IBM

NUOVI PERCORSI PER LA PUBBLICA AMMINISTRAZIONE

G.Pietro Trovesi
Sistema di gestione per la Sicurezza delle Informazioni

UNINFO

IBM ITALIA aderisce al progetto Impatto Zero® di LifeGate.
Riduce e compensa le emissioni di Co2 con la creazione di nuove foreste.

IMPATTO ZERO® www.lifegate.it LIFEGATE

UNINFO

Ente di normazione per le
Tecnologie Informatiche
e loro applicazioni
Ente federato all'UNI

- **studiare ed elaborare norme nazionali,**
- **partecipare a studio - elaborazione di norme affidate ai Comitati Tecnici internazionali,**
- **Segreteria di Comitati, Sottocomitati e Gruppi di Lavoro di Enti di Normazione inter.li,**
- **svolgere attività proposte da Organismi e Autorità Stato Italiano e UE, da Associazioni di Categoria, da Enti esterni che fanno parte dell'associazione, dai Soci.**

www.polito.uninfo.it

© 2008 IBM Corporation

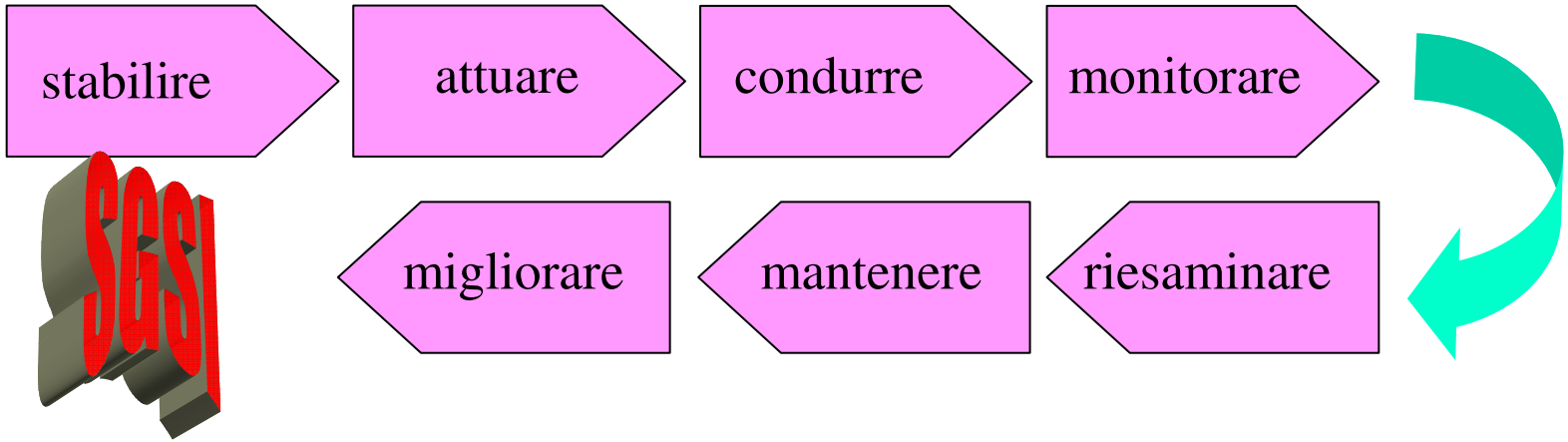
Articolazione normativa Sicurezza delle informazioni: ISO 27K

codice	*contenuti*	*stato*
ISO 27000	Introduzione, definizioni e terminologia usata in tutti gli standard ISO 27k	in elaborazione
ISO 27001	Sistema di gestione per la sicurezza delle informazioni: requisiti	*pubblicata in italiano*
ISO 27002	Code of practices (raccolta di obiettivi di controllo e menu delle migliori prassi dei controllo)	*pubblicata*
ISO 27003	Guida attuativa	in elaborazione
ISO 27004	Misurazione dell'efficacia del sistema di gestione per la sicurezza delle informazioni	in elaborazione
ISO 27005	Gestione dei rischi di sicurezza delle informazioni	in elaborazione
ISO 27006	Guida per il processo di certificazione/registrazione da parte degli organismi accreditati	*pubblicata*
ISO 27007	Guida per l'audit al sistema di gestione per la sicurezza delle informazioni	in elaborazione
ISO 27008-059	Norme dedicate a standard di sicurezza specifici ed alle relative guide applicative (per settore industria, risorsa/area tecnologica)	in elaborazione

© 2008 IBM Corporation

Requisiti generali

L'organizzazione deve



Sistema: Insieme di elementi tra loro correlati o interagenti.

