Schema *SCS*

“Supply Chain Security Management System”

Norma ISO 28000_2007

Schema *SCS*

“Supply Chain Security Management System”

Norma ISO 28000_2007

In rosso i Paesi aderenti all'OECD; in blu i richiedenti l'ingresso nell'organizzazione

In verde i Paesi che stanno sviluppando politiche doganali e di tutela dei traffici coerenti +/- con politiche OCSE

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

Schema *SCS*

“Supply Chain Security Management System”

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

OECD

Norma ISO 28000_2007

International Organization for Standardization

Word Custom Organization

WCO

OMD

ACCREDIA

L'ENTE ITALIANO DI ACCREDITAMENTO

Tra gli obiettivi della WCO vi è la Security nella gestione delle catene di fornitura e, di conseguenza, nei commercio e nei trasporti tra i diversi Paesi.

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

WORLD CUSTOMS ORGANIZATION

Guidelines for developing a mutual recognition arrangement/agreement

TAPA
Transported Asset Protection Association

Beating cargo crime

WORLD CUSTOMS ORGANIZATION

WCO SAFE
Framework of Standards

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

Aree di rischio
nelle quali
le Organizzazioni
“Authorized Economic Operator”
AEO, possono decidere o
possono essere sollecitate a
sviluppare delle misure di
Trade Security, coinvolgendo
i diversi partner logistici
e commerciali...

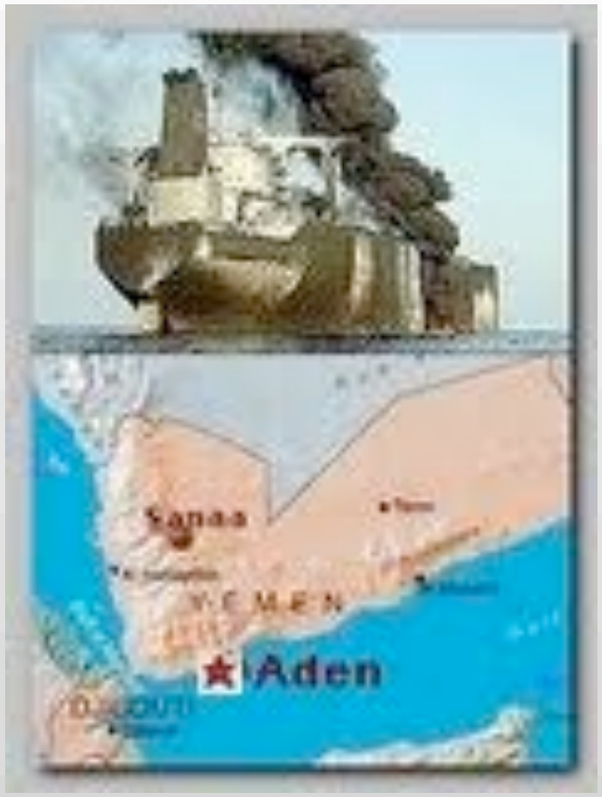
Responsibilities

- UNODC-WCO Container Control Programme
- Global Supply Chain Security
- Commercial Fraud
- Tobacco and Cigarette Smuggling
- Intellectual Property Rights (IPR)
- Customs Intelligence
- Drugs and Chemical Precursors
- Money Laundering
- Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES)
- Environmental Crime
- Electronic Crime
- Firearms
- Bio terrorism
- Nuclear and other radioactive materials
- Stolen Cultural Heritage
- Avian influenza epidemic

Un’immagine simbolo degli attuali scenari di rischio per i traffici

2002 10 06 - Limburg 157.000t - 2 morti (almeno1 terrorista), 4 feriti - primo attacco al-Qaeda a traffici petrolio/chimici

