



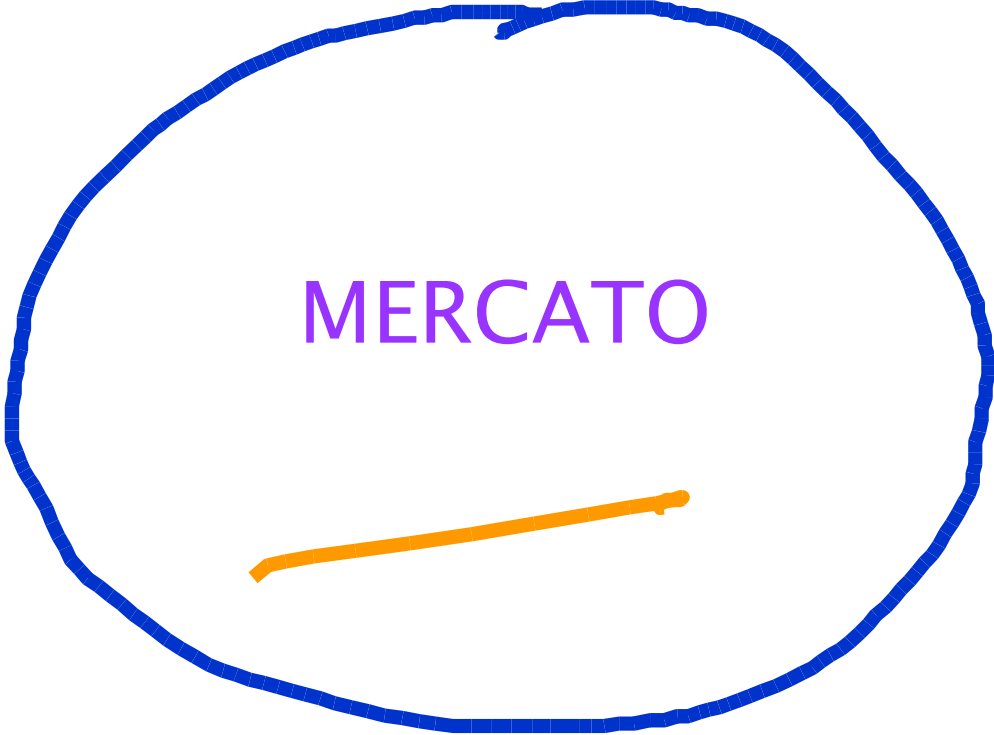
PUNTO DI RIFERIMENTO PER LA QUALITÀ  
QUALITÀ GARANTITA SOTTO LE PARTI

**ISO 27001:2005 – ISMS**  
**Rischi ed Opportunità**  
**Nell' approccio certificativo**



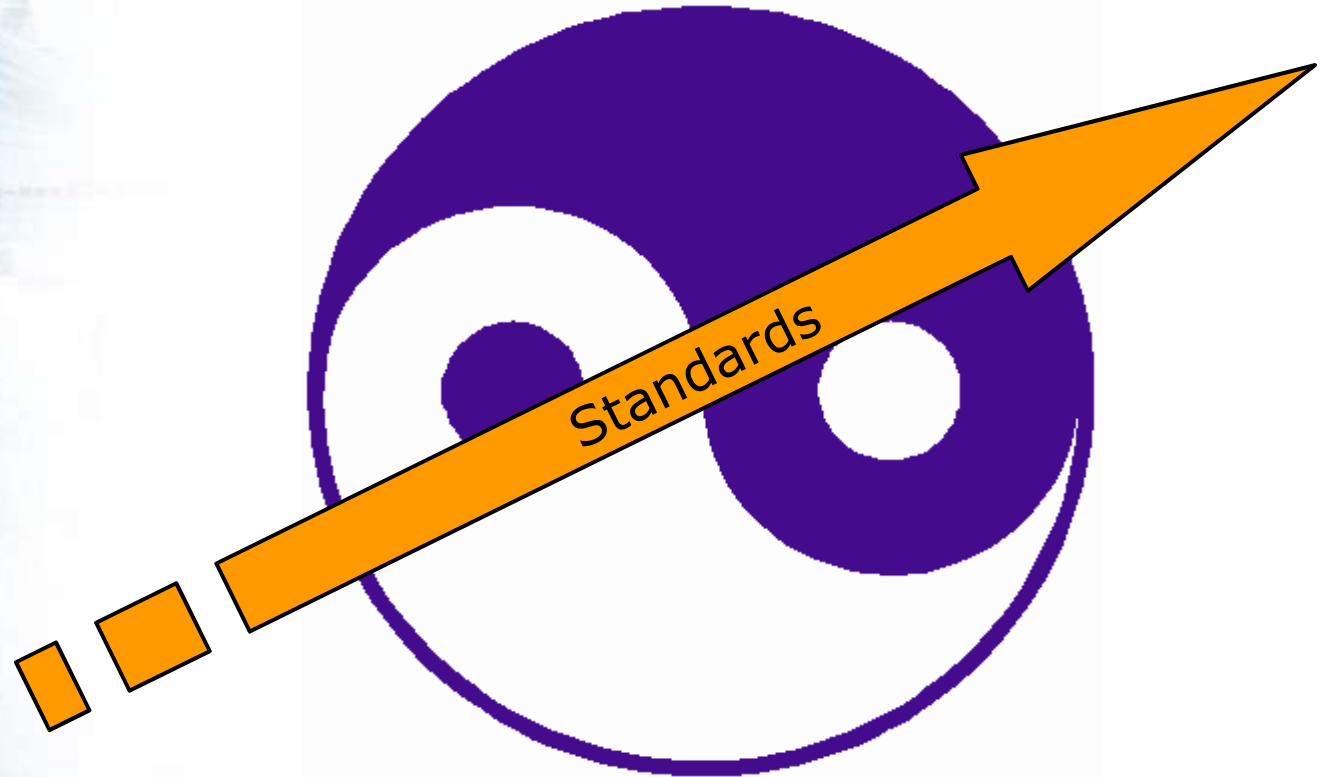
**SINCERT**







# ISO 27001:2005 – ISMS – Rischi ed Opportunita'



# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

## ***Gli Standard sono un presupposto di valore:***

- Definiscono degli importanti elementi di garanzia (contrattuali), interpretabili anche come "livelli di servizio", oppure come specifiche organizzative condivise tra le parti.
- Definiscono la macro-struttura organizzativa per il controllo e per il miglioramento continuo per definiti aspetti del controllo di gestione.
- Introducono l' Auditing interno, quale processo per il monitoraggio della presenza e dell' efficacia dei controlli, nonché la necessità della pianificazione delle attività di miglioramento
- Definiscono le condizioni per una corretta gestione dei diversi rischi, tra i quali quelli relativi alla sicurezza delle informazioni.

# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

## Valore per le Organizzazioni:

- Maggiore fiducia nella capacità di operare con efficienza, ma soprattutto con efficacia per la protezione delle informazioni!
- Maggiore fiducia nella capacità di saper gestire l'impatto delle leggi e regolamenti cogenti
- Miglioramento della cultura di Gestione del Rischio (ove ci si sforzi di introdurre delle buone pratiche di Risk Management)

# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

## Risorse Umane:

- Maggiore consapevolezza
- Migliore probabilità di conservare il lavoro
- Migliore definizione dei ruoli

## Clienti:

- Privacy
- E-commerce
- Gestione del segreto industriale

# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

## Investitori:

- Asset protection capability
- Risk Management capability
- Legal Compliance
- Business improvement
- Business duration

## Autorita - Collettività:

- Anti Bribery
- Maggiore gettito fiscale
- Occupazione

# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

## Management:

- Conoscenza e gestione dei rischi
- Approccio coerente con la IT Governance
- Integrazione del Sistema di Gestione
- Disponibilità di un modello per il miglioramento (Anthony docet!!)

## Come darne evidenza?

(quando la comunicazione è un plus,  
ovvero quando il Cliente vuole la  
migliore fiducia sull' applicazione)

Certificazioni rilasciate secondo  
regole condivise e riconosciute da  
Terze Parti indipendenti.

**ISO 27001:2005**

# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

## 2005 edition

Security policy

Organising information security

Asset management

Human resources security

Physical & environmental  
security

Communications & operations  
management

Access control

Information systems acquisition,  
development and maintenance

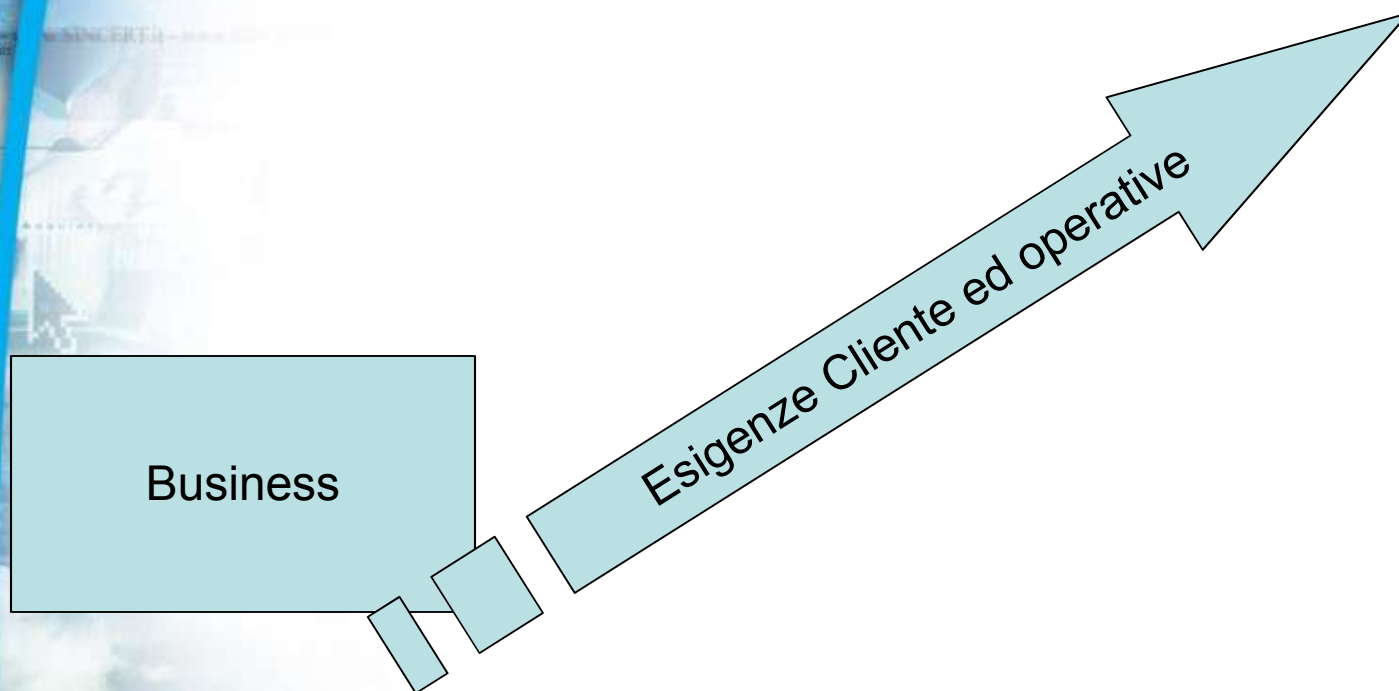
Information security incident  
management