Sistema gestione: sistema per stabilire politiche ed obiettivi, e regole per conseguire tali obiettivi.

Sistema di gestione per la sicurezza delle informazioni

sistema di gestione per guidare e tenere sotto controllo un'organizzazione con riferimento alla sicurezza dei beni.

© 2008 IBM Corporation

PRINCIPALE OBIETTIVO DELLO STANDARD

SUPPORTO
ALLA REALIZZAZIONE E ALLA GESTIONE DI UN
EFFICACE
SISTEMA DI GESTIONE DELLE INFORMAZIONI
USANDO
UN APPROCCIO DI CONTINUO MIGLIORAMENTO

è una norma per la linea manageriale

© 2008 IBM Corporation

I PRINCIPI ISPIRATORI

RECEPIRE
REQUISITI
CONTROLLO
INTERNO

GOVERNANCE

GOVERNO DEL RISCHIO

guida/indirizzo **governo**

POLITICHE E STRATEGIE
OBIETTIVI ISTITUZIONALI

RISK ASSESSMENT

IDENTIFICAZIONE
MISURAZIONE
CLASSIFICAZIONE RISCHI

DEFINIZIONE LIVELLO
RISCHIO RESIDUO

OBIETTIVI DI CONTROLLO

ATTIVITA' DI CONTROLLO

RISCHIO RESIDUO
EFFETTIVO

MONITORAGGIO CONTINUO

© 2008 IBM Corporation

I PRINCIPI ISPIRATORI

- **ADOZIONE DI UN METODO:**
  IL METODO E' ARBITRARIO
  MA DEFINITO E DOCUMENTATO

- **PUNTUALIZZAZIONE OBIETTIVI DI SICUREZZA**

- **MISURE DI SICUREZZA =**
  RISULTATO DEL RISK ASSESSMENT

© 2008 IBM Corporation

I PRINCIPI ISPIRATORI

- **SCELTA CONTROLLI COMPETE AD ORGANIZZAZIONE**
- **CONTROLLI RISPONDONO AI REQUISITI DI BUSINESS**
- **PROCESSO PER ASSICURARE**
  MONITORAGGIO CONTINUO
  (RIESAMI MANAGERIALI, VERIFICHE ED AUDIT)
- **PROCESSO PER ASSICURARE**
  CONTINUO MIGLIORAMENTO

© 2008 IBM Corporation

I PRINCIPI ISPIRATORI DEVONO INTEGRARSI CON GLI OBIETTIVI DELL'ENTE PUBBLICO

DISCIPLINE GESTIONALI

- ADEGUATEZZA E TRASPARENZA DEI CONTROLLI
- VERIFICA LEGALITA'
- ATTENDIBILITA' BILANCIO
- CONFORMITA'
- EQUITA' DI TRATTAMENTO
- FIDUCIA
- LOTTA ALLE FRODI

(regolamenti EU/Corte conti Europea)

© 2008 IBM Corporation

I PASSI PER ISTITUIRE IL SGSI

DEFINIRE IL CAMPO DI APPLICAZIONE ED IL PERIMETRO

DEFINIRE UNA POLITICA

DEFINIRE L'APPROCCIO ALLA VALUTAZIONE DEI RISCHI

IDENTIFICARE E VALUTARE I RISCHI

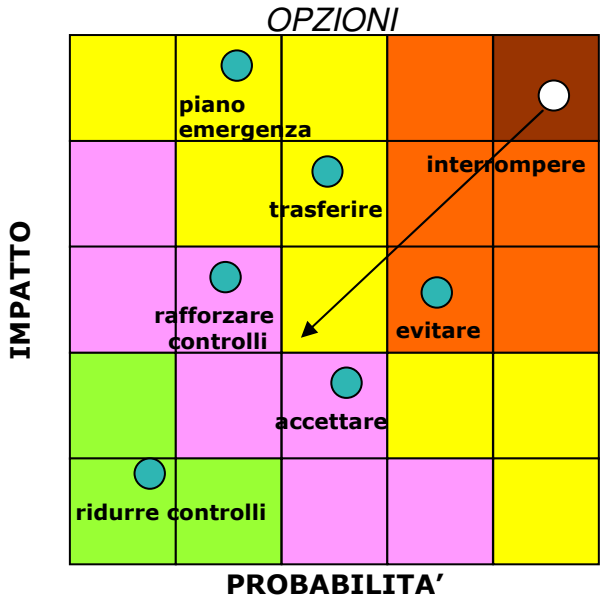
SCELTA OBIETTIVI CONTROLLO E CONTROLLI

© 2008 IBM Corporation

I PASSI PER ISTITUIRE IL SGSI

INDIVIDUARE E PONDERARE OPZIONI TRATTAMENTO RISCHI

1. **applicare controlli appropriati**
   (rafforzamento del controllo)
2. **accettare i rischi**
3. **evitare i rischi**
4. **trasferire i rischi ad altre parti**



