

# Sicherheitsstandards in der Lieferkette – Einführung und Zertifizierung –

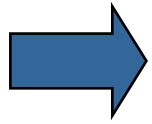
Wilhelm Loskot – Germanischer Lloyd Certification GmbH

2008-01-31



**Germanischer Lloyd**

# Inhalt



## Ein Szenario

- Ganzheitliche Sicherheitskonzepte
- AEO und andere Sicherheitsinitiativen
- Anforderungen der ISO 28000
- Die ISO 28000 Zertifizierung
- GLC Hilfsmittel

# Ein Szenario – Spedition mit 18 Fahrz



- Madrid, Spanien
- Region Flughafen
- Innerhalb der letzten 6 Monate
  - wiederholte Diebstähle aus LKWs
  - wiederholte Überfälle auf LKWs
  - Weitere Überfälle absehbar
  - Verlust wertvoller Ladung

# Sicherheitsmaßnahmen?

- E-Seal, elektronischer Alarm
- GPS
- „High“
- „Imm“
- Panic Button
- Traileralarm
- Eskorte

**KOSTEN!**

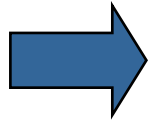


- Sind diese vorbeugenden Maßnahmen kosteneffizient und ausreichend zur Sicherung



# Inhalt

- Ein Szenario

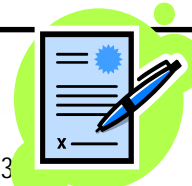
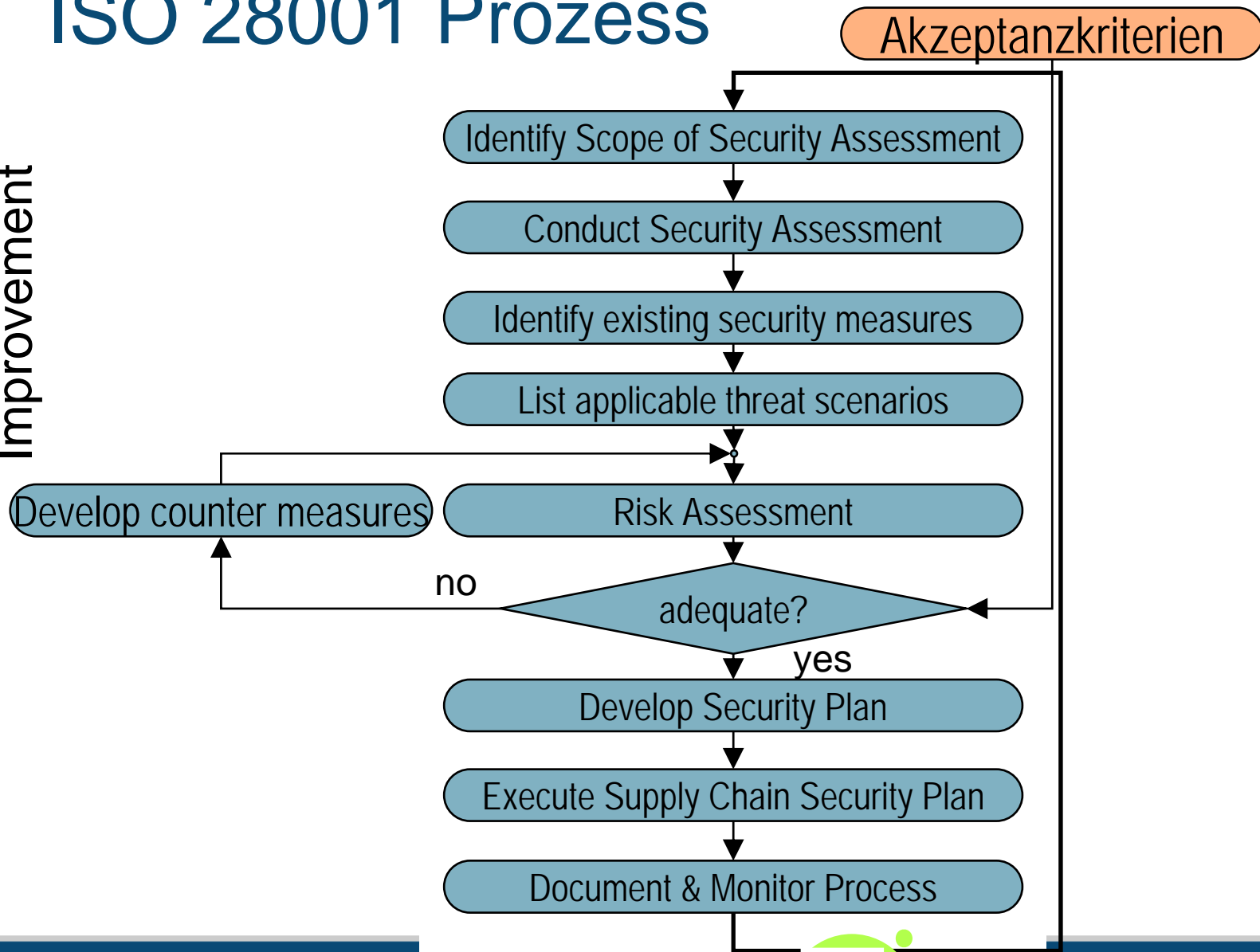


