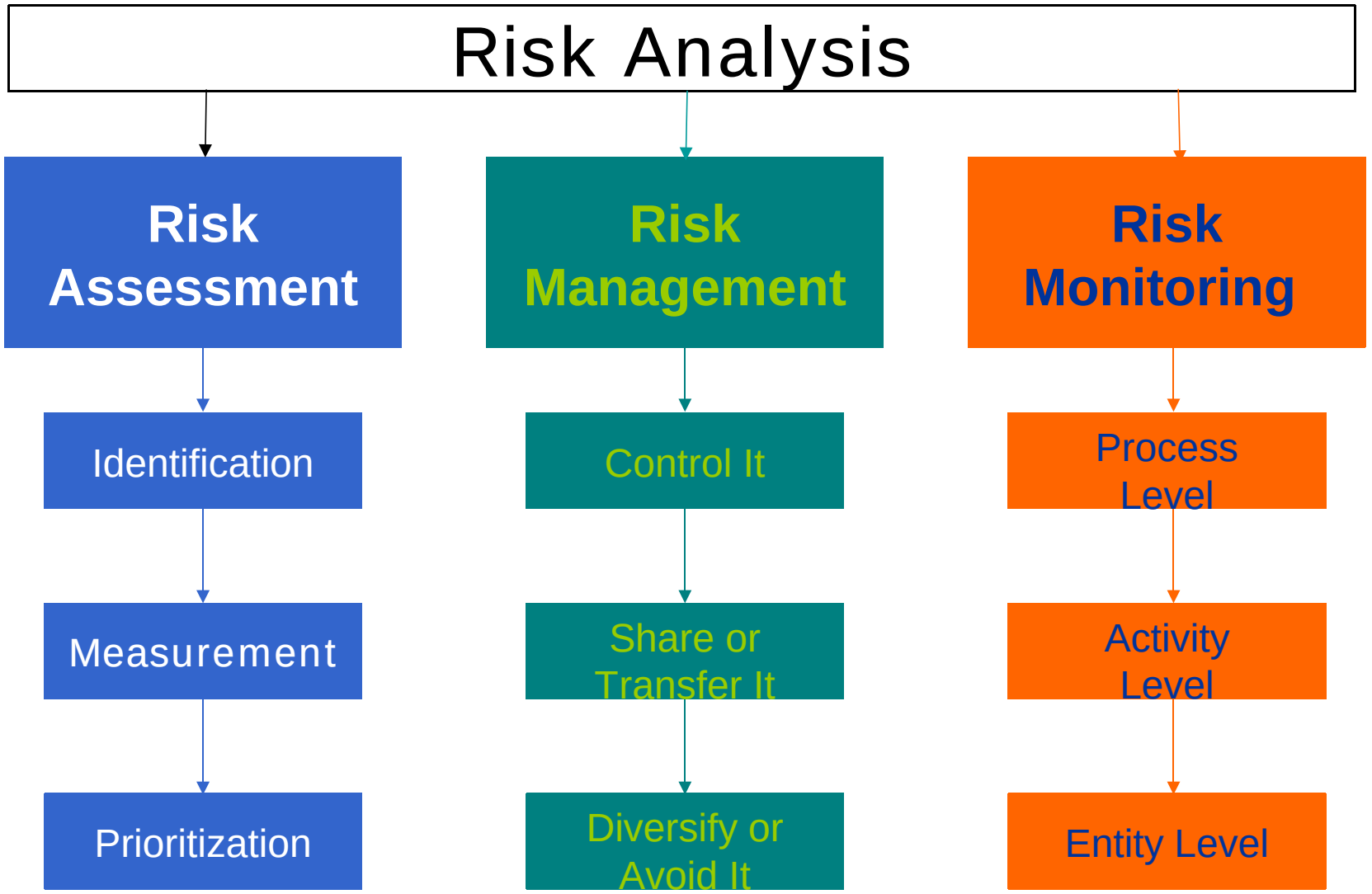
Istat

Il Processo del Risk Management



Fonte: Australia/New Zealand Standard 4360:2004

Le fasi del sistema di gestione del rischio



Le classi di rischio individuate

Le **classi di rischio** identificano le macrocategorie di rischi che deve affrontare l'Istituto.