CONSAPEVOLEZZA, OBIETTIVITA' MANAGERIALE, NON PIU' SORPRESE

© 2008 IBM Corporation

LE 11 AREE DI ATTENZIONE DELLA NORMA

- *Politiche per la sicurezza*
- *Organizzazione della sicurezza delle informazioni*
- *Gestione dei beni*
- *Sicurezza delle risorse umane*
- *Sicurezza fisica ed ambientale*
- *Gestione delle comunicazioni e della operatività*
- *Controllo degli accessi*
- *Acquisizione, sviluppo e manutenzione dei sistemi informativi*
- *Gestione degli incidenti relativi alla sicurezza delle informazioni*
- *Gestione della continuità operativa*
- *Conformità*

© 2008 IBM Corporation

IL SGSI DEVE ESSERE A REGIME SEMPRE

- ***GESTIRE FUNZIONAMENTO E RISORSE***
- ***MISURAZIONE EFFICACIA CONTROLLI***
- ***FORMAZIONE, ADDESTRAMENTO***
- ***MONITORAGGIO E RIESAME***
- ***AUDIT INTERNI***
- ***AGGIORNAMENTO***
- ***DOCUMENTAZIONE***

© 2008 IBM Corporation

LA NORMA RICHIEDE IL RISCONTRO

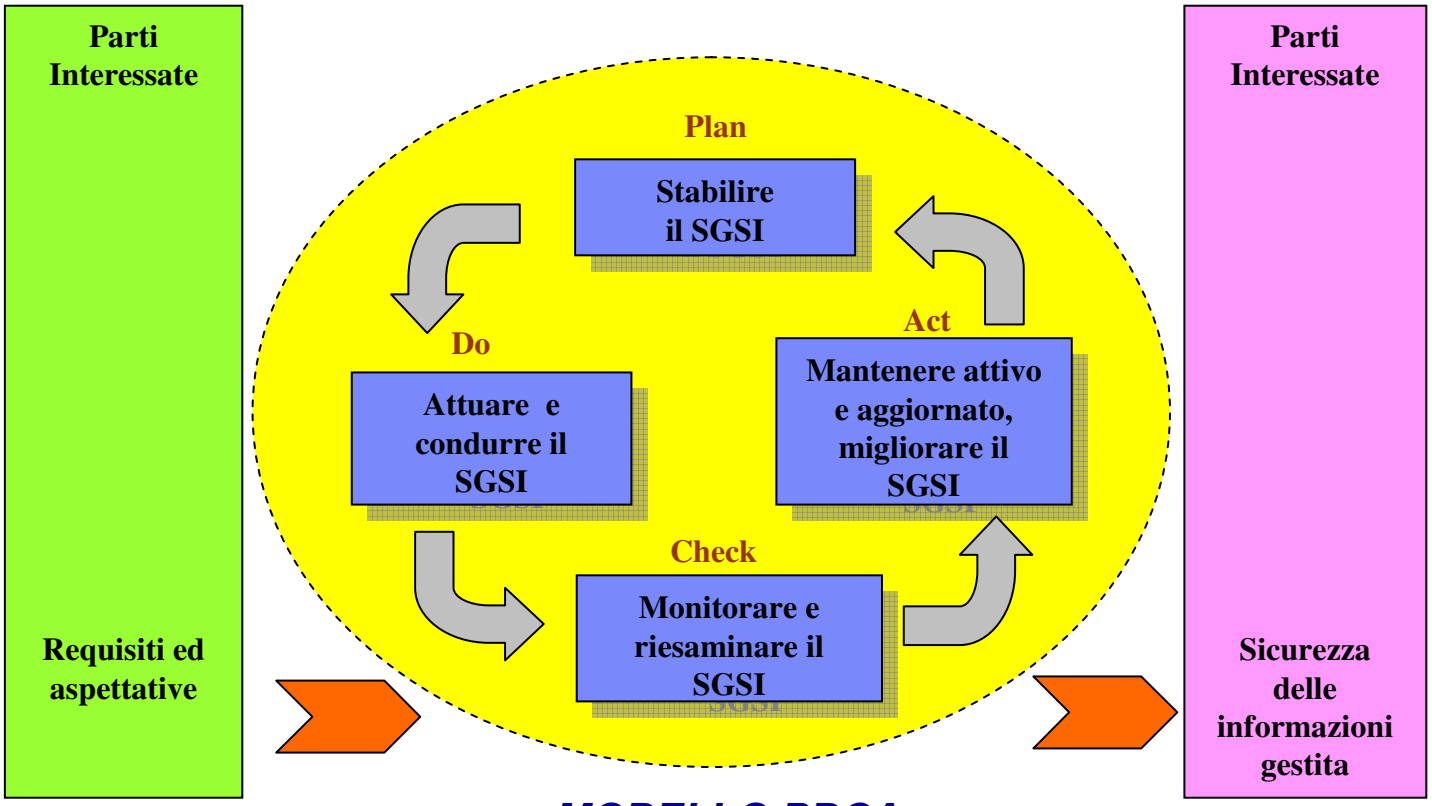
DICHIARAZIONE DI APPLICABILITA'