## Ganzheitliche Sicherheitskonzepte

- AEO und andere Sicherheitsinitiativen
- Anforderungen der ISO 28000
- Die ISO 28000 Zertifizierung
- GLC Hilfsmittel

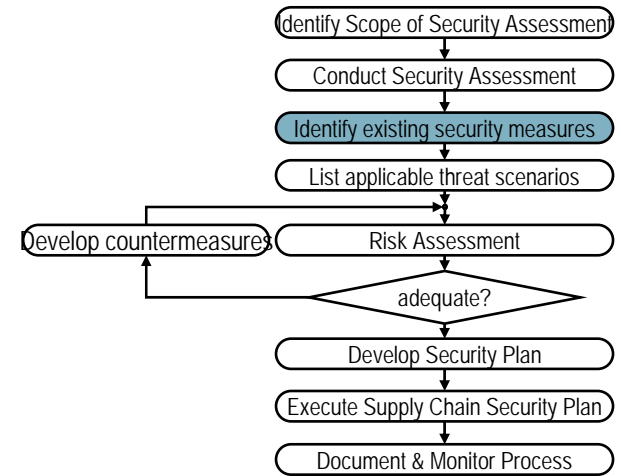
# ISO 28001 Prozess

Continual  
Improvement



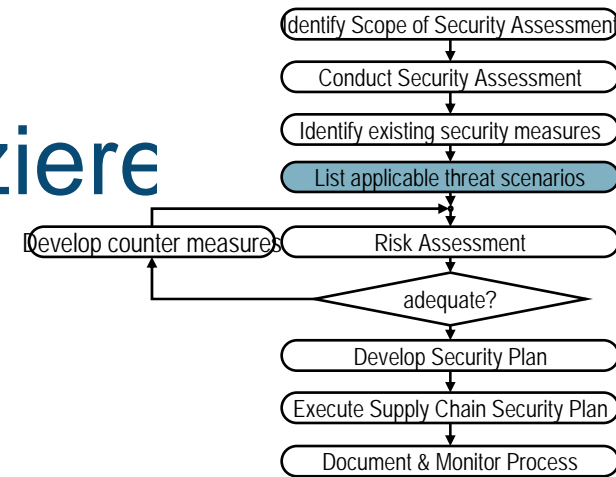
# Bestehende Sicherheitsmaßnahmen

- Anweisungen
- Diebstahlssicherung
- Zugangskontrollen
- Sendungsnachverfolgung
- TAPA FSR
- TAPA TSR
- Bewusstsein und Kenntnisstand der Mitarbeiter...



