Le certificazioni di sicurezza e la direttiva europea 114/08

Roma, 27 Maggio 2010

mediaservice.net
CORPORATE SECURITY & IMAGE

Presentazione Relatore

Fabio Guasconi

- Presidente del SC27 di UNINFO e membro del direttivo
- Head of Delegation per l'Italia, JTC1/SC27 ISO/IEC
- ISECOM Deputy Director of Communications
- ESCoRTS Stakeholder Advisory Board
- Membro di CLUSIT, ITSMF, ANSSAIF, ISACA Roma
- CISA, CISM, LA27001, ITILv3, ISFS, PCI-QSA

- **Team Manager, Senior Security Advisor @ Mediaservice.net**

Programma

- **Sintesi dei requisiti della direttiva**
- **Norme applicabili**
- **Uso delle norme e certificazione**
- **Sistema di gestione per la sicurezza**

Direttiva 114/2008: requisiti

Infrastruttura critica europea

Asset, un sistema o una sua parte, essenziale per il funzionamento della società e il cui danneggiamento o distruzione avrebbe un significativo impatto in tale ambito su due stati membri.

Criteri

- Perdita di vite umane
- Effetti economici (anche disservizi e danni ambientali)
- Effetti pubblici (impatti psicologici, servizi essenziali)

Individuazione e designazione delle infrastrutture critiche europee

Direttiva 114/2008: requisiti

Piani di sicurezza per gli operatori

1. Identificazione degli asset (elementi)
2. Analisi dei rischi sulla base degli scenari di minaccia, vulnerabilità e impatti potenziali
3. Identificazione, selezione e prioritizzazione delle contromisure (permanenti o graduali):
   a) Tecniche
   b) Organizzative
   c) Controllo e verifica
   d) Comunicazione
   e) Consapevolezza e addestramento
   f) Sicurezza dei sistemi informativi

Funzionari di collegamento e modalità di comunicazione

Valutazione delle minacce (con relazione a EC biennale)

Direttiva 114/2008: highlights

- La Commissione, in collaborazione con gli Stati membri, elabora linee guida per l'applicazione dei **criteri intersettoriali e settoriali** e fissa soglie approssimative da utilizzare per l'individuazione delle ECI (art 3)
- È necessario il consenso dello Stato membro nel cui territorio è ubicata l'infrastruttura che deve essere designata come ECI (art 4)
- La Commissione può elaborare, in cooperazione con gli Stati membri, linee guida metodologiche comuni per la **valutazione dei rischi** in relazione alle ECI (art 7)
- Gli Stati membri adottano le misure necessarie per conformarsi alla presente direttiva entro il **12 gennaio 2011** (art 12)
- Settori per le ECI: **Energia** (Elettricità, Petrolio, Gas), **Trasporti** (Stradale, Ferroviario, Aereo, Navale interno ed esterno) (Allegato 1)

Regolamento UE No 73/2010

Stabilisce i requisiti relativi alla qualità dei dati aeronautici e delle informazioni aeronautiche per il cielo unico europeo

Allegato VII, PARTE C

1. Gli obiettivi di gestione della protezione sono:

— garantire che i dati aeronautici e le informazioni aeronautiche ricevuti, prodotti o altrimenti utilizzati, siano protetti da interferenze e che possano accedervi solo le persone autorizzate,

— fare in modo che le misure di gestione della protezione di un'organizzazione rispondano ai requisiti nazionali o internazionali adeguati in materia di infrastrutture critiche e continuità delle operazioni e alle norme internazionali in materia di gestione della protezione, comprese le norme ISO di cui all'allegato III, **punti 22 e 23***.

2. Per quanto riguarda le norme ISO, il relativo certificato emesso da un organismo debitamente accreditato è considerato una prova sufficiente di conformità. Le parti di cui all'articolo 2, paragrafo 2, acconsentono a rendere nota all'autorità nazionale di vigilanza la documentazione relativa alla certificazione su richiesta della medesima.

***ISO/IEC 17799:2005**, ISO 28000:2007

Programma

- **Sintesi dei requisiti della direttiva**
- **Norme applicabili**
  - ISO/IEC 27001:2005
  - ISO/PAS 22399:2007
  - BS OHSAS 18001:2007
  - ISO 31000:2009
  - ISO/IEC 15408
- **Uso delle norme e certificazione**
- **Sistema di gestione per la sicurezza**