Una prima ipotesi di classificazione dei rischi:

A. rischi legati alla produzione statistica
B. rischi legati alla diffusione dei dati statistici
C. rischi connessi alla *compliance a leggi, regolamenti e framework internazionali*
D. rischi legati alle persone
E. rischi connessi all'organizzazione
F. **rischi tecnologici**
G. rischi finanziari ed economici
H. rischi materiali e tecnici
I. rischi di immagine e reputazione
J. rischi esogeni

I rischi specifici

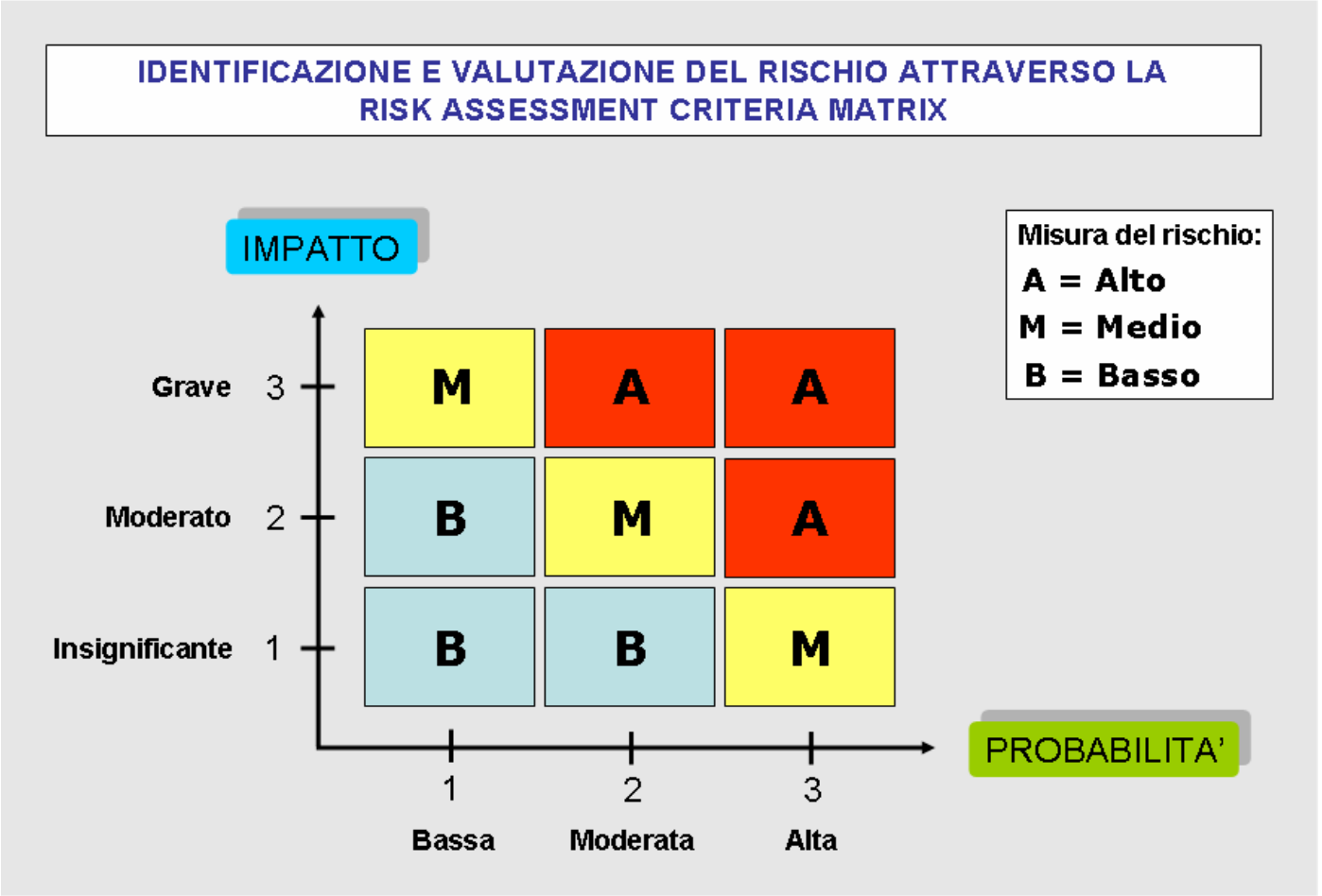
Ogni classe di rischio deve essere suddivisa per identificare i **rischi specifici** che la compongono in modo da realizzare una descrizione più puntuale delle criticità riscontrate all'interno della macrocategoria relative ai processi e agli asset.

