AEO e sicurezza dei sistemi informativi

Luca Boselli, Senior Manager, KPMG Advisory S.p.A.

Milano, 26 giugno 2008

Agenda

- **La sicurezza delle informazioni: introduzione e scenario di riferimento**
- **La sicurezza delle informazioni in ambito AEO**
- **Approccio metodologico per la valutazione e la gestione dei rischi di sicurezza**

La sicurezza delle informazioni

Che cos'è la "Sicurezza delle informazioni" ?

- E' installare un *firewall* per la protezione della rete……
- E' gestire i sistemi attraverso l'uso di *user-ID* e *password*……
- E' cifrare i dati per renderli illeggibili alle persone non autorizzate…..
- E' un costo che non produce benefici per l'azienda……

La sicurezza delle informazioni

L'informazione come *asset* da proteggere:

- "***Information*** *is an* ***asset*** *which, like other important business assets, has value to an organization and consequently needs to be suitably protected*."

- "*Whatever* ***form*** *the information takes, or means by which it is shared or stored, it should always be* ***appropriately protected***."

(ISO 17799:2005)

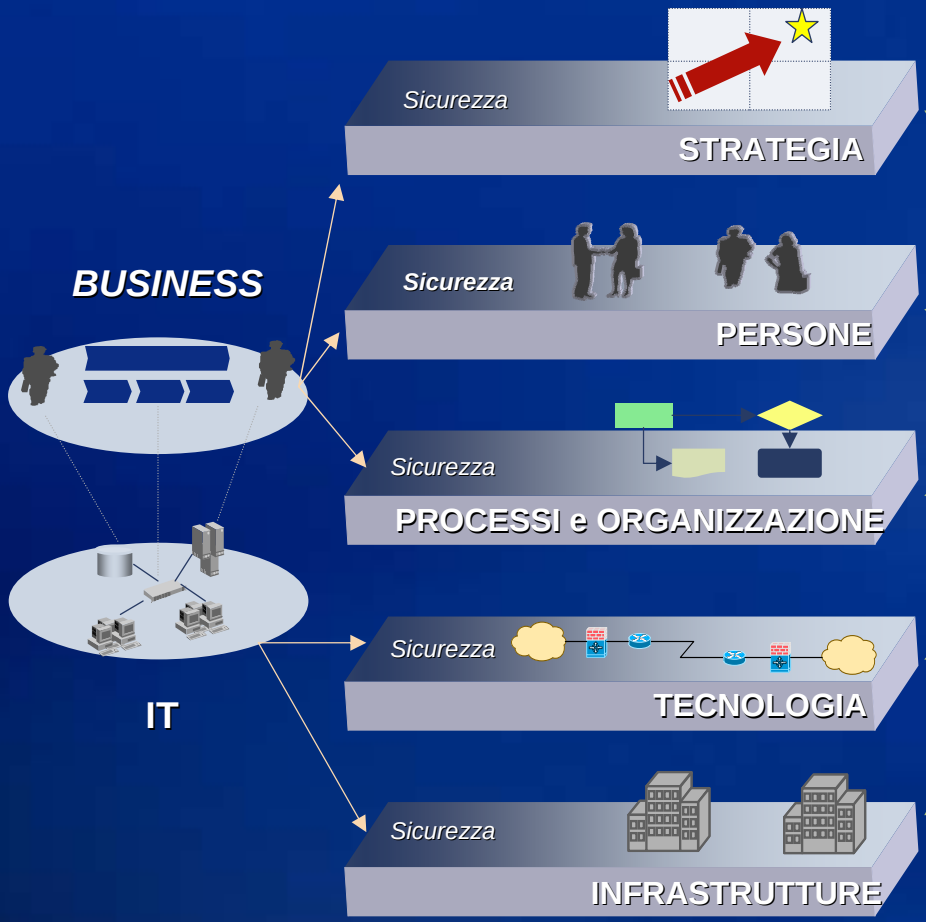
La sicurezza delle informazioni

- La ***Sicurezza delle informazioni*** consiste nella salvaguardia e protezione di tre caratteristiche fondamentali delle informazioni stesse:

- Altre qualità rilevanti delle informazioni sono: **l'autenticità e la non-ripudiabilità, la proprietà e la responsabilità, l'affidabilità**

La sicurezza delle informazioni

Una visione integrata della sicurezza:



- La sicurezza delle informazioni è strettamente connessa a tutti gli aspetti legati:
  - al *business*
  - all'infrastruttura tecnologica

Supply chain e sicurezza delle informazioni

Evoluzione scenario rischi

- Rapida evoluzione **minacce** (terrorismo, contraffazione, frodi telematiche, ecc.)
- Riduzione del ***time to market*** per nuovi prodotti o servizi
- Necessità di **aggiornamento continuo** rispetto a tematiche organizzative, culturali, tecnologiche, legislative, ecc.

Crescente domanda di sicurezza dal *business*

- **Incidenti di sicurezza** con forte risonanza mediatica
- Maggior **consapevolezza** dei clienti rispetto alla sicurezza
- **Vincoli** di tipo normativo/regolamentare
- *Smart sourcing*

Evoluzione ICT

- **Processi di business sempre più estesi** verso soggetti terzi (clienti, fornitori, ecc.)
- Aumento **dell'importanza dell'ICT** nella gestione delle *supply chain*
- Crescita della dipendenza e della **pervasività di network insicuri** (Internet) nei processi aziendali
- Nuove tecnologie (*wireless, PDAs*, ecc.)
- Crescita dell'***outsourcing*** **IT** (*data centres*, *WANs, LANs*, gestione *desktop*, ecc.)

Obiettivi aziendali

- Maggior **controllo dei costi**
- **Ritorno degli investimenti** in *Information Security*
- Necessità di **razionalizzare** gli investimenti

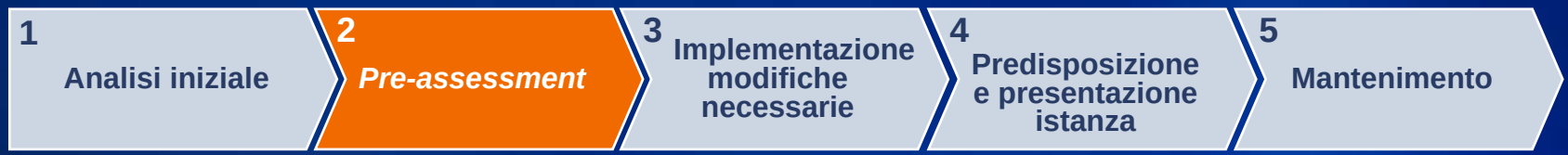
Agenda

- La sicurezza delle informazioni: introduzione e scenario di riferimento
- **La sicurezza delle informazioni in ambito AEO**
- Approccio metodologico per la valutazione e la gestione dei rischi di sicurezza

La sicurezza delle informazioni in ambito AEO

Requisiti di sicurezza e attività per gli AEO:

- Adozione di adeguate misure di sicurezza per tutelare sistema informatico
- Identificazione e valutazione rischi di sicurezza legati all'utilizzo dei sistemi IT a supporto dei processi della *Supply chain*
- Adozione approccio strutturato per identificazione e valutazione dei rischi
- Identificazione e valutazione delle misure di sicurezza e dei rischi anche relativamente ai rapporti con terze parti (*outsourcing*)