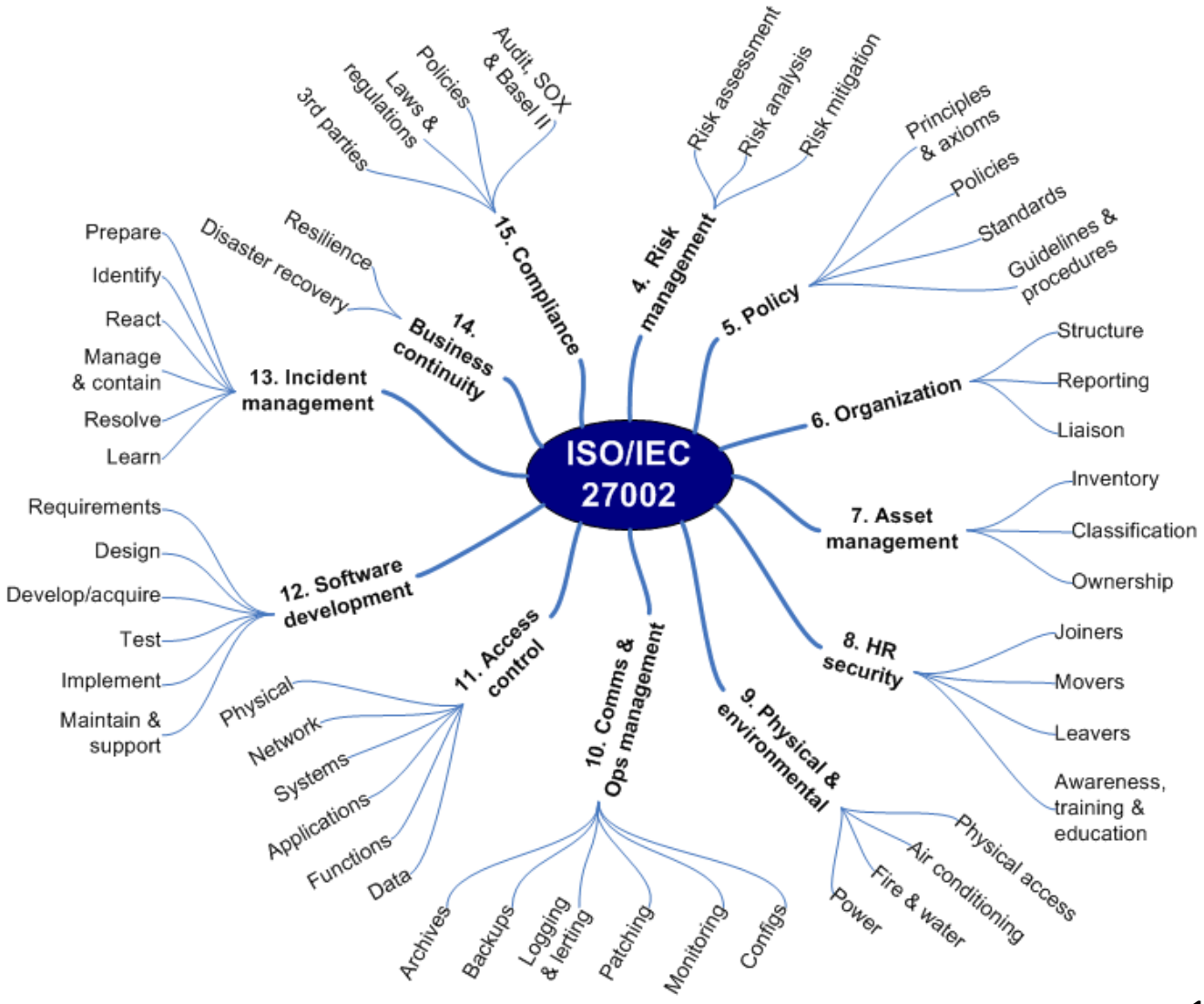
ISO/IEC 27001:2005

Sistema di Gestione per la Sicurezza delle Informazioni (SGSI o **ISMS**)

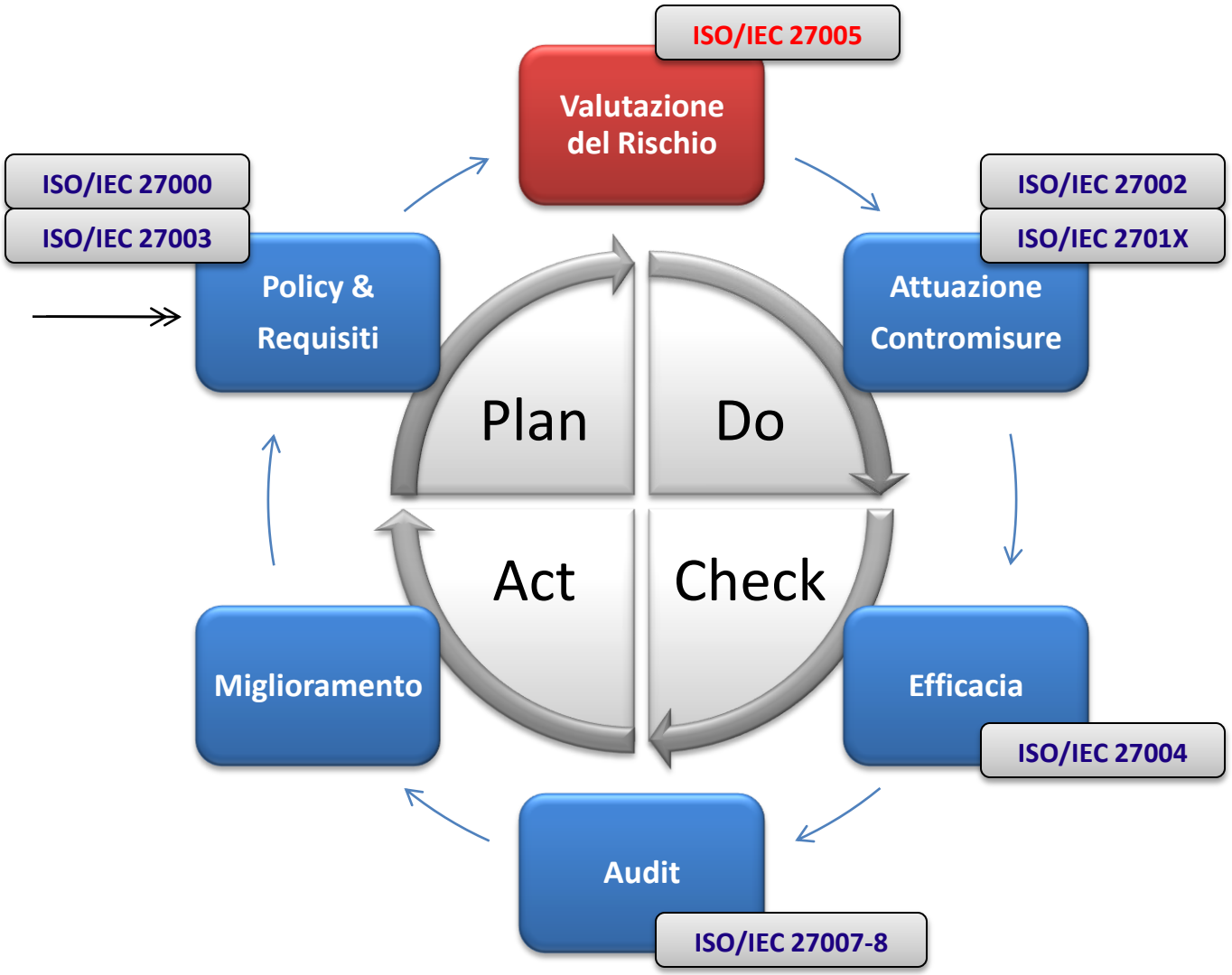
Un SGSI è progettato per assicurare la selezione di controlli per la sicurezza adeguati e proporzionati, in grado di proteggere gli asset informativi e dare fiducia alle parti interessate.

- Impostazione di sistema (coinvolgimento del management, documentazione)
- Applicabilità aperta a ogni tipo di organizzazione
- Flessibilità dell'ambito di applicazione
- Approccio ciclico (PDCA)
- Orientamento ai processi
- Parte di framework completo
- Indica **cosa** fare, non **come**
- Orientata al miglioramento continuo
- Universalmente riconosciuta
- Si può certificare

ISO/IEC 27002:2005



Norma ISO/IEC 27001:2005

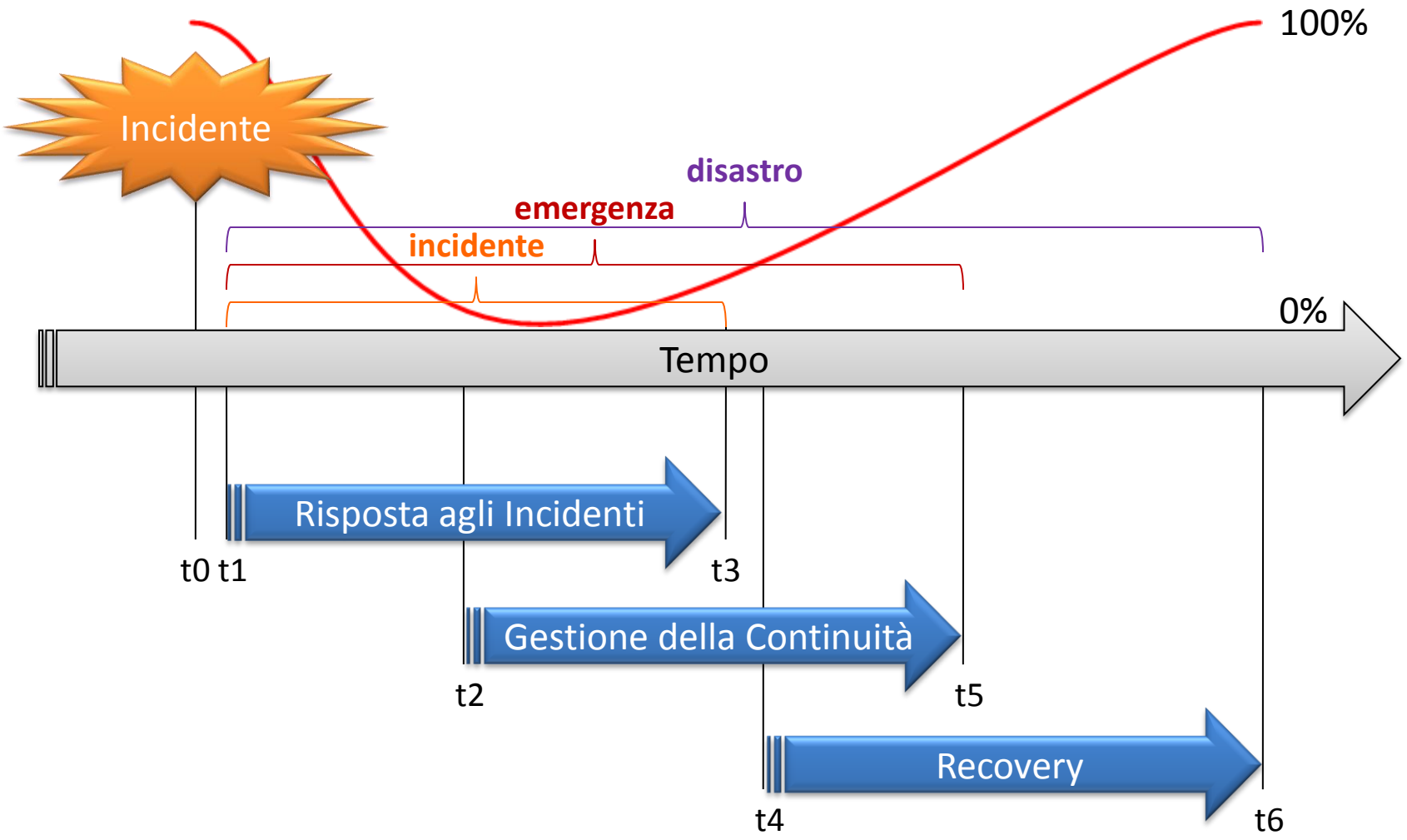


ISO/PAS 22399:2007

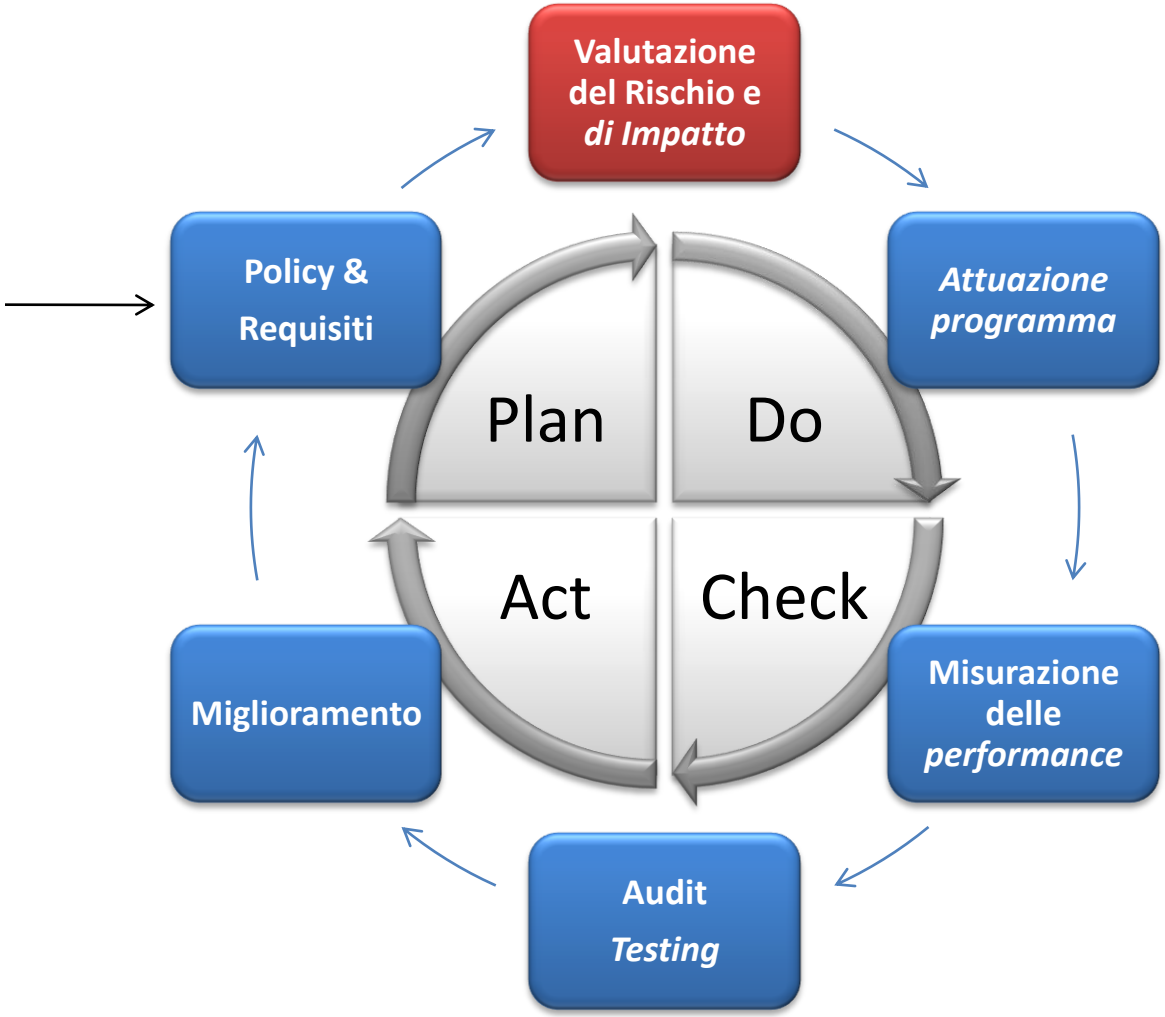
Linee guida per garantire la prontezza verso gli incidenti e la gestione della continuità operativa

- Impostazione di sistema (coinvolgimento del management, documentazione)
- Applicabilità aperta a ogni tipo di organizzazione
- Approccio ciclico (PDCA)
- Orientamento ai processi
- Orientata al miglioramento continuo
- Universalmente riconosciuta (nella versione inglese BS 25999)
- **Non** si può certificare (futura 22301 sì)

ISO/PAS 22399:2007



ISO/PAS 22399:2007



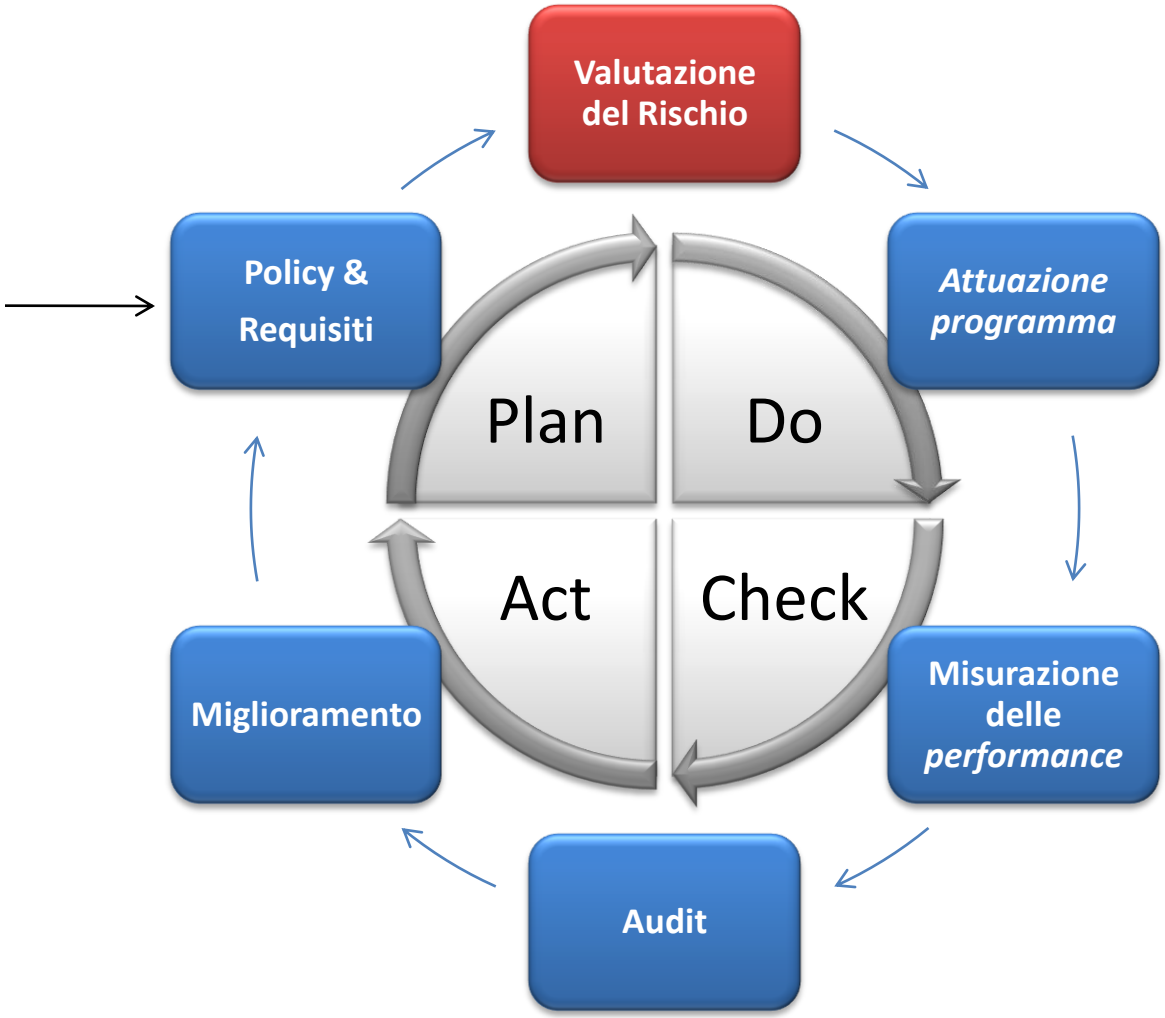
BS OHSAS 18001:2007

Sistema di gestione per la salute e la sicurezza sul lavoro

Un sistema volto a minimizzare i rischi all'incolumità dei lavoratori e delle altre parti coinvolte nelle attività dell'organizzazione.

- Impostazione di sistema (coinvolgimento del management, documentazione)