Business continuity management

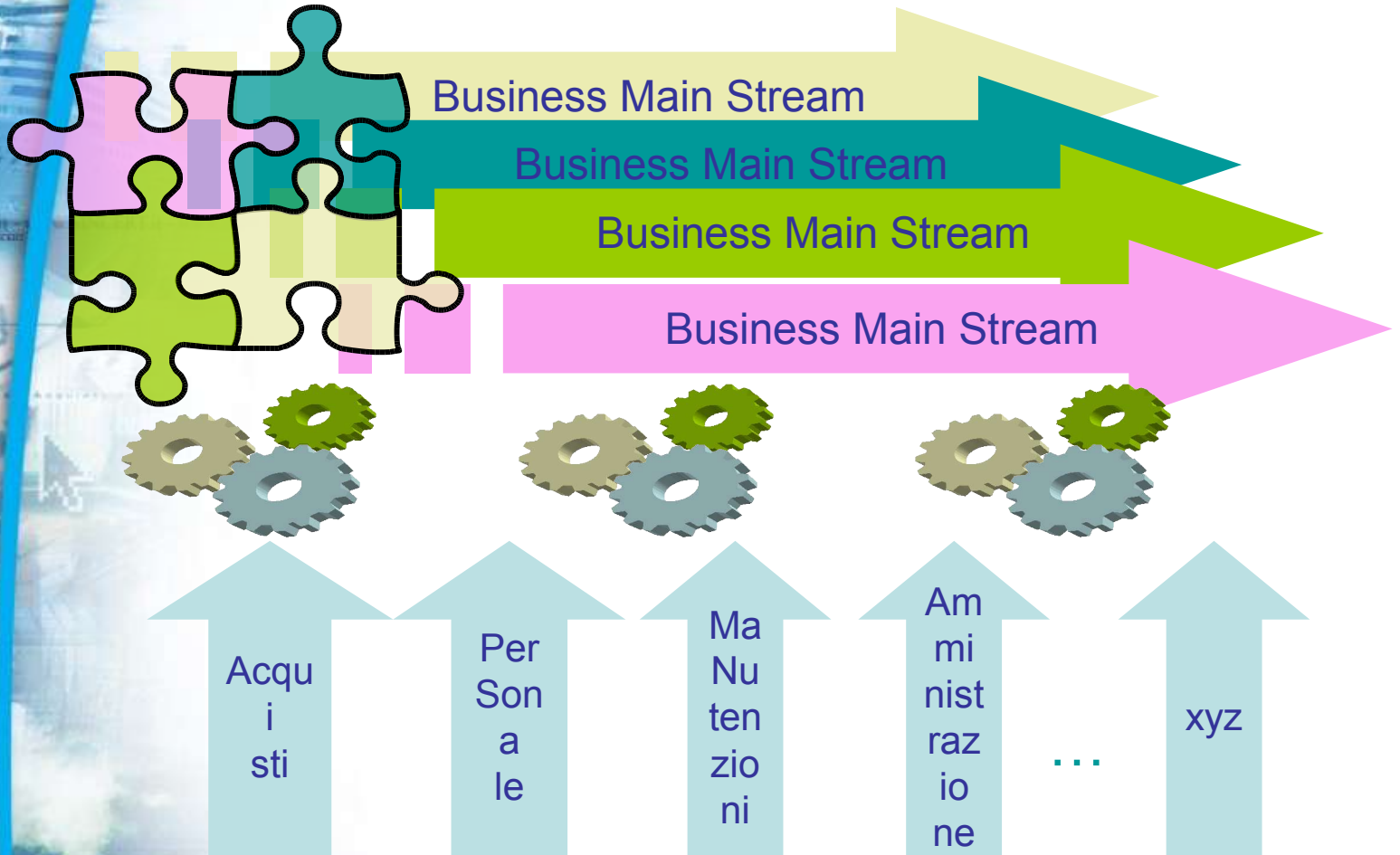
Compliance

**Quali logiche?**

## ISO 27001

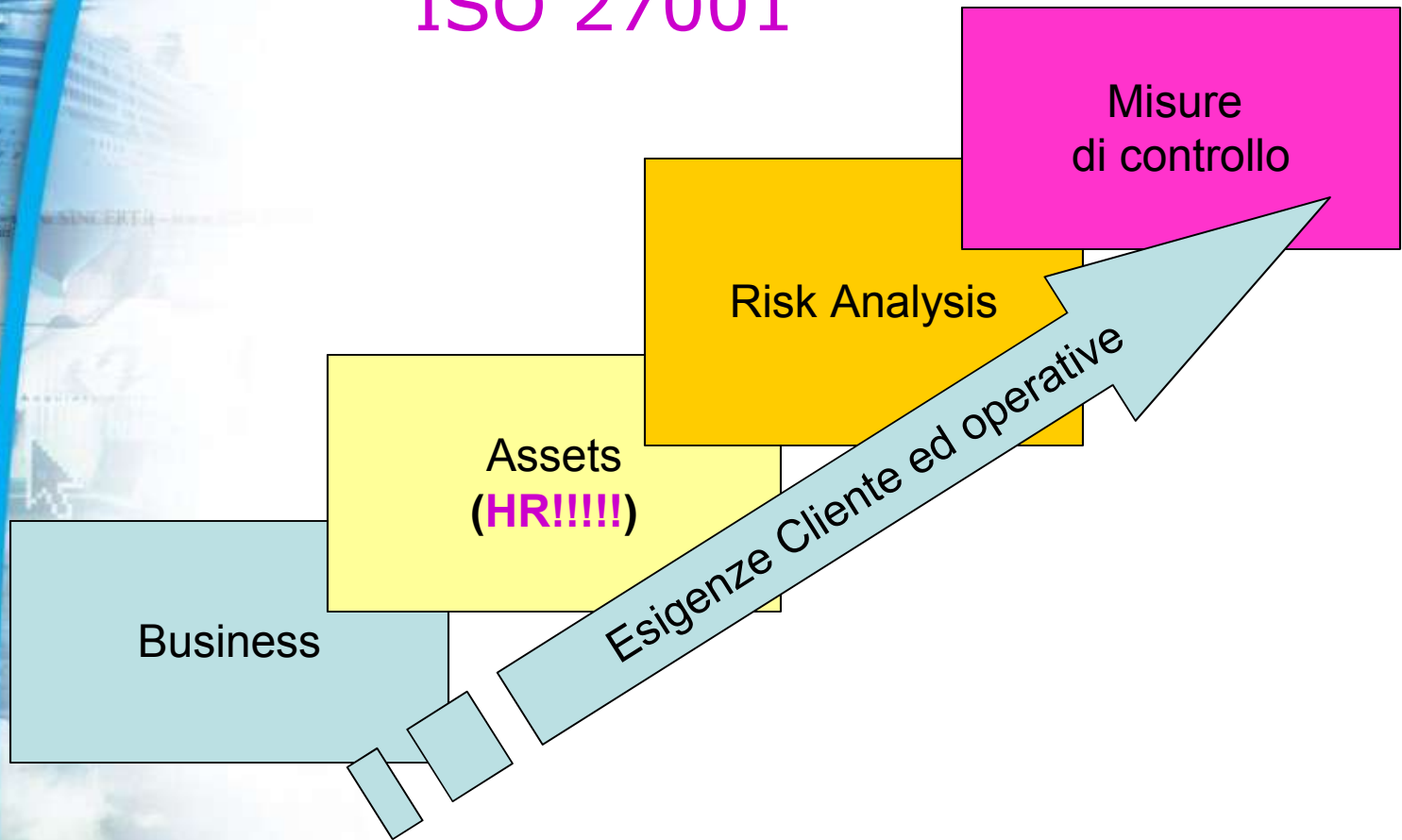


# ISO 27001:2005 – ISMS – Rischi ed Opportunita'



# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

## ISO 27001



# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

## Modello gestionale

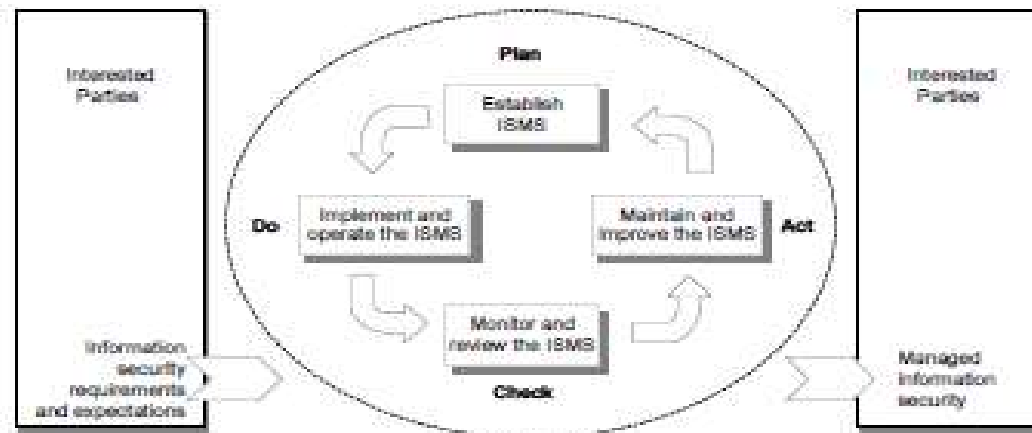


Figure 1 — PDCA model applied to ISMS processes

<b>Plan (establish the ISMS)</b>	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
<b>Do (Implement and operate the ISMS)</b>	Implement and operate the ISMS policy, controls, processes and procedures.
<b>Check (monitor and review the ISMS)</b>	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
<b>Act (maintain and improve the ISMS)</b>	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.



Politiche **IAF** ed **EA** per l'Accreditamento:

**Creare valore per le Parti Interessate**  
ed i  
**presupposti per la libera circolazione di**  
**merci e servizi,**  
grazie al  
**riconoscimento del valore della**  
**certificazione di conformità**  
a standard accettati.