# Gefahrenszenarien identifiziere

Form: Meeting der Arbeitsgruppe

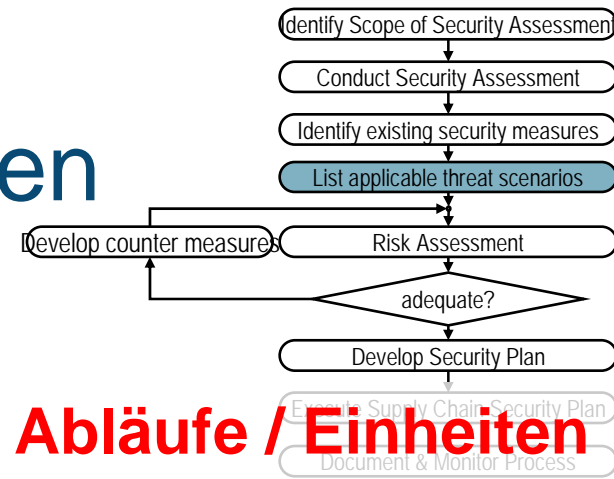


was passieren könnte ist, dass .....



vor Jahren hatten wir den Fall, dass .....

# Gefahrenszenarien identifizieren



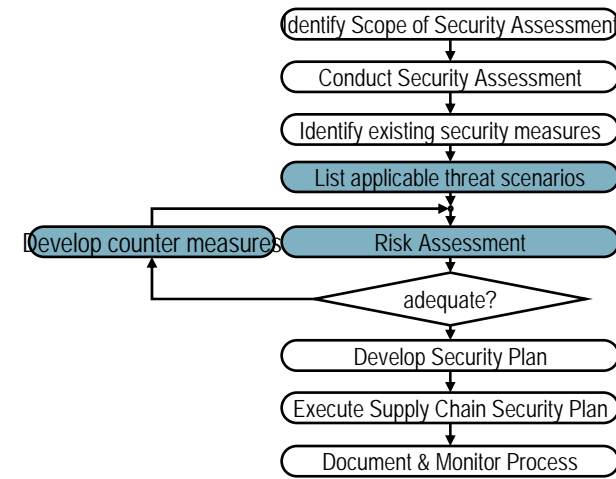
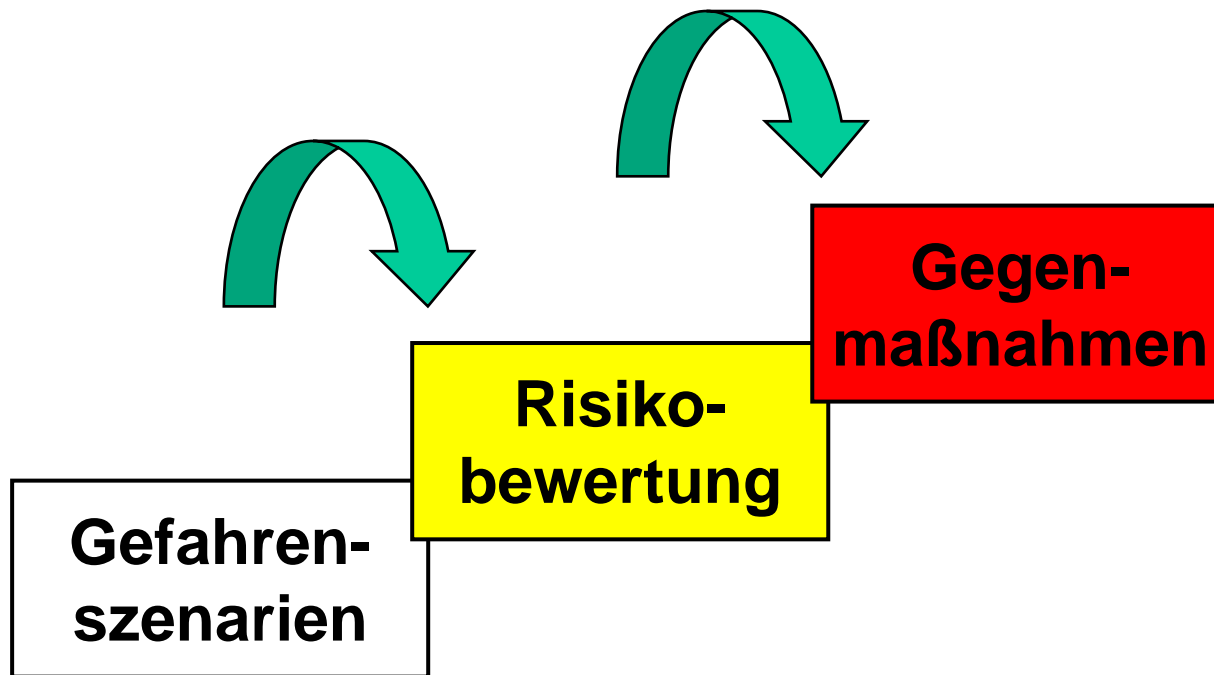
## Kategorien