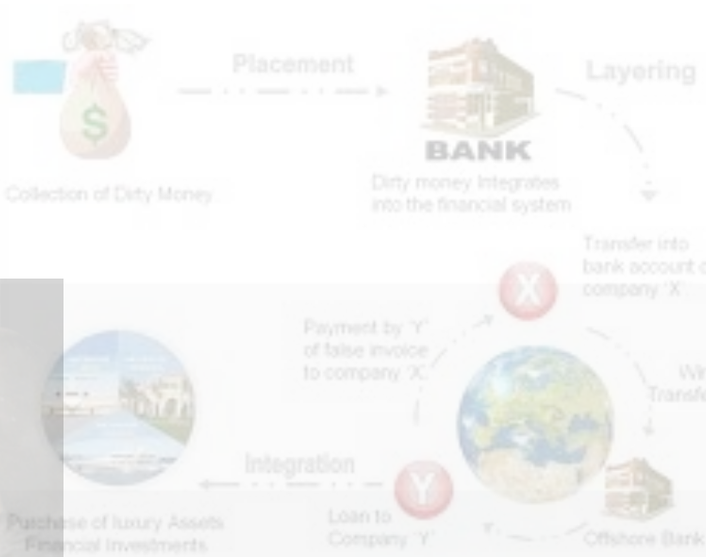
Un’immagine simbolo degli attuali scenari di rischio per i traffici



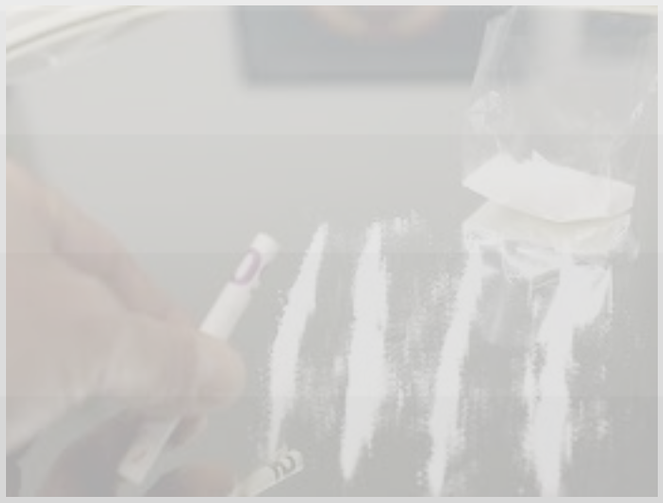
Limburg

Il riciclaggio del denaro; la contraffazione dei marchi e prodotti protetti; il commercio di droghe, di specie vegetali ed animali protette; i crimini informatici; i crimini ambientali; il traffico di armi; il terrorismo... sono alcune aree critiche per gli AEO.

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO



Molte di queste “aree di rischio” hanno anche una connessione, non casuale, con il D. Lgs. 231/01 (e 231/2007)



ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

Security: un termine poco usato, ma che sempre più sarà al centro dell'attenzione tra gli addetti ai trasporti.

Le spinte alla integrazione di modalità "sicure" nella gestione dei traffici internazionali di "beni a rischio" e della protezione di "obiettivi sensibili" sono molteplici.

Gli stati sono chiamati a fornire un supporto talora molto costoso, che non potrà gravare per sempre sulle spalle dei contribuenti, ma che deve essere gestito dagli interessati...

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

Security: significa anche un qualcosa in più, rispetto a quanto abbiamo appena osservato.

Le industrie che operano su mercati critici (per la criticità del prodotto o della logistica) debbono aver ben chiari i fattori di rischio per la Supply Chain da governare, per raggiungere i propri obiettivi di business...

In definitiva, si parla di una delle aree del ***Risk Management***.

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

Da una stima approssimativa [fonte Portale Trasporti www.aziendeditrsporto.it], in Italia possono essere mappati almeno:

- 1210 Operatori Logistici
- 1095 Soc. di trasporto e spedizioni
- 59 Operatori di trasporto marittimo
- 82 Operatori di trasporto aereo
- oltre 2000 operatori di trasporto terrestre
- oltre 1200 operatori di trasporto internazionale
- diverse migliaia di operatori di supporto...
- diverse centinaia di operatori portuali ed aeroportuali, a cominciare dalla Soc. di manutenzioni, per arrivare alle Soc. di catering e Ship Chandling fino ai vettori.