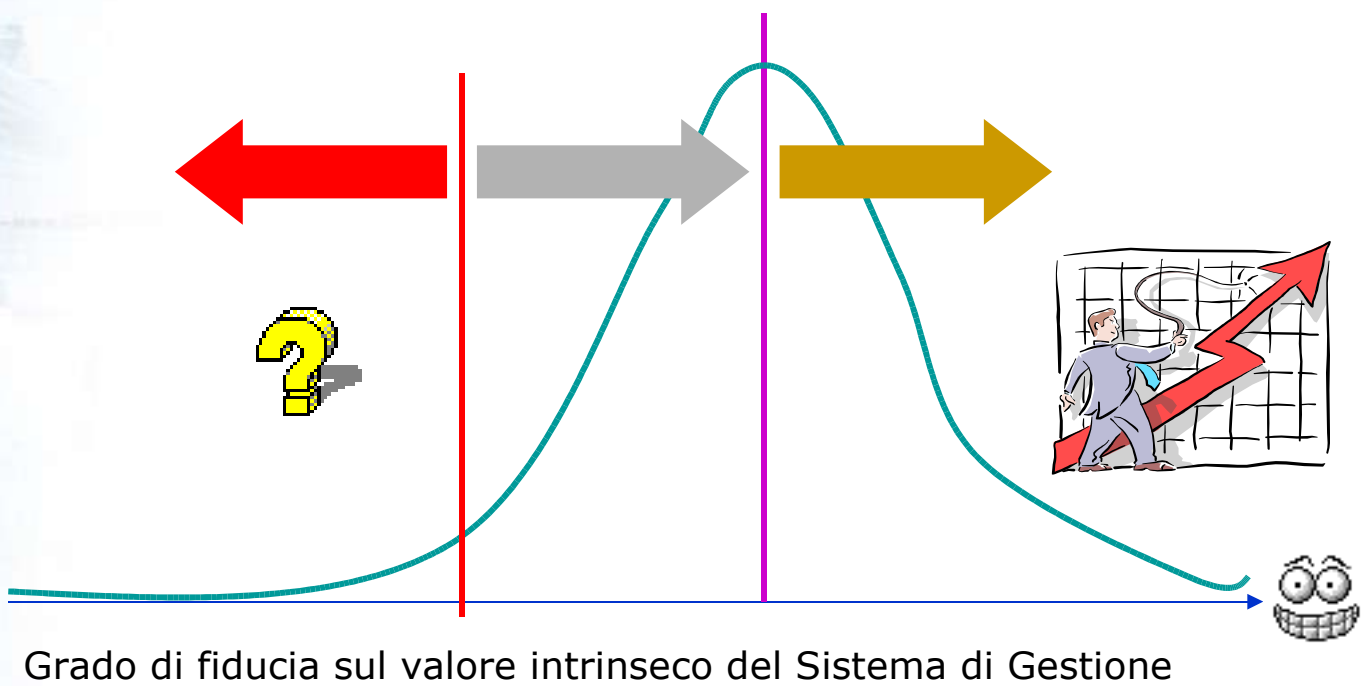
# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

## Certificazione

- Valutazione a fronte dello standard ISO 27001:2005, eseguita con criteri di indipendenza ed assenza di conflitto di interessi.
- Assicurazione nella **continuità della validità**, nel tempo, del Sistema di Gestione adottato, con **prospettive di miglioramento dello stesso**.
- Creazione della esigenza di **consapevolezza**
- Attenzione sulle problematiche di **sicurezza a tutto campo**, non solo ambientali o logiche localizzate in singole aree (fisiche o logiche)



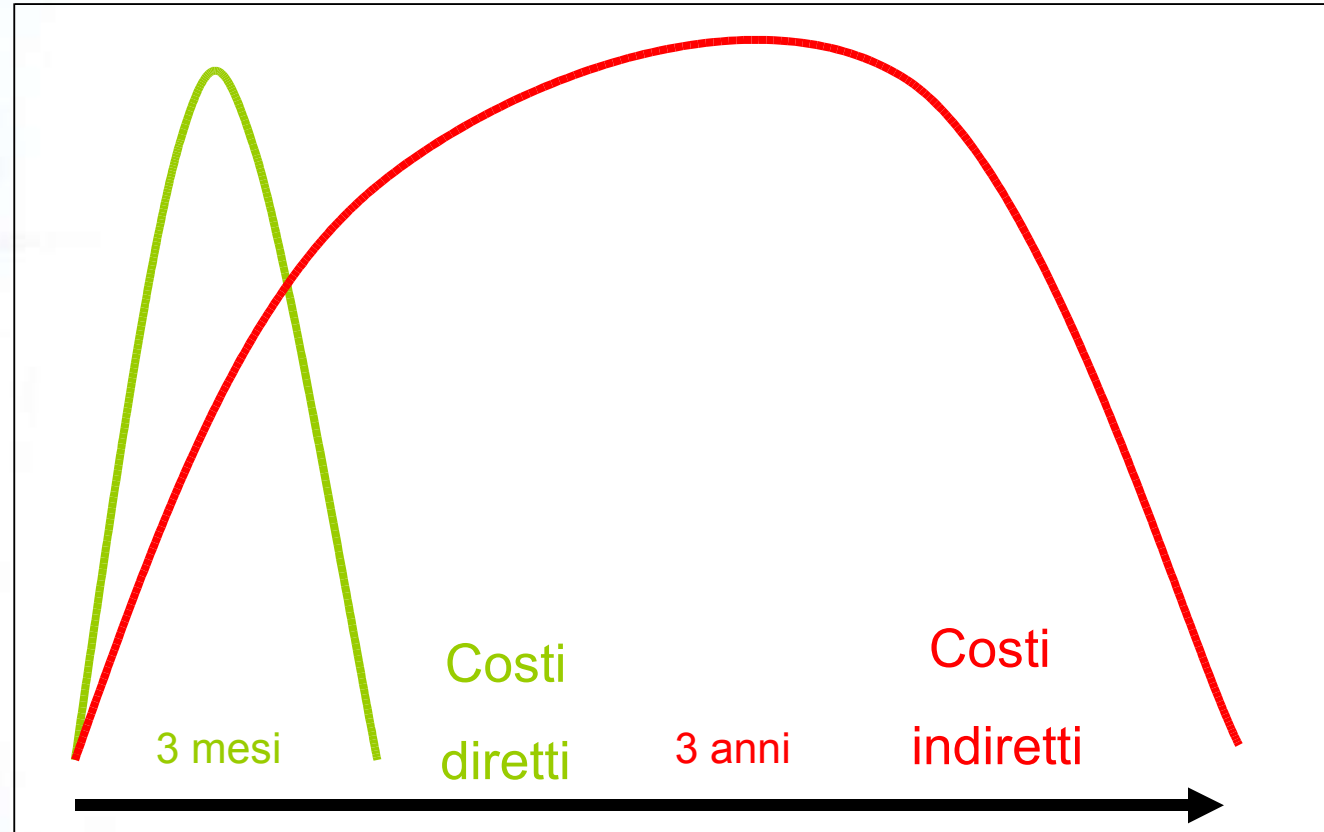
# ISO 27001:2005 – ISMS – Rischi ed Opportunita'