Questa suddivisione in **rischi specifici** è necessaria per identificare le cause dei rischi, la loro natura e gli effetti che possono comportare per l'Istituto.

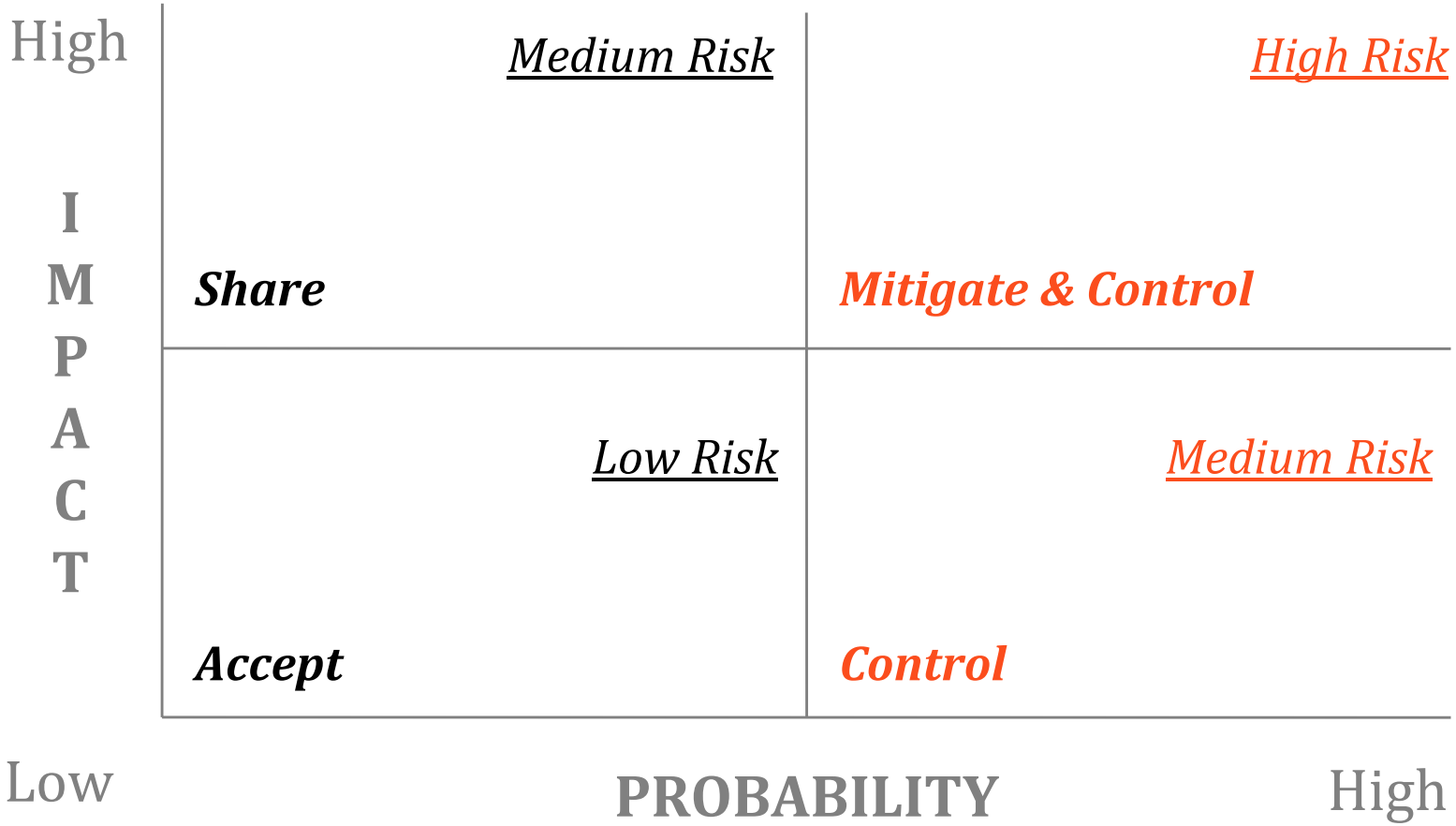
L'attuale classificazione dei **rischi specifici** è molto parziale perché è stata determinata in base alle informazioni finora acquisite dalla Commissione