- Beschädigung/ Zerstörung
- kriminelle/ terrorist. Handlungen
- betriebl. Störung / Unterbrechungen
- Umwelteinflüsse
- IT-Manipulationen
- Zulieferer

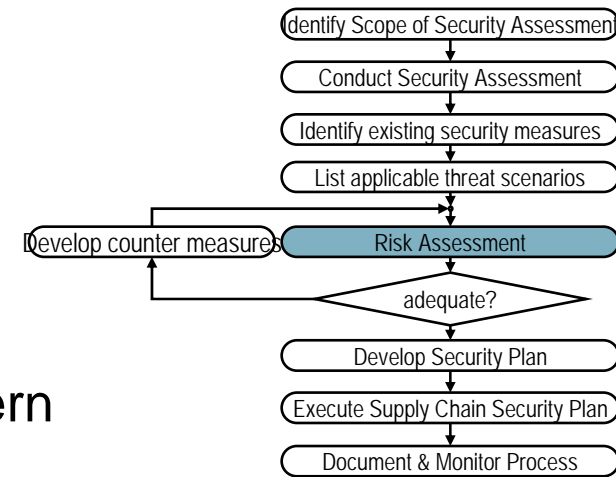
## betroffene Abläufe / Einheiten

- Gesellschaft
- Zulieferer
- Betriebsabläufe
- Anlagen/ Betriebsteile
- Wirtschaftsinteressen
- Inhaber/ Anteilseigner
- Wirtschaftsgebaren

# Risikoanalyse



# Risikoanalyse



Beispiel: Einbruch und Diebstahl von Fernsehern

**Risiko = Eintrittswahrscheinlichkeit \* Konsequenz**



wie wahrscheinlich  
kommt das vor?

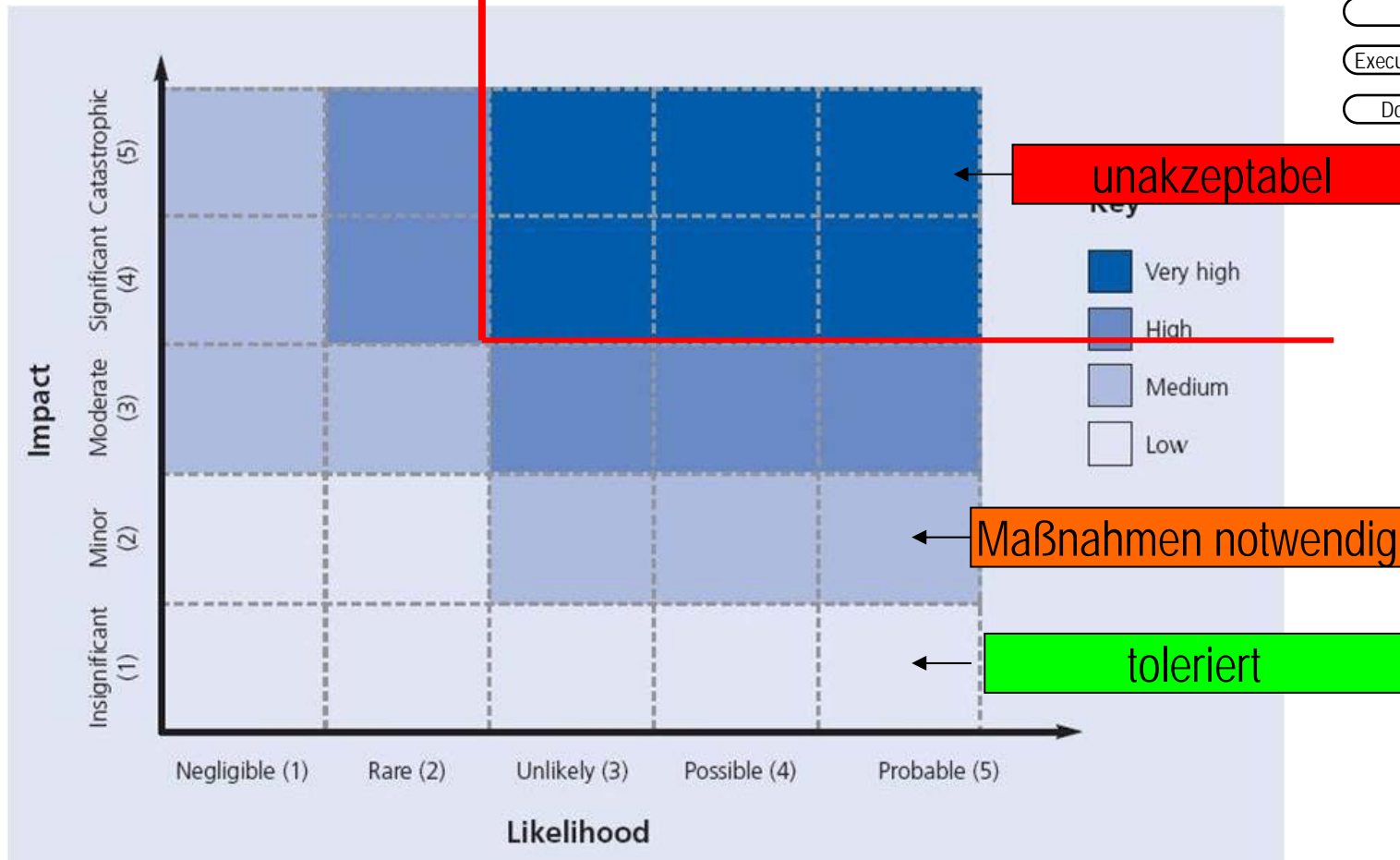
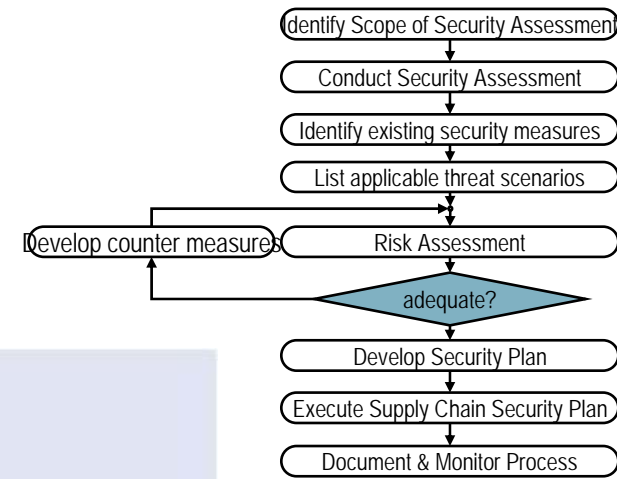
gering / mittel / hoch



Verlust der Fernseher (Wert)  
Verlust des Daten  
Ruf des Unternehmens(?)