La Norma ISO 28000_2007 non indirizza specifiche modalità di contrasto dei rischi legati al terrore, alla droga, al traffico d'armi o al riciclaggio o specifiche modalità di gestione della Security della propria catena logistica.

La Norma fa riferimento alla gestione dei rischi per la

"Security" logistica, adottando il modello del ciclo di Deming:

4 Security management system elements

Figure 2 — Security management system elements

ACCREDIA L'ENTE ITALIANO DI ACCREDITAMENTO

La Norma ISO 28000_2007 fa esplicito riferimento al rispetto delle leggi cogenti applicabili, ma anche ai “framework” di normative esistenti per la gestione dei terminal portuali e delle comunicazioni tra vettori marittimi e terminal/hub:

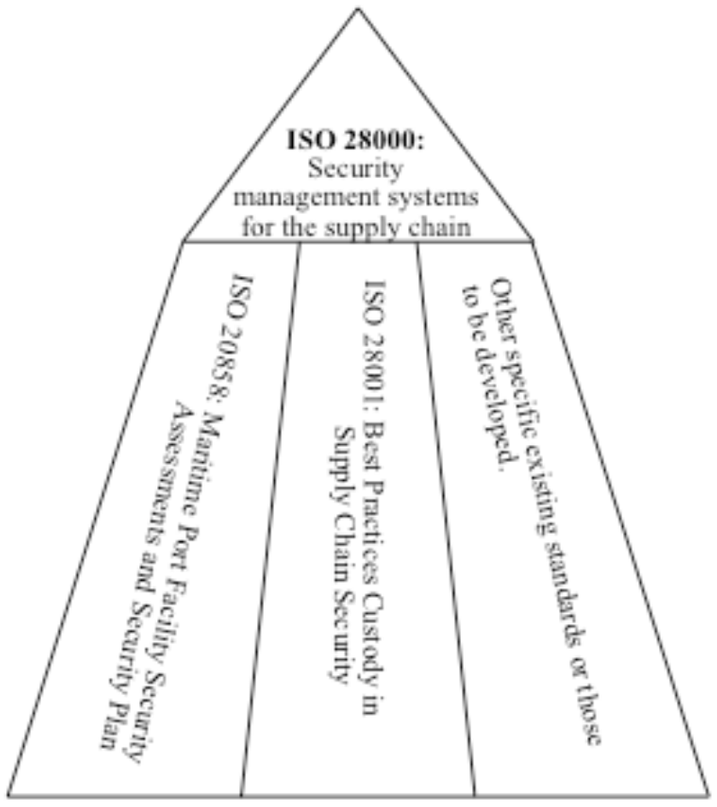


Figure 1 — Relationship between ISO 28000 and other relevant standards

La Norma ISO 28000_2007 fa esplicito riferimento al rispetto delle leggi cogenti applicabili, ma anche al “framework” di normative esistenti per la gestione dei terminal portuali e delle comunicazioni tra vettori marittimi e terminal/hub:

Tale approccio si applica a tutti i mezzi e gli scali merci e passeggeri: marittimi, stradali, ferroviari ed aeroportuali, così come agli operatori.