- Applicabilità aperta a ogni tipo di organizzazione
- Approccio ciclico (PDCA)
- Orientamento ai processi
- Orientata al miglioramento continuo
- Universalmente riconosciuta
- Si può certificare

BS OHSAS 18001:2007

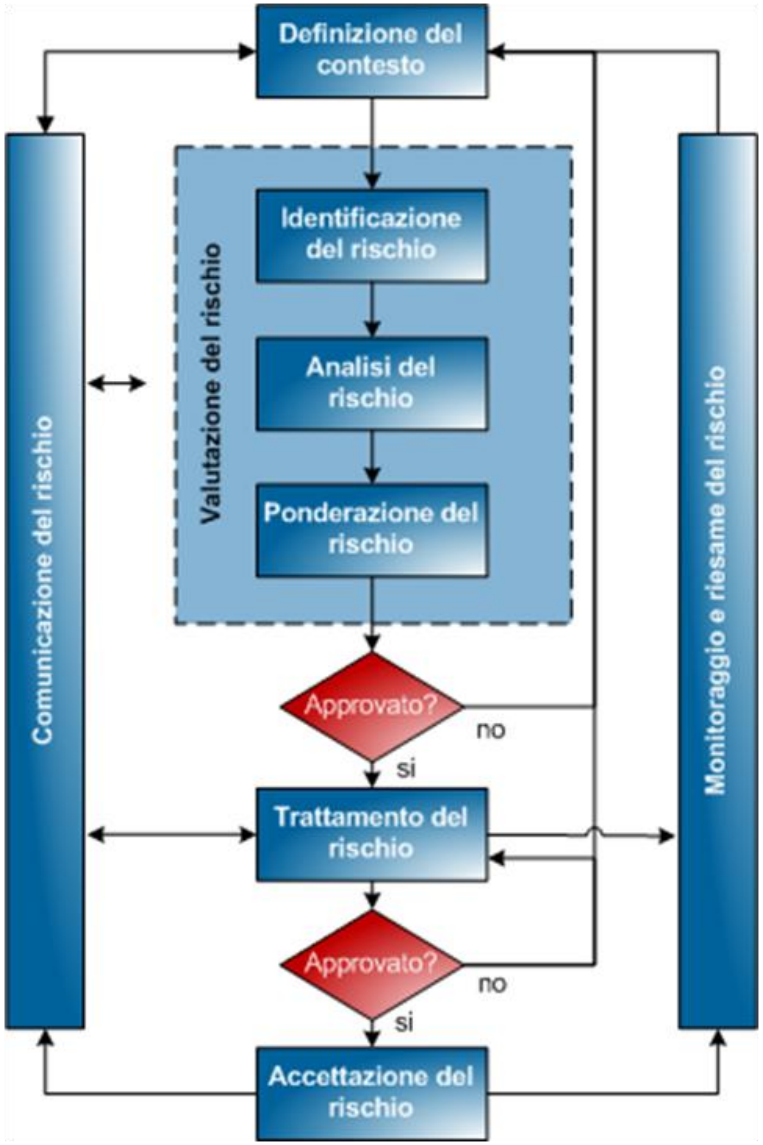


ISO/IEC 31000:2009

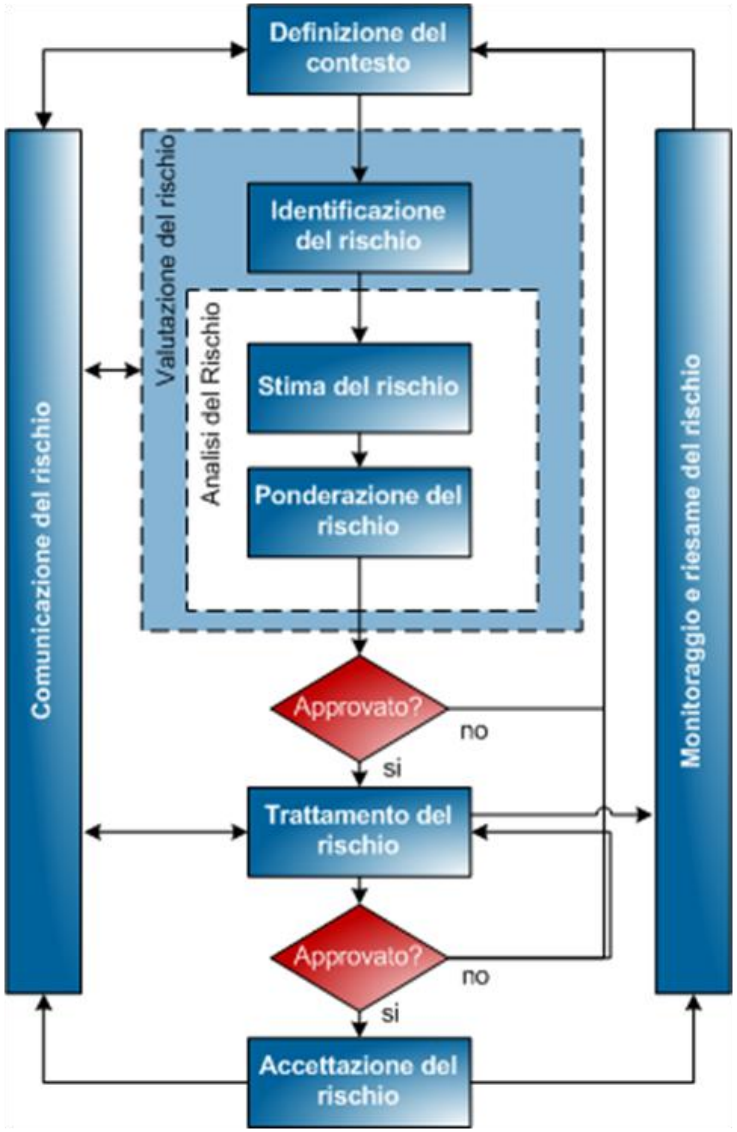
Gestione del rischio — Principi e linee guida

- Impostazione compatibile con i sistemi (coinvolgimento del management, documentazione)
- Orientamento all'impostazione di un framework
- Applicabilità aperta a ogni tipo di organizzazione
- Considerazione di tutti i tipi di rischio
- Base per armonizzare la gestione del rischio nelle norme
- Di alto livello
- **Non** si può certificare

ISO/IEC 31000:2009



ISO/IEC 27005:2008 (ISRM)



ISO/IEC 15408: Common Criteria

Criteri di valutazione per la sicurezza IT

- Impostazione compatibile con i sistemi (coinvolgimento del management, documentazione)
- Rivolto alla sicurezza di un prodotto
- Applicabile a qualsiasi prodotto IT
- **Non** è basato sul rischio
- Universalmente riconosciuto
- Dice **cosa** e **come** fare
- Si può certificare

Applicabilità diretta

27001, 23999, 18001

Sono per loro natura direttamente applicabili alla gestione di diversi aspetti della sicurezza.

31000

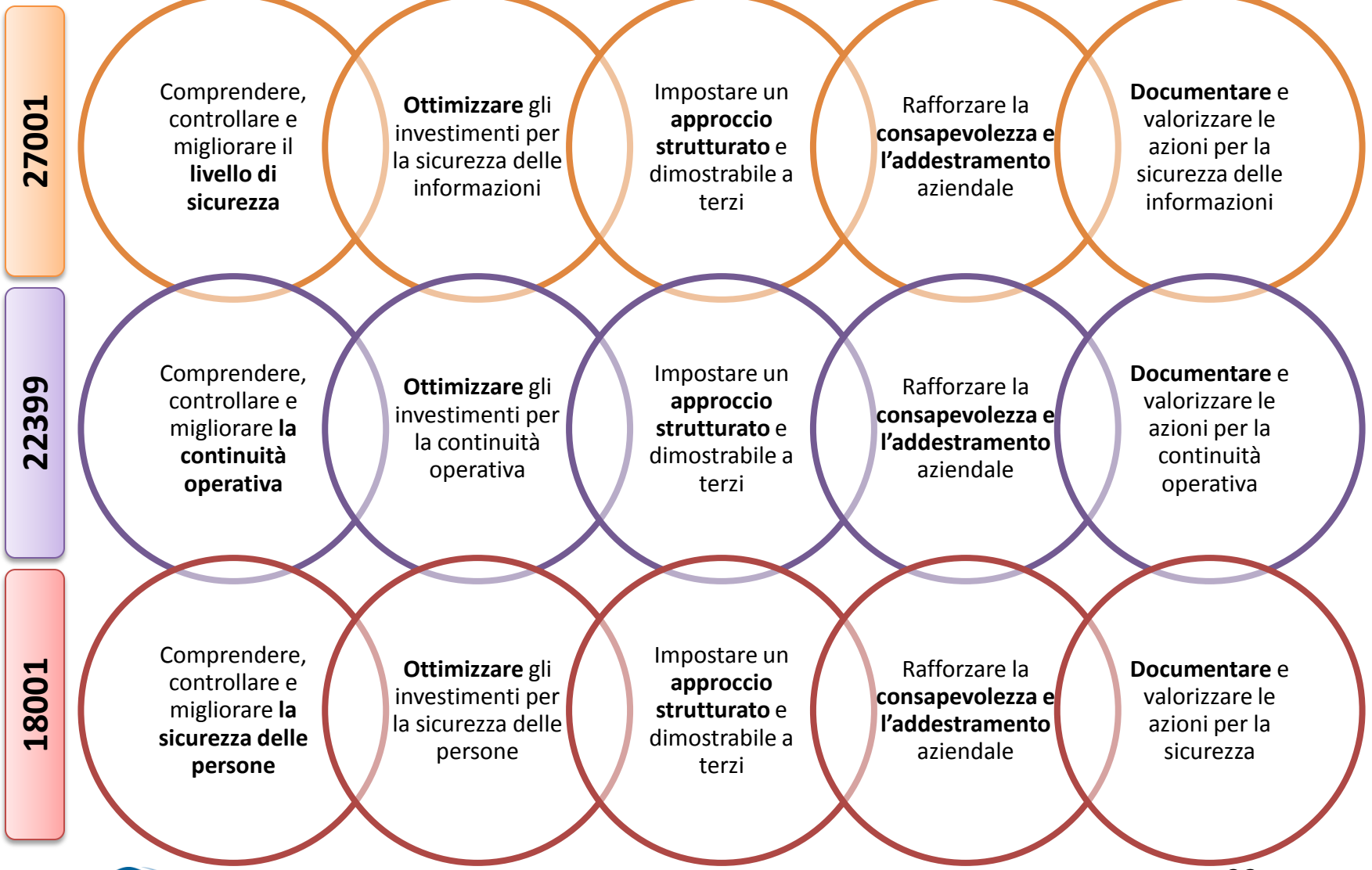
E' assolutamente centrale per l'ambito ma resta **di troppo alto livello** per potersi applicare (anche utilizzando la 31010)

E' necessaria una metodologia più specifica, come suggerisce peraltro la direttiva.