E' L'ATTESTAZIONE MANAGERIALE CHE LA SICUREZZA DELLE INFORMAZIONI DELLA PROPRIA ORGANIZZAZIONE E' STATA PROGETTATA E REALIZZATA IN CONFORMITA' ALLO STANDARD

adeguati o motiva

© 2008 IBM Corporation

IL SGSI E' SEMPRE MIGLIORABILE



MODELLO PDCA

© 2008 IBM Corporation

IL MODELLO PDCA CONSIDERA TUTTI I COMPONENTI

OBIETTIVI

REQUISITI

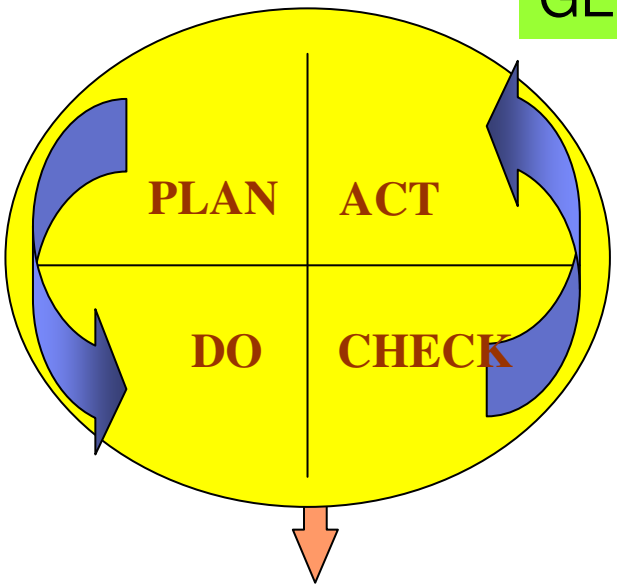
PROCESSO RISK MGMT

RISK ASSESSMENT

RISCHIO RESIDUO

AZIONE MITIGAZIONE
DEL RISCHIO

LIVELLO RISCHIO
ACCETTABILE



GESTIONE

INCIDENTI

AUDIT

MONITORAGGIO CONTINUO
E RIESAME DA PARTE
DELLA LINEA MANAGERIALE

MIGLIORAMENTO

© 2008 IBM Corporation

LA CERTIFICAZIONE

PROCESSO ATTRAVERSO IL QUALE UNA ENTITA' ESTERNA SPECIALIZZATA CONFERMA CHE UN PRODOTTO, PROCESSO O SERVIZIO E' CONFORME AD UNO SPECIFICO STANDARD

- SEGUE SPECIFICI SCHEMI
- GLI SCHEMI PERMETTONO ALLE ORGANIZZAZIONI DI DIMOSTRARE IL LORO GRADO DI ASSURANCE
- PREREQUISITI: *DEFINIZIONE AMBITI D'AZIONE*
  DICHIARAZIONE DI APPLICABILITA'

- NON FORNISCE GARANZIE

© 2008 IBM Corporation

Conclusioni

Le norme Uni Cei Iso/Iec 27000 mettono a disposizione della linea manageriale gli elementi per progettare, realizzare, gestire, monitorare e tenere aggiornato il sistema di gestione per la sicurezza delle informazioni, attraverso misure adeguate alle proprie caratteristiche amministrative, di personale e dell'ambiente tecnologico, proporzionando lo sforzo tecnologico e finanziario per realizzarlo ai rischi.

© 2008 IBM Corporation

Conclusioni

Le norme aiutano a:

- ***assicurare, ragionevolmente e nel continuo, servizi di info. e informazioni affidabili;***
- ***garantire presenza di un reale clima di sicurezza;***
- ***mantenere capacità di esercitare l'azione di monitoraggio continuo;***
- ***governare rischi di conformità con i regolamenti applicabili e con la legislazione, coerentemente con la propensione di rischio dell'organizzazione.***

© 2008 IBM Corporation