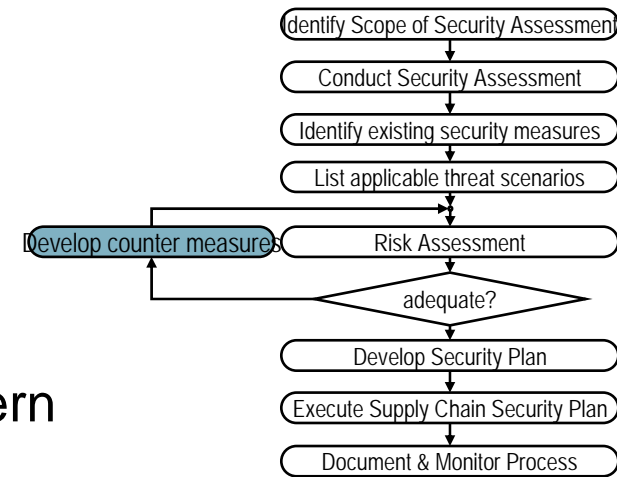
gering / mittel / hoch

# Akzeptanzkriterien

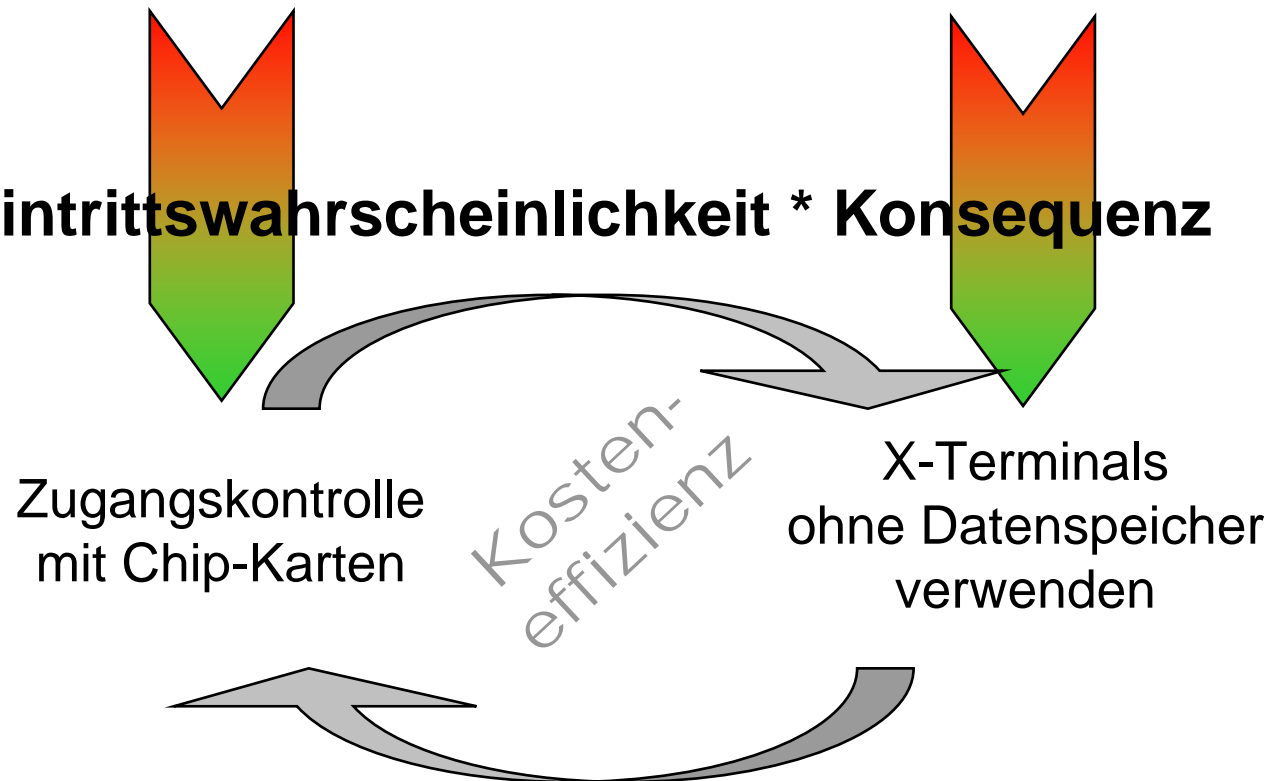