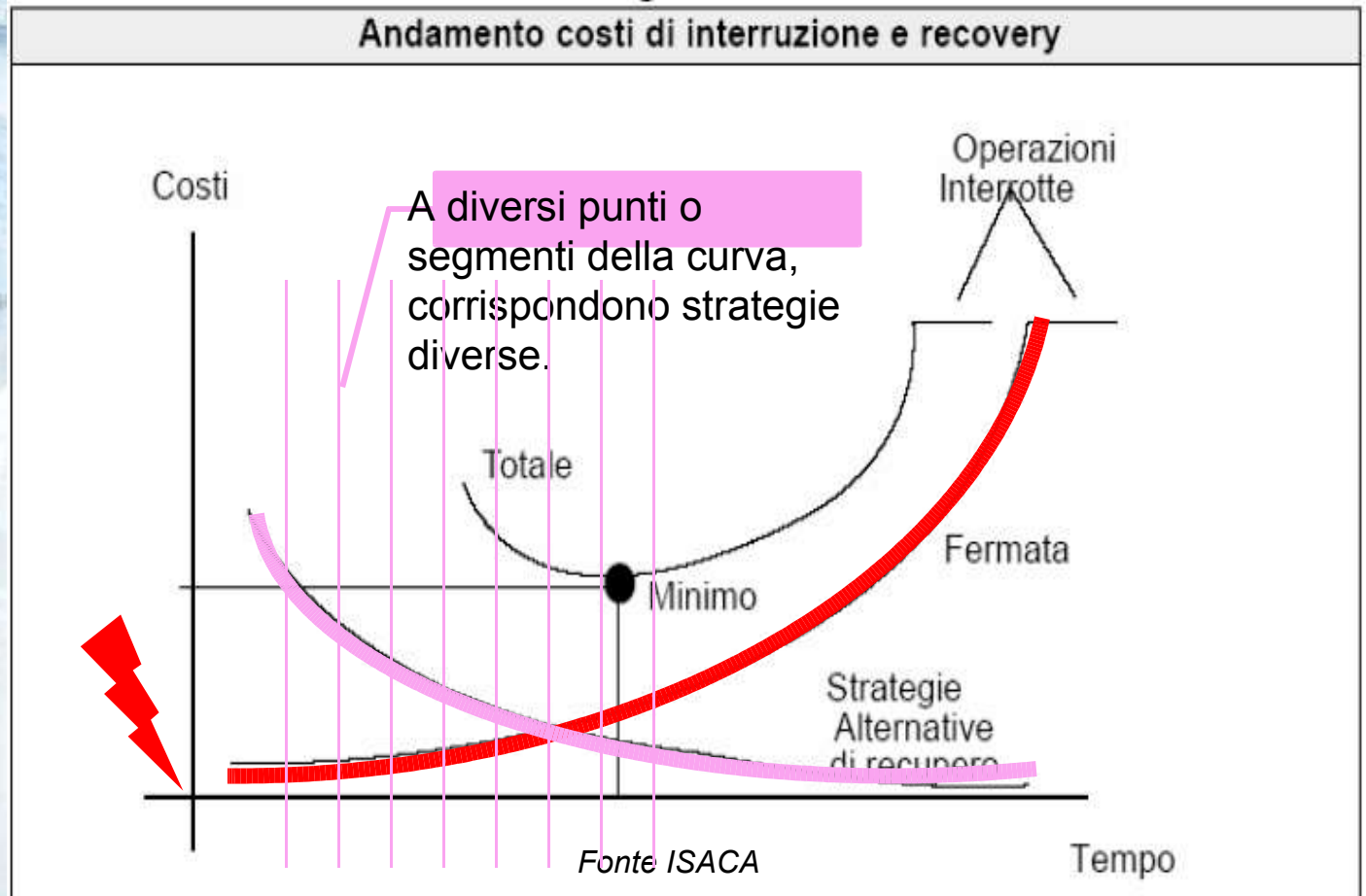
La cultura di Risk Management

La valutazione dell' impatto economico degli incidenti o degli exploit di sistema