Per la definizione delle categorie di **rischi specifici** all'interno della **classe di rischio** relativa alla **produzione e diffusione statistica,** sarà necessaria la collaborazione con la Commissione di audit sulla qualità dei processi statistici,

L’identificazione del rischio



La gestione del Rischio



Fonte: AIIA - Applying COSO's Enterprise Risk Management — Integrated Framework

La catalogazione dei Rischi

Il Framework del Catalogo dei rischi rappresenta: attività, criticità ed effetti

Sezione 1 - Analitica attività		Sezione 2 - Rischio				Sezione 3 - Effetti e risposte	
Macroattività	**Struttura responsabile**	**Classe di rischio**	**Rischio specifico**	**Criticità interne**	**Criticità esterne**	**Effetto/ conseguenza**	**Proposta intervento**
Rilevazione Numeri Civici (RNC)	SCD/ B	E. organizzazione	E.1.organizzazione attività	Uffici regionali molto impegnati in altri progetti e manca la nomina dei referenti RNC	• Modelli di rilevazione fatti con le basi territoriali della DCET (solo 344 già disponibili, 54 disponibili a breve, 106 entro novembre)	Gli Uffici regionali non hanno le risorse formate per coordinare la RNC a livello sub regionale	Iniziare con i Comuni i cui dati sono disponibili e rinviare l'inizio per gli altri (mancata RNC non pregiudica il censimento)
Piano Generale di Censimento (PGC)	DCCG	J. esogeni	J.1 Relazioni istituzionali	Mancata comunicazione e diffusione del soggetto responsabile a redarre il PGC Criticità relative ai tempi di approvazione interna e alle eventuali modifiche PGC • Manca la nomina dei referenti regionali RIT per carenza risorse negli Uffici Regionali	• Per approvare il PGC e quindi attribuire le competenze a livello decentrato è necessaria la Conferenza Unificata con tempistiche convocazione lunghe e incerte • Occore l'approvazione del Comune dell'Aquila; Comuni alluvionati di Messina; Ufficio regionale a Roma (non c'è più) • Ricorsi • Richiesta	I Comuni non possono inserire in bilancio preventivo le spese necessarie per fare il censimento Rischio ritardi nella costituzione della rete censuaria con conseguente ritardo: • nel reclutamento del personale ad hoc • nella formazione del personale della rete • nella richiesta delle LAC Ritardo nell'inserimento del	• Separazione dell'approvazione dei contributi ai Comuni e dell'approvazione della rete organizzativa (entro 9/ 2010) • Attingere da liste aperte per velocizzare le procedure di reclutamento:
Costituzione Uffici di Censimento (UCC)	SCD/ D	E. organizzazione	E.1.organizzazione attività	• Manca la nomina dei referenti regionali RIT per carenza risorse negli Uffici Regionali	Comune dell'Aquila; Comuni alluvionati di Messina; Ufficio regionale a Roma (non c'è più)	Rischio ritardi nella costituzione della rete censuaria con conseguente ritardo: • nel reclutamento del personale ad hoc • nella formazione del personale della rete • nella richiesta delle LAC Ritardo nell'inserimento del	
Definizione				• Selezione • Concorso	• Richiesta		

FORUM PA 2011

Istat

Le azioni di risposta e il monitoraggio

Il report del rischio

REPORT DI RISCHIO			
PROCESSO			
RISCHIO	COD RISCHIO	CATEGORIA	DESCRIZIONE RISCHIO
VALUTAZIONE	PROBABILITA'	IMPATTO	GIUDIZIO FINALE

Il monitoraggio delle azioni di risposta

Struttura Responsabile	Azioni di risposta	Effetti attesi della risposta al rischio	Indicatore di risposta al rischio	Risultati delle Azioni correttive	Periodicità rilevazione e aggiornamento

Il Rischio di disastro IT

Il Rischio di disastro IT

La complessità dei sistemi informatici e dell'interazione tra i vari componenti software impone alle aziende e alle pubbliche amministrazioni una **maggiore attenzione** sull'importanza della prevenzione e della gestione dei disastri informatici.