# Gegenmaßnahmen

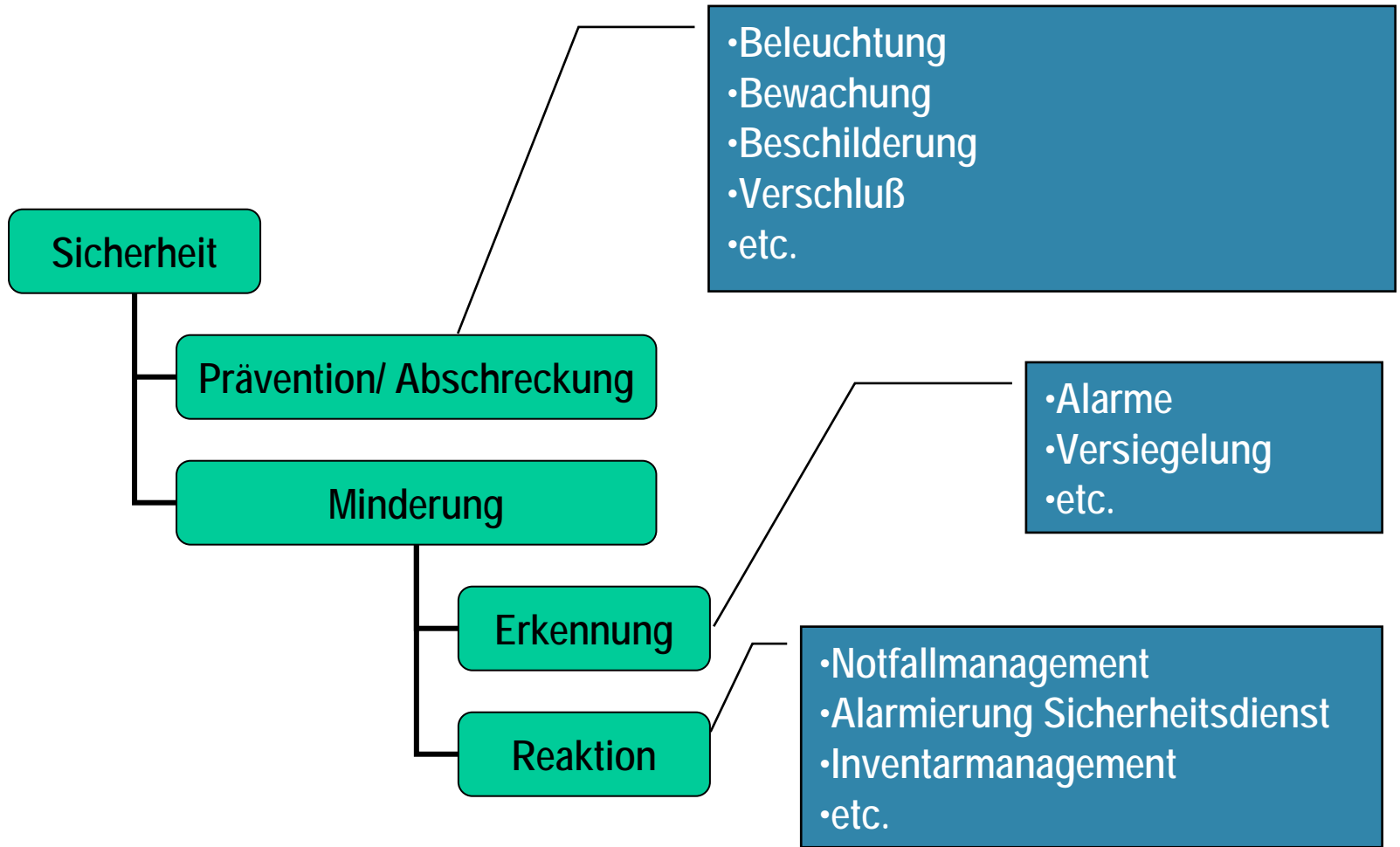
Beispiel: Einbruch und Diebstahl von Computern