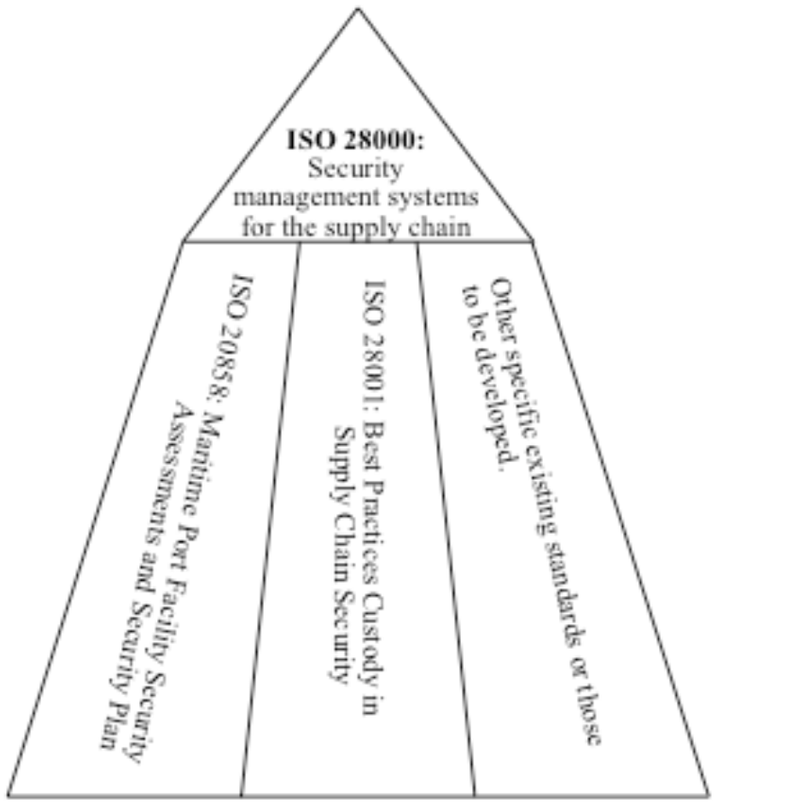


Figure 1 — Relationship between ISO 28000 and other relevant standards

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

La Norma ISO 28000_2007 è corredata da Norme ancillari:

ISO 28001 [Best practices for implementing... (sviluppata da un comitato con interessi >> nel settore marittimo)]

ISO 28002 [Developing of Resilience in Supply Chain]

ISO 28003 [Requirements for CABs (17021_2006...)]

ISO 28004 [Guideline for implementing... (generica)]

ISO 28005 [Electronic Port Clearence EPC]

ISO 20858 [Maritime port facility security assessments and security plan development]

La Norma ISO 28000_2007 sembra di banale applicazione, dato che alla lettura appare "vuota" come, per i poco avveduti, potrebbe sembrarlo la Norma "ISO 9001".

La Norma è generica volutamente. A dare valore ai suoi requisiti sono le "best practices" aziendali, ma prima ancora il rispetto delle leggi applicabili, nazionali e soprattutto quelle internazionali, come l'emendamento alla SOLAS [**International Convention for the Safety of Life (and environment) at Sea (SOLAS), 1974**], chiamato ISPS [International Ship and Port Security - **Regulation No 725/2004 of the EU Parliament and of the Council of 31 March 2004**]

Evidentemente, nessun Sistema di Gestione per la Security della “Supply Chain” potrà essere adottato senza dar di conto di come sia applicata la normativa cogente. Ciò, a maggior ragione, con riferimento ai requisiti di cui ai §§ 9.1.2.2.2 e 9.1.10.i della Norma ISO/IEC 17021_2011, pur se gli Audit in parola non dovranno essere intesi come audit di conformità legislativa (vedi il citato § 9.1.2.2.2 nella specifica Nota).

Appare altrettanto evidente che la Norma ISO 28000_2007 non possa essere considerata come risposta esclusiva per il rischio “terrore”, anche se i lavori ISO hanno avuto impulso e l’avvio dopo l’attentato alle Torri Gemelle del Settembre 2001. Parimenti, anche le modifiche alla normativa SOLAS (ISPS Code) sono state sviluppate dopo lo stesso attentato.

La Norma indirizza l’esigenza, per ogni organizzazione, di effettuare una analisi dei rischi che impattano la catena di fornitura, tenendo conto delle proprie specificità: quindi è una Norma che indirizza l’adozione di una cultura basata sul Risk Management, che sarà tanto più applicata, quanto più sarà giustificata in termini di “business” (o dalla Legge!).

I rischi che indirizza la Security sono quelli ove il valore creato dall'attività economica può essere diminuito o annullato (creando danni di alta magnitudo) da un evento indesiderato, che si manifesta con modalità inattese e/o tempi ed intensità indesiderate; voluto o meno.
In questo caso, si tratta anche dei rischi che impattano sulla società civile..., questo spiega l'interessamento delle Autorità!