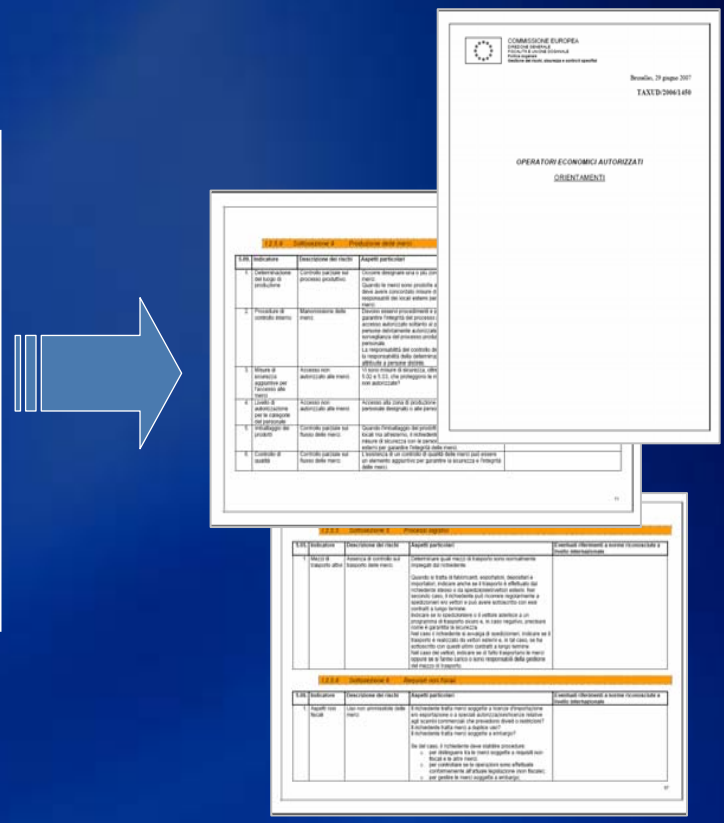


La sicurezza delle informazioni in ambito AEO

Aree di sicurezza:

- Gli aspetti di sicurezza delle informazioni che le linee guida UE richiedono di prendere in considerazione ai fini AEO possono essere ricondotte alle seguenti aree:

- **Gestione del controllo degli accessi**
- ***Business continuity/Backup and recovery management***
- **Gestione della sicurezza logica perimetrale dei sistemi**
- **Gestione della sicurezza fisica degli *asset* IT**
- **Tracciabilità delle attività effettuate sui sistemi IT**
- **Requisiti di sicurezza per terze parti**



La sicurezza delle informazioni in ambito AEO

Lo standard ISO27001:

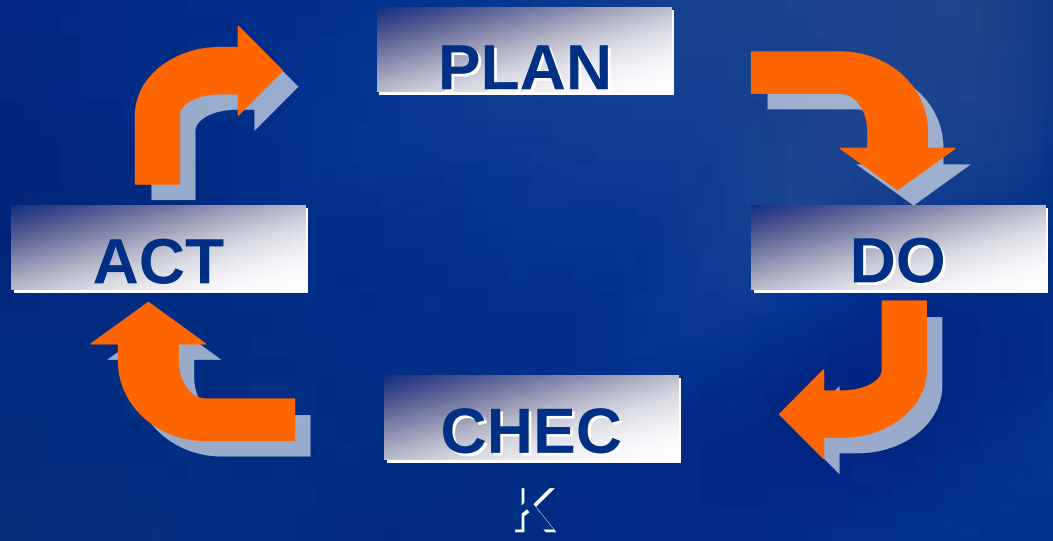
- Le linee guida per la sicurezza dei sistemi informativi in ambito AEO fanno esplicito riferimento alle indicazioni contenute nello **standard ISO 27001** (*Information security management systems – Requirements*)
- Tale standard è comunemente adottato a livello internazionale per l'implementazione di **sistemi di gestione della sicurezza delle informazioni** e la loro eventuale certificazione, e fornisce indicazioni in merito alle seguenti aree:
  - ***Security Policy***
  - ***Organization of information security***
  - ***Asset management***
  - ***Human resources security***
  - ***Physical and environmental security***
  - ***Communications and operations management***
  - ***Access Control***
  - ***Information systems acquisition, development and maintenance***
  - ***Information security incident management***
  - ***Business Continuity management***
  - ***Compliance***