Il **15° Censimento della popolazione e delle abitazioni** si avvale di tre sistemi informatici:

1) La gestione della **rete** dei rilevatori

2) La gestione della **rilevazione** (7 aree funzionali per circa 50 funzionalità)

3) **L'acquisizione online dei dati**

(Ovviamente) Prevenire è meglio che…

Un efficace sistema di gestione per la prevenzione di un disastro IT richiede la mappatura:

a) di tutte le funzionalità previste dai tre sistemi IT del Censimento;
b) delle infrastrutture tecnologiche del sistema: architetture server, versione degli applicativi in uso etc.;
c) degli eventuali protocolli di sicurezza, protocolli di business continuity, disaster recovery, backup e restore dei dati e degli applicativi;

(Ovviamente) Prevenire è meglio che…

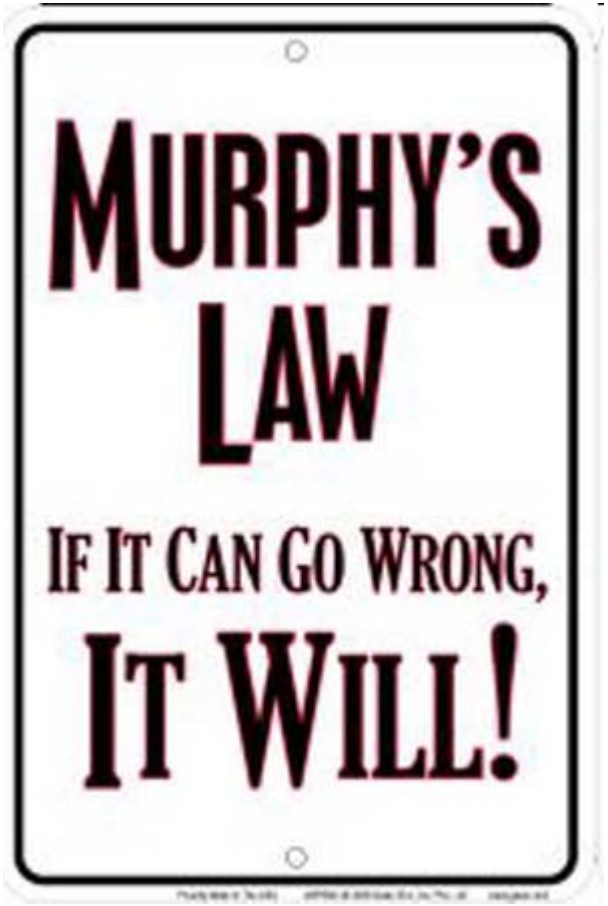
Un efficace sistema di gestione per la prevenzione di un disastro IT richiede inoltre la mappatura:

d) dei contratti con i fornitori di servizi (Telecom Italia) e un'analisi puntuale di tutta la documentazione ufficiale.

Occorre inoltre prevedere un efficiente **piano di test** e una prova (**simulazione**) di crisi.

Legge di Murphy

La definizione di un sistema di prevenzione dei rischi non evita però che situazioni critiche possano verificarsi.



Legge di Murphy

Cosa fare per gestire e superare la crisi

Prime valutazioni (rescue remedy)

Caos, ovverosia il brainstorming iniziale

Questo caos non è fine a se stesso, è un'importante fase di **brainstorming** necessaria a definire un **piano della crisi**.

Unità di crisi

La task force per la gestione della crisi

Quando costituirla?

Unità di crisi

- Un (uno solo) **responsabile**: questa figura diventa il commander-in-chief della crisi;
- **Staff IT**: Progettisti e sviluppatori, esperti database, sistemisti, esperti di sicurezza e team leader;
- Il **dirigente di collegamento** con Telecom Italia;
- Il **responsabile del Risk Management** o un suo incaricato;
- Un'ombudsman (*un uomo che funge da tramite*) per i rischi IT: una figura dirigenziale rispettata e autorevole per il personale IT, al quale rivolgersi per esprimere le proprie idee e preoccupazioni sulle attività dell'unità di crisi.