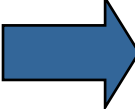
**Risiko = Eintrittswahrscheinlichkeit \* Konsequenz**



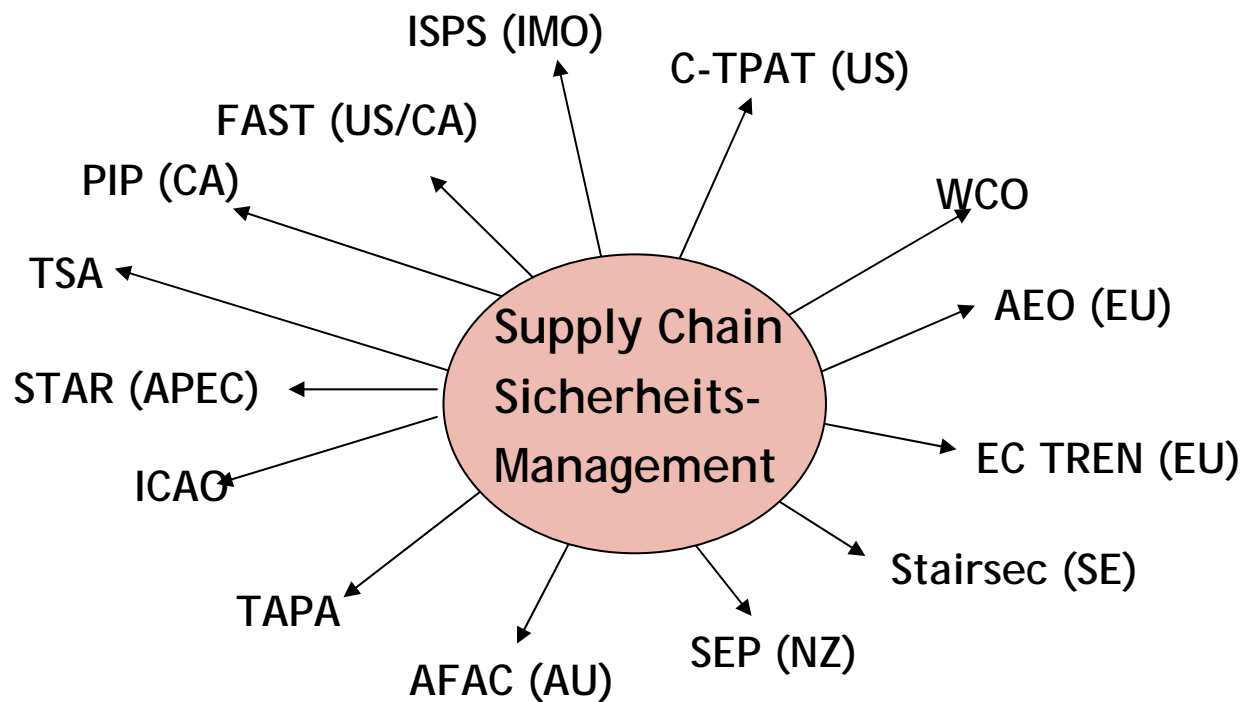
# Ganzheitliche Gegenmaßnahmen



# Inhalt

- Ein Szenario
- Ganzheitliche Sicherheitskonzepte
-  AEO und andere Sicherheitsinitiativen
- Anforderungen der ISO 28000
- Die ISO 28000 Zertifizierung
- GLC Hilfsmittel

# Verschiedene Sicherheitsinitiativen