Aree di maggior sovrapposizione tra i requisiti richiesti dall'AEO e quelli indicati dallo standard ISO 27001

La sicurezza delle informazioni in ambito AEO

Lo standard ISO27001:

- Lo standard introduce inoltre si caratterizza per una serie di aspetti rilevanti:
  - Modello PDCA (*Plan-Do-Check-Act*)
  - Ciclo di miglioramento continuo
  - Stessi principi dell'**ISO 9001 (Sistemi di gestione della Qualità)**



Agenda

- La sicurezza delle informazioni: introduzione e scenario di riferimento
- La sicurezza delle informazioni in ambito AEO
- **Approccio metodologico per la valutazione e la gestione dei rischi di sicurezza**

Approccio metodologico per la valutazione e la gestione dei rischi di sicurezza

Il concetto di rischio di sicurezza

"Rischio" → **probabilità** che si verifichi un **evento**, in relazione all'entrata, all'uscita, al transito e all'uso finale di merci trasportate tra il territorio doganale della Comunità e paesi terzi e la presenza di merci non aventi una posizione comunitaria che:

- impedisce l'applicazione corretta di misure comunitarie o nazionali
- compromette gli interessi finanziari della Comunità e dei suoi Stati membri
- costituisce una minaccia per la sicurezza della Comunità, la salute pubblica, l'ambiente o i consumatori

Modello Compact AEO

Tale definizione di rischio specifica in ambito AEO può essere declinata nel contesto della **sicurezza delle informazioni**:

Rischio di sicurezza: è la possibilità che una determinata **minaccia** sfrutti una **vulnerabilità** per provocare **perdite** o **danni** ad un **bene** o ad un insieme di beni costituiti da **informazioni**

Approccio metodologico per la valutazione e la gestione dei rischi di sicurezza

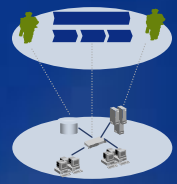
Esempi di rischi di sicurezza e controlli in ambito AEO

RISCHI	CONTROLLI
Accesso non autorizzato e/o intrusione nei sistemi informatici dell'operatore economico	• Quali misure esistono (ad esempio, *firewall, password* periodicamente modificate) per proteggere i sistemi informatici degli operatori economici da intrusioni non autorizzate? • Sono state effettuate prove d'intrusione? In caso negativo, il richiedente deve effettuare tali prove per dimostrare la sicurezza del sistema.
Distruzione intenzionale o perdita di informazioni pertinenti	
Uso improprio del sistema informatico dell'operatore economico per compromettere la catena di approvvigionamento	• Quali categorie di personale hanno accesso a informazioni dettagliate sui flussi di merci e sui flussi di dati? • Quali categorie di personale sono autorizzate a modificare tali informazioni?
Utilizzo di un sistema di gestione complesso che consente di nascondere transazioni illegali	• Qual è il livello di separazione delle funzioni (sviluppo, prova e funzionamento) all'interno del servizio informatico?