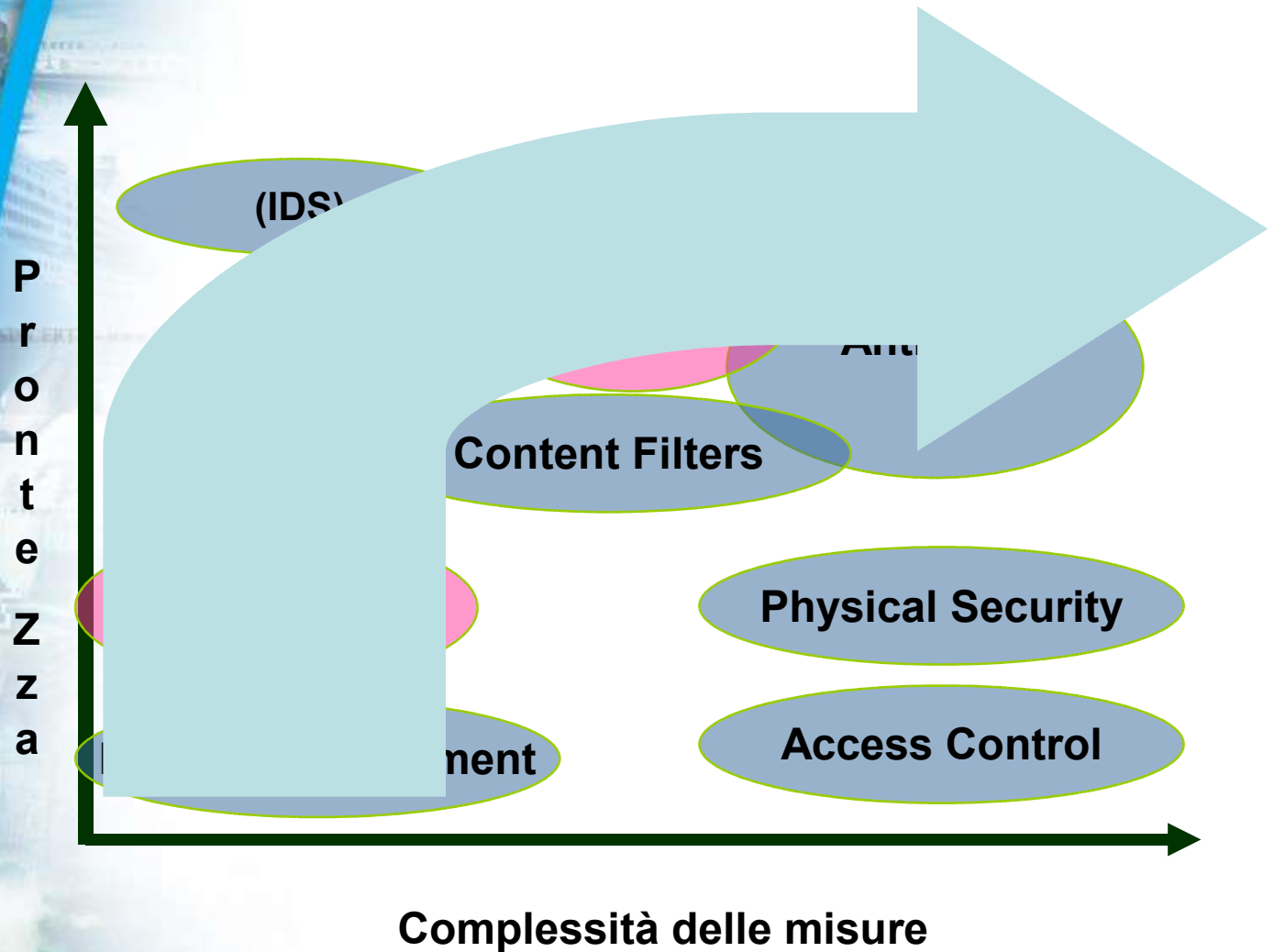
# ISO 27001:2005 – ISMS – Rischi ed Opportunita'



# ISO 27001:2005 – ISMS – Rischi ed Opportunita'



# ISO 27001:2005 – ISMS – Rischi ed Opportunita'



# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

Incidenti, livello di rischio

Malicious Activity

Gap

Sicurezza dell'organizzazione

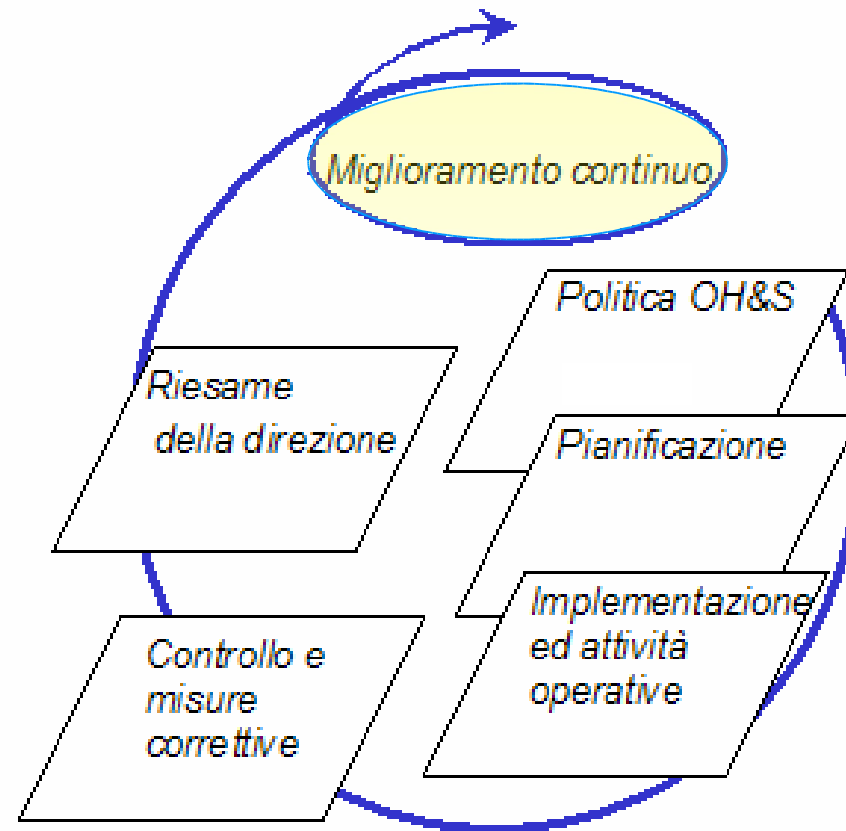
Dati, misure ed infrastrutture di sicurezza