Unità di crisi

E ancora:

- Una persona dell'area **Comunicazione**;
- Una persona dell'area **Organizzazione**, esperta di analisi dei processi, descrizione delle procedure e verifiche di auditing;

- Eventuali **consulenti esterni**.

E' inoltre necessario allertare l'area **Amministrativa** affinché possa procedere ad eventuali acquisti da effettuare in condizioni di emergenza.

Comunicazione in tempo di crisi

Interna al gruppo dell'unità di crisi: devono sempre essere chiari ruoli, attività, esiti delle operazioni e scadenze;

Interna all'azienda: anche i dipendenti che non partecipano all'unità di crisi devono essere correttamente informati;

Esterna: va definito un accurato piano di comunicazione con gli utenti, i media e va posta particolare attenzione alla cura dei profili dell'istituto sui social media (caso Aruba).

La crisi

Diario della crisi

Gestione del team

Riunioni periodiche

La fine della crisi

Diagnosi e risoluzione del problema;

Test: prima di tornare online, l'istituto deve eseguire accurati test sia internamente che esternamente;

Monitoraggio della messa in produzione;

Reportistica accurata di quanto accaduto;

Comunicazione delle soluzioni adottate e condivisione della conoscenza acquisita nella gestione delle problematiche emerse sia internamente che esternamente.

Biblio&Sitografia

ISO/FDIS 31000:2009; ISO/FDIS 31010:2009. Risk management - Principles and guidelines – Risk Assessment

FERMA 2004. Standard of Risk management

ISO/IEC 27005:2008; 27001:2009. Information technology - Information security Risk management - Code of practice

ISO/IEC 16085:2006. System and software engineering - Life cycle processes - Risk management

ACT AS/NZS 4360:2004. Risk management

PD ISO/IEC Guide 73:2002 - Guidelines for use in standards, 2002

BS 31100:2008. Risk Management – Code of Practice

OECD. Corporate Governance Principles. 2004

EUROPEAN COMMISSION. Risk Management - Guide. 04 2008

DELIBERE C.i.V.I.T nn. 88, 89, 104, 105 e 112

ASSOCIAZIONE ITALIANA INTERNAL AUDITORS, Disegno e funzionamento del sistema di controllo interno, AIIA, 2008

ASSOCIAZIONE ITALIANA INTERNAL AUDITORS/PRICEWATERHOUSECOOPERS. La gestione del rischio aziendale. Sole24 ORE, 2006

ATTAL J., **Sopravvivere alla crisi**, Fazi Editore

BRODNITZ G., CURTIS G.A., EMMEL R., **Disaster recovery. Non chiedetevi se accadrà, ma quando**,, Accenture

FERRUZZI C, FRONGIA D., **Il disastro informatico: come gestire la crisi** (SegnalazionIT, 2010)

HINNA L., MONTEDURO F., Amministrazioni pubbliche. Evoluzione e sistemi di gestione. ARACNE, 2006

ISTAT, Commissione Tecnica Risk Management, La definizione del Framework e della metodologia operativa per l'introduzione del

processo di Risk Management in Istat, 2010

LEWIS G., **Organizational Crisis Management: The Human Factor**,, Auerbach Publications

PEZZANI, F. Performance management nelle pubbliche amministrazioni e nelle istituzioni internazionali. EGEA, 2009

TALEB, N. N. The Black Swan: the Impact of the Highly Improbable. New York. Random House, 2007

TELECOM ITALIA, **Piano di Sicurezza per la piattaforma ISTAT,** 2010, (documento USO INTERNO)

TELECOM ITALIA, **Progetto dei Fabbisogni SPC per Istat,** 2010, (documento USO INTERNO)

TELECOM ITALIA ,**Piano di Attuazione,** 2010, (documento USO INTERNO)

www.anra.it
www.aiiaweb.it
www.oecd.org
http://twitter.com/nntaleb
http://epp.eurostat.ec.europa.eu

http://www.ferma-asso.org
http://rmmagazine.com
http://delpup.wordpress.com
http://www.theirm.org
http://www.iso.org

risk.istat.it

2011 FORUM PA

Istat