Approccio metodologico per la valutazione e la gestione dei rischi di sicurezza

Il processo di analisi e gestione dei rischi:

Identificazione ed analisi sistemi informativi a supporto della *supply chain*



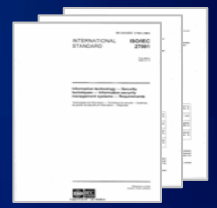
PROCESSI DI BUSINESS

SISTEMI ICT

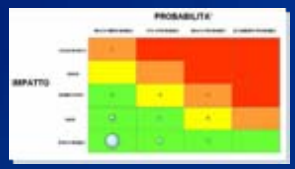
Identificazione dei rischi IT applicabili nell'ambito della *supply chain*

Analisi dei controlli di sicurezza adottati dalla società sui sistemi IT identificati

AEO Guidelines EU



Controlli ISO27001



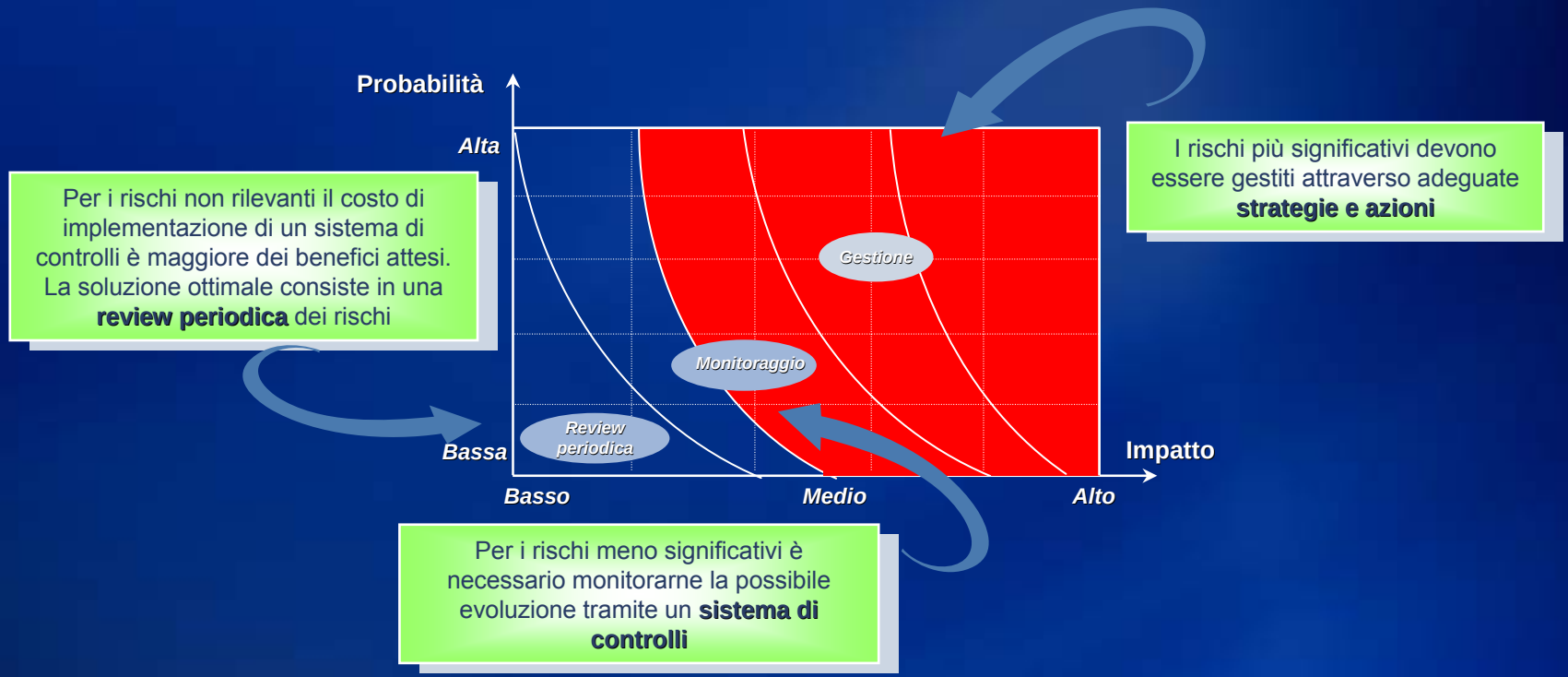
Valutazione dei livelli di rischio

Determinazione delle azioni di gestione dei livelli di rischio

Approccio metodologico per la valutazione e la gestione dei rischi di sicurezza

Analisi e valutazione dei rischi:

in questa fase è indispensabile adottare un **approccio strutturato** per l'identificazione e la valutazione dei rischi, classificandoli per priorità in funzione del loro impatto e della probabilità che si verifichino.



Approccio metodologico per la valutazione e la gestione dei rischi di sicurezza

Strategie di gestione dei rischi:

- Adozione di contromisure di reazione, contrasto, monitoraggio (ad esempio: riducendo le minacce, riducendo le vulnerabilità, riducendo i possibili impatti)

- Minimizzare o eliminare la probabilità di accadimento di un evento dannoso rimuovendo totalmente il rischio o prevenendo la minaccia (ad esempio: non elaborando un certo tipo di informazioni, impedendo connessioni a rete pubbliche, selezionando siti che evitino problemi di disastri naturali)

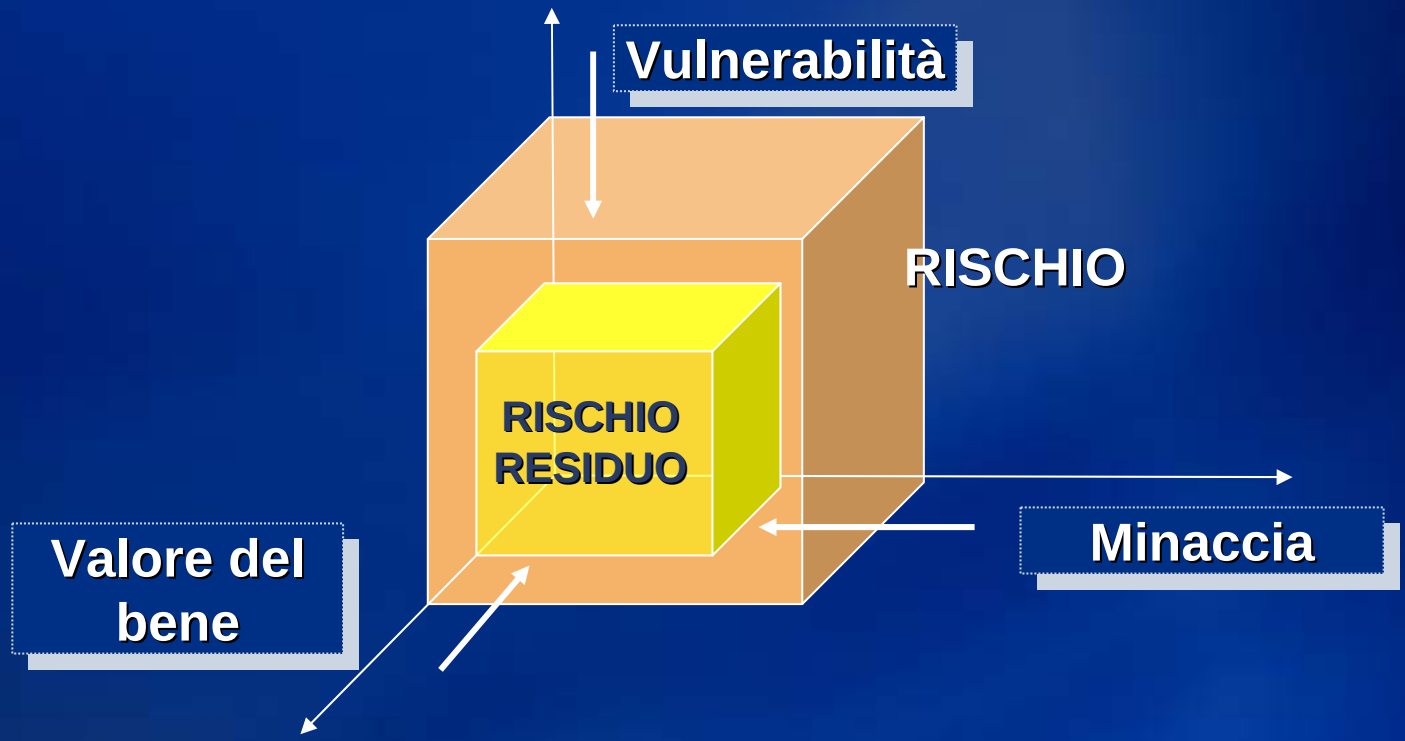
- Rischi con basso impatto e bassa probabilità di accadimento
- Costi delle contromisure talmente elevati da non poter essere sostenuti in ogni caso

- Trasferire completamente ad un altro soggetto o condividere con esso gli impatti derivanti da un evento dannoso (ad esempio: stipulando contratti assicurativi, utilizzando terze parti o *outsourcer*, ecc.)

Approccio metodologico per la valutazione e la gestione dei rischi di sicurezza

Il rischio residuo:

Il rischio residuo, ovvero che permane dopo l'adozione delle azioni correttive, esiste sempre poiché è impossibile rendere sicuro in modo assoluto un sistema informativo



Approccio metodologico per la valutazione e la gestione dei rischi di sicurezza

Dall'analisi dei **progetti pilota** realizzati dall'Agenzia delle Dogane sono emerse alcune indicazioni rilevanti:

Fasi procedurali richieste per l'attribuzione dello status AEO

- Necessità di definire un **approccio *risk-based***
- Analisi delle misure di mitigazione e/o prevenzione dei rischi
- **Governo e monitoraggio dei rischi residui**

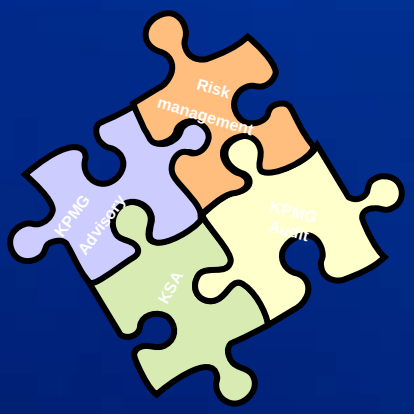
Elementi critici evidenziati

- Previsione di specifici **accordi contrattuali** per il riconoscimento di partner affidabili
- Miglioramento degli aspetti di **sicurezza degli accessi**

Documentazione/elementi presi in considerazione in materia di sicurezza

- Sistemi di gestione certificati (**ISO9001 / ISO27001**) e relativa documentazione (manuali e procedure)
- Documentazione di sicurezza (piani di sicurezza / **DPS**/ **piano di *Business Continuity*** o di *Disaster Recovery*)

Approccio metodologico per la valutazione e la gestione dei rischi di sicurezza



Alcuni benefici dell'approccio KPMG:

- Conformità all'approccio richiesto dall'UE
- Approccio multidisciplinare in grado di fornire una vista integrata dei rischi
- Allineamento dell'approccio metodologico con i principali modelli e standard di sicurezza informatica maggiormente diffusi
- Disponibilità di competenze specifiche nell'ambito della sicurezza dei sistemi informativi
- Identificazioni di possibili aree di miglioramento in ambito IT