# Comportamenti e migliori pratiche

# Gestione degli incidenti

# Gestione della motivazione

# ISO 27001:2005 – ISMS – Rischi ed Opportunita'



# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

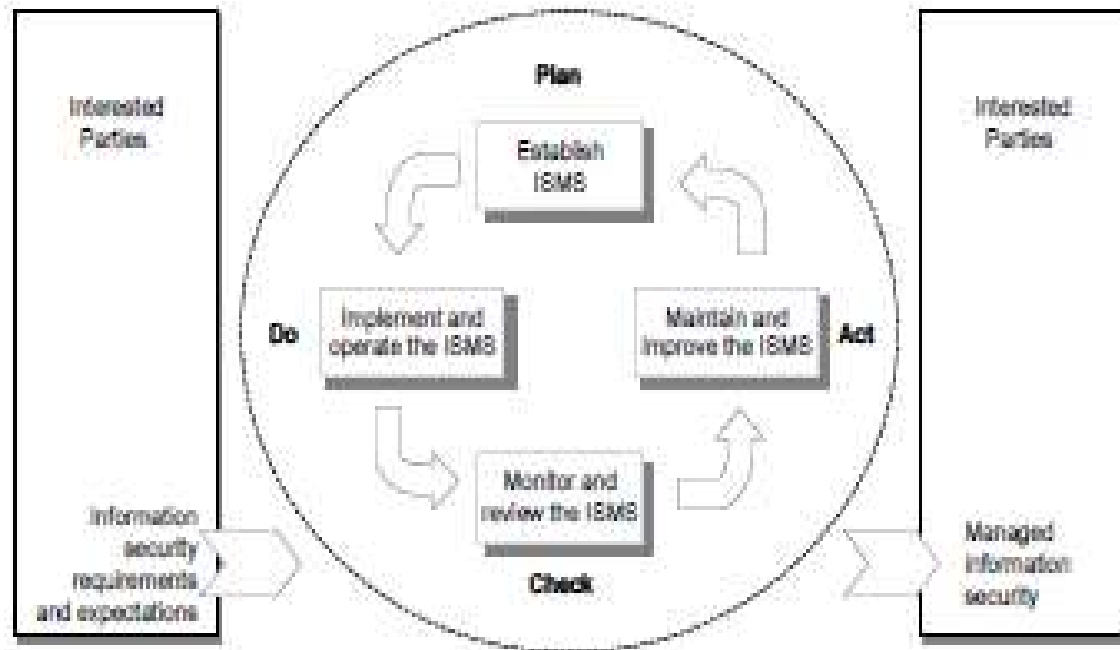


Figure 1 — PDCA model applied to ISMS processes

# Quale fiducia in questo scenario ottimale



# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

Abbiamo visto i possibili benefici

Dobbiamo riconoscere i rischi ed i punti di debolezza

**I principali rischi sono (almeno):**

## Organismi di Certificazione:

- Quale omogeneità di approccio?
- Quali "buone pratiche" promuovono, entro quali limiti?
- Quale intensità e frequenza di monitoraggio?
- Come si mantengono integri rispetto ai possibili conflitti di interesse ed alla indipendenza di giudizio?

# ISO 27001:2005 – ISMS – Rischi ed Opportunita'



Auditor:

- Correttezza (accountability)
- Competenza ed abilità



**DANGER**



Competenza:

Il saper usare la conoscenza;  
ma quale estensione deve avere tale  
conoscenza, affinché il processo di  
auditing sia efficace?

Possono essere accettati diversi  
approcci di audit, in quali fasi?

# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

Organizzazioni:

- Se non è un' istanza interna vi sono i rischi di:
  - Moral hazard
  - Asymmetric Information
- Definizione dell' ambito
- Metodologia di valutazione dei rischi
- Management del "Risk Appetite" (SoA)

} Vs OdC e  
mercato

**La gestione di questi rischi  
è parte integrante del  
processo di accreditamento**

# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

**Grazie all' accreditamento è possibile monitorare le prestazioni ed i comportamenti degli OdC.**

**Si verifica, innanzi tutto, che l' O.d.C. operi con politiche dettate dalle parti interessate**

**(ISO IEC 45012:98)**

Gradi di libertà commerciale ed operativi dell' OdC

Sistema di Gestione interno allo stesso OdC

# ISO 27001:2005 – ISMS – Rischi ed Opportunita'

L' Accredитamento svolto sotto l' egida IAF/EA garantisce almeno:

Competenze tecniche dello O.d.C. ed Auditor



Competenza di Auditing



Tempo di Auditing



Campionamento



Indipendenza



## Principali Rischi

Possibili interpretazioni delle logiche di accreditamento e di certificazione

Minore è il tempo allocato agli Audit, maggiore è il conseguente **Rischio di Audit**

Minore è la competenza di Auditing, maggiore è la possibilità di avere una sottovalutazione degli aspetti organizzativi ed in particolare della “**consapevolezza**”

**Approccio commerciale**



**Buon Lavoro**