15408

E' un mattone importante per raggiungere livelli di sicurezza accettabili ma è **limitatamente applicabile** a contesti di sistema.

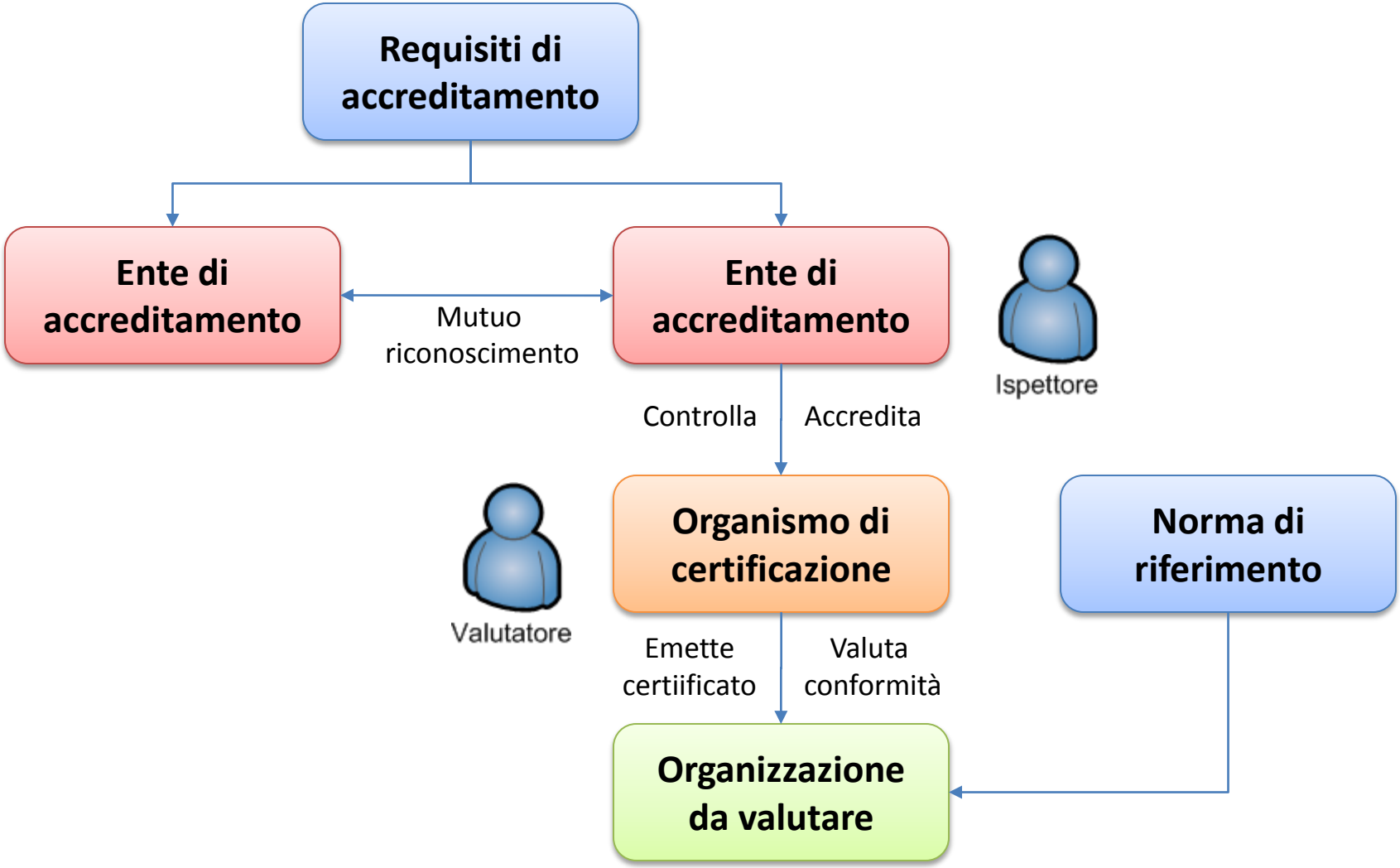
Sintesi degli obiettivi



Programma

- Sintesi dei requisiti della direttiva
- Norme applicabili
- **Uso delle norme e certificazione**
- Sistema di gestione per la sicurezza

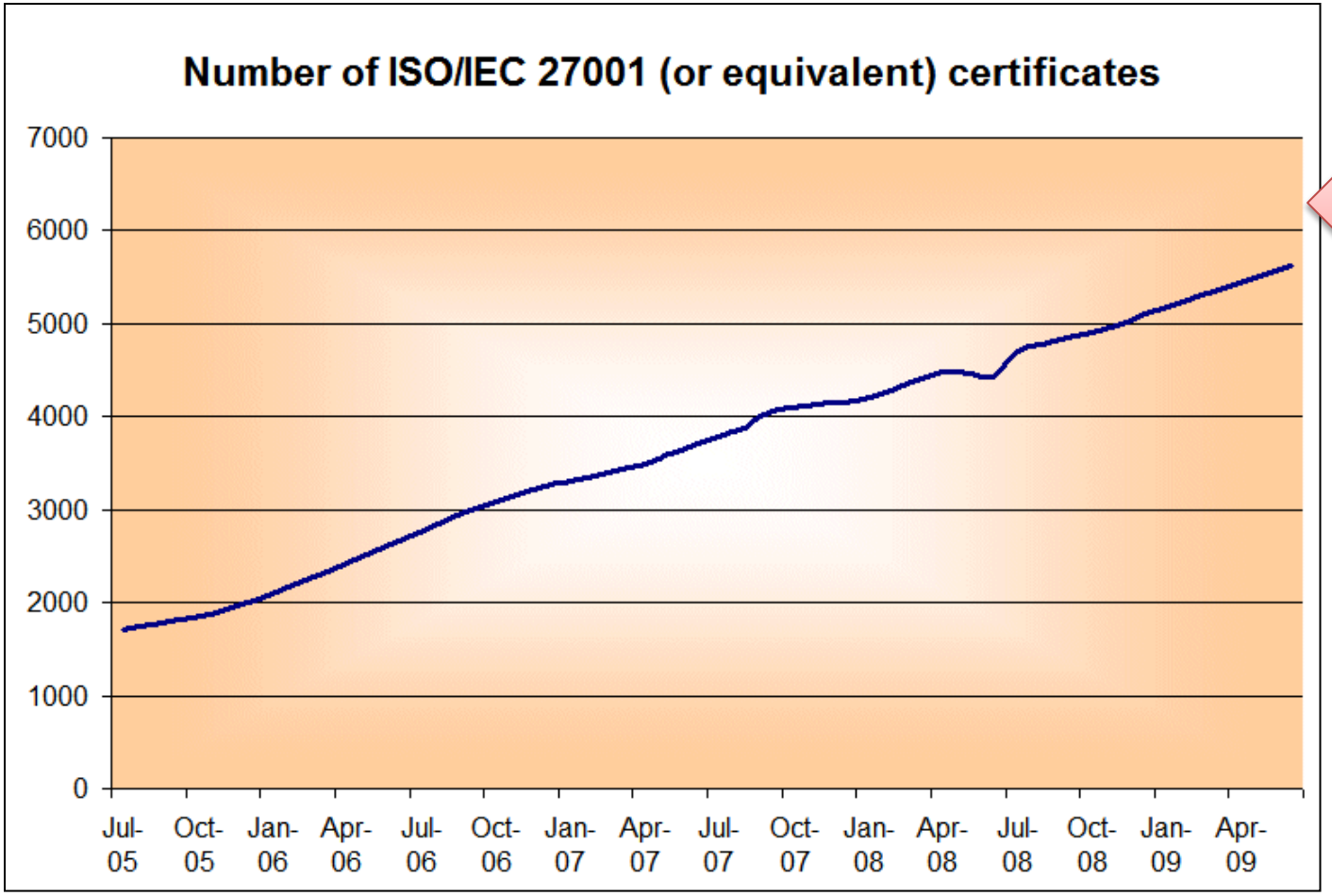
Esempio di schema di certificazione



Certificazione

- La certificazione è basata sul concetto della fiducia (**trust**)
- Una **terza parte indipendente** valuta la conformità rispetto a uno o più criteri (norme) e ne valida la bontà
- L'accreditamento, inteso come **controllo del controllore**, può essere più o meno forte (modello a campione o modello esaustivo)
- Le certificazioni dei sistemi di gestione attualmente diffuse sono un sistema a **bassa garanzia** ma possono rappresentare un valido modo per **dimostrare** qualcosa a terzi

Certificati 27001 Worldwide



Certificati in Italia

Norma	Siti Produttivi	Certificati
AVSQ MIA	9	5
BS OHSAS 18001:2007	2341	1085
ISO 27001:2005	314	144
ISO/IEC 20000-1:2005	3	1
UNI EN 9100:2005	280	207
UNI EN ISO 13485:2004	1216	969
UNI EN ISO 14001:2004	14358	8682
UNI EN ISO 3834:2006	229	195
UNI EN ISO 9001:2000	56799	43490
UNI EN ISO 9001:2008	65431	46155

Dati Accredia, Febbraio 2010

Programma

- **Sintesi dei requisiti della direttiva**
- **Norme applicabili**
- **Uso delle norme e certificazione**
- **Sistema di gestione per la sicurezza**

Copertura dei Requisiti

Direttiva 114/2008	ISO/IEC 27001	ISO/PAS 22399	OHSAS 18001
Criteri di settore			
Piani di sicurezza per gli operatori			
1. Identificazione degli asset (elementi)			
2. Analisi dei rischi sulla base degli scenari di minaccia, vulnerabilità e impatti potenziali			
3. Identificazione, selezione e prioritizzazione delle contromisure (permanenti o graduali):			
a) Tecniche			
b) Organizzative			
c) Controllo e verifica			
d) Comunicazione			
e) Consapevolezza e addestramento			
f) Sicurezza dei sistemi informativi			
Funzionari di collegamento			
Valutazione delle minacce			

Risk Management

Unico processo con considerazione dei diversi impatti su:

- Sicurezza delle informazioni (**27001**)
  Focus su Disponibilità, Integrità e Riservatezza degli asset legati alle informazioni
- Disponibilità dei servizi (**22399**)
  Focus su Disponibilità dei servizi erogati e degli asset a loro legati
- Sicurezza delle persone (**18001**)
  Focus su Disponibilità delle persone interne e esterne, legate alle attività dell'organizzazione

Spesso gli asset sono i medesimi e necessitano una considerazione sotto diversi aspetti.

27001 può avere una rilevanza variabile a seconda di quanto l'organizzazione si basa sulle informazioni.

Vision


Salute e Sicurezza sul Lavoro
OHSAS 18001
Sicurezza delle Informazioni
ISO/IEC 27001
ISO 31000
ISO/IEC 15408
Continuità Operativa
ISO 22399

Integrazione dei Sistemi di Gestione

Oltre a integrare il processo di Risk Management, è possibile attuare quello che è definito come **sistema di gestione integrato** considerando i tre schemi e mettendo a fattor comune:

- Pianificazione e gestione delle risorse
- Assegnazione di responsabilità (anche rispetto a cogente)
- Coinvolgimento della Direzione
- Struttura e gestione della documentazione
- Monitoraggio delle performance e dell'efficacia
- Audit interni
- Riesami della Direzione
- Gestione delle azioni correttive e preventive

Benefici nell'uso delle norme

- Nessuna necessità di inventare ex novo, minima necessità di integrazione per il tema specifico
- Efficacia dell'approccio già provata
- Approccio non attaccabile
- Circuiti di certificazione / supporto / valutazione già pronti
- Risparmio di costi per chi già ha intrapreso questa strada (anche solo attraverso una 9001!)
- Maggiori possibilità di interoperabilità intra e infra settore (con particolare riguardo alle interdipendenze)

Contatti

http://www.mediaservice.net

Via San Bernardino 17
10141 Torino, ITALY
Tel. +39 0113272100
Fax. +39 0113246497

mediaservice.net
CORPORATE SECURITY & IMAGE

fabio.guasconi@mediaservice.net