Ciò presuppone un’analisi di rischi correlati con i processi operativi della propria catena di fornitura (Risk Assessment), che dovrà portare allo sviluppo di opportuni controlli operativi [misure organizzative e tecniche per mitigare gli stessi rischi].

La Certificazione del sistema di gestione aziendale preposta ai rischi per la Security della Supply Chain, rappresenta, per alcuni vettori un elemento contrattuale critico per il mantenimento dei traffici merci e passeggeri, nonché di aiuto per il rispetto delle leggi applicabili.

Quindi?
Come intende muoversi **ACCREDIA**?

La Norma da adottare per l'Accreditamento, come abbiamo visto, è la ISO 28003... "*mutatis mutandis*", per renderla coerente con la versione 2011 della corrispondente Norma ISO/IEC 17021.

Sarà necessario, tra le altre valutazioni, che gli OdC adottino dei criteri robusti per la selezione delle Risorse Umane che possano risultare "affidabili" per tale schema..., per altro come è richiesto dalla stessa Norma 28003.

Dall’analisi appena condotta risulta palese che il tema della Security viene sentito con particolare forza in un settore, quello dei trasporti, che già soffre pesantemente dello attuale stato congiunturale.

Il nostro obiettivo è realizzare opportunità per la creazione di valore e non per affaticare il tessuto industriale.

Dall’analisi appena condotta si evince anche che il Sistema di Gestione per la Security coinvolge quelle aree di rischio che, normalmente, sono presidiate o possono essere presidiate con una logica di Risk Management tipica di tutti i Sistemi di Gestione basati sul modello ISO 14001. Cioè, basate proprio sulla logica di gestione dei rischi.

Proprio per questo motivo, la tabella di calcolo del tempo di audit prevede un fattore di riduzione per i sistemi integrati, a partire da un certo livello di numerosità dei dipendenti.

Nei casi ove la tabella in annesso A della ISO 28003 prevede la durata di audit di “1” giorno (organizzazioni sino a 9 dipendenti), non si accetteranno riduzioni del tempo di audit di alcun tipo.

Le attività di Stage 1 e Stage 2 debbono essere svolte presso il “sito” del Cliente. Fa eccezione la sola analisi documentale, che potrà essere estesa **solamente** ai documenti di sistema non classificati e/o classificabili come “riservati”. In quest’ottica, ACCREDIA valuterà la congruità dei comportamenti degli OdC in occasione delle verifiche in accompagnamento o in sede. Il mancato rispetto di questo requisito di prudenza comporterà la registrazione di una specifica Non Conformità a carico dell’OdC.

Appare evidente la forte sinergia che è attesa nello sviluppo dei Sistemi di Gestione per la Security delle catene di fornitura ove venga integrato lo sviluppo dei Sistemi di Gestione della Sicurezza delle Informazioni (ISO/IEC 27001) **e/o** di Gestione della Continuità Operativa (ISO 22301).

Per stimolare la buona pratica della adozione congiunta e sinergica di tali Norme - **ove il campo di applicazione a livello logico, organizzativo e fisico possa essere considerato coerente** - in tali casi sarà considerata accettabile la predisposizione di offerte che prevedano l'applicazione del requisito di allocazione del tempo di Audit del 20% off-site, anche per la Norma ISO/IEC 27001, e l'applicazione della riduzione del 20% prevista dalla Norma ISO 28000 (ove applicabile).

Attenzione anche nel caso della Norma ISO/IEC 27001, le attività di valutazione documentale svolte “off-site” dovranno essere limitate alla documentazione di sistema che non possa essere considerata “riservata”, quindi non al Documento di Valutazione dei Rischi, ma alla sola Procedura; non al SoA, non ad alcun documento aziendale che possa creare potenzialmente delle fughe di notizie riservate e/o critiche per la sicurezza del Cliente.

Grazie per l'attenzione,

se avete domande...

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO