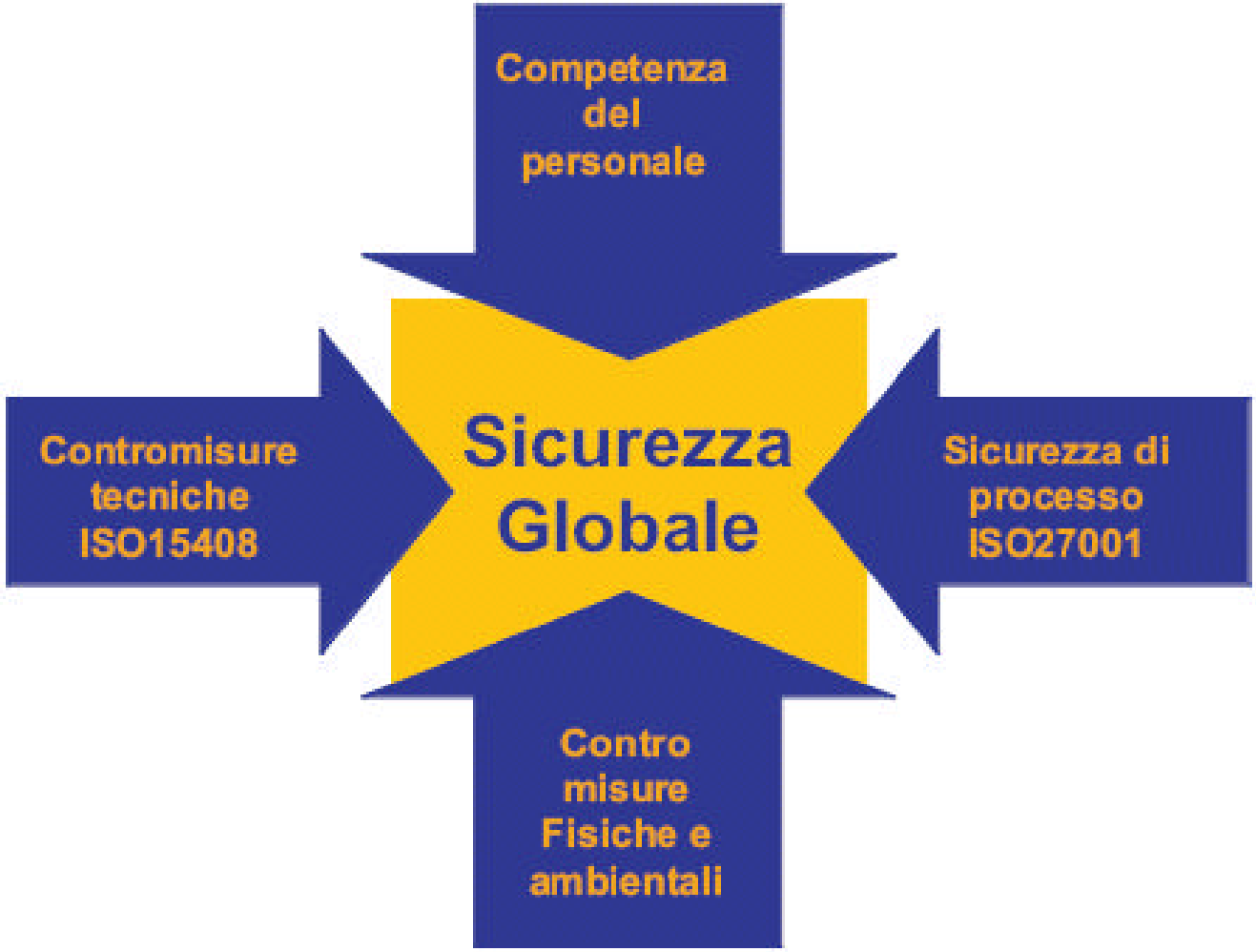
Linea Guida ISCOM
CERTIFICAZIONE DELLA SICUREZZA ICT

Silvano Bari
ALITALIA, AIEA

Scopo della Linea Guida

Affrontare in modo organico
i problemi relativi alla certificazione della sicurezza ICT
fornendo indicazioni concrete sul perché, come e quando
sia opportuno affidarsi a processi formali di certificazione,
evidenziandone i percorsi obbligati e/o consigliati.


Competenza del personale
Contromisure tecniche ISO15408
Sicurezza Globale
Sicurezza di processo ISO27001
Contro misure Fisiche e ambientali

Schema generale della linea guida

Quadro normativo

valore aggiunto

ambiti di applicazione

Schemi di certificazione e di accreditamento

Certificazione di processo

ISO27001

Certificazione di prodotto

ISO15408 (Common Criteria) e ITSEC

Certificazione di competenza del personale

Certificazione di sicurezza fisica

Il contributo AIEA

Oltre al riesame generale,
in particolare:

lo schema di certificazione e di accreditamento di un ISMS secondo la norma ISO27001

le best practices per l'introduzione di un ISMS in una organizzazione

la certificazione del personale

La certificazione delle competenze del personale

n particolare per quanto riguarda il personale di valutazione

dalla seconda metà del 2007
obbligo per i Responsabili dei Gruppi di Audit
del possesso della relativa Certificazione professionale
rilasciata da un Organismo di Certificazione
accreditato o riconosciuto da SINCERT

idoneità delle certificazioni CISA, CISM, CISSP
se accompagnate da un corso di 40 ore sulla norma ISO27001:2005
qualificato da un organismo di certificazione del personale
accreditato o riconosciuto da SINCERT

Le Best Practices AIEA per l'introduzione di un ISMS in azienda

Raccolte dalla esperienza sul campo
dei componenti del Gruppo di Ricerca dell'AIEA sugli ISMS
e contenute nel White Paper
"Information Security Management System.
Un valore aggiunto per le aziende"
pubblicato da AIEA a giugno 2005.

Le Best Practices AIEA - 1

1. **Ottenere il committment del Top Management per l'introduzione dell'ISMS**

2. **Diffondere, al proprio interno e a tutti gli stakeholder, la cultura della sicurezza delle informazioni e l'importanza degli ISMS**

3. **Calcolare il valore degli Information Assets**

4. **Nel condurre l'analisi dei rischi valutare sempre la gravità del danno potenziale in termini di impatto economico**

5. **Tenere conto degli impatti legati ad eventuali esternalizzazioni di attività o ad attività di 'merging/acquisition'.**

6. **Valutare i benefici legati all'introduzione degli ISMS**

Le Best Practices AIEA - 2

7. **Disegnare ed implementare gli ISMS partendo dalle esigenze e dalle caratteristiche delle attività e del business**

8. **Cercare di recepire in maniera organica tutti i vincoli di legge e normativi rilevanti per la sicurezza delle informazioni**

9. **La sicurezza si basa, in larga parte, sulle persone. Tenere conto della rilevanza del fattore umano nel disegno del sistema di gestione della sicurez**

10. **Reperire nell'ambito della cultura e dell'esperienza dell'Auditing gli schemi di riferimento per il coordinamento ed il controllo dei sistemi di gestione della sicurezza**

11. **Nell'implementazione degli ISMS procedere per gradi. Partire dagli asset più critici e poi estendere progressivamente il sistema di gestione agli altri asset**

Le Best Practices AIEA - 3

12. **Partire con l'obiettivo di mettere in campo un sistema di gestione della sicurezza e una volta realizzato, valutare l'opportunità di certificarlo**

13. **Nell'implementazione degli ISMS, curare con attenzione la descrizione dei processi e delle procedure di sicurezza**

14. **Nell'analisi dei rischi tenere conto non solo delle minacce correnti ma effettuare anche delle analisi prospettiche individuando i rischi legati a nuov tipologie di minacce.**

15. **L'implementazione degli ISMS richiede attenzione nelle relazioni interne e nei processi di comunicazione**

16. **Cogliere l'occasione di significativi progetti di change management** *(es: revisione di applicazioni strategiche, adeguamento delle infrastrutture tecnologiche)* **per partire con l'avvio o l'ampliamento di un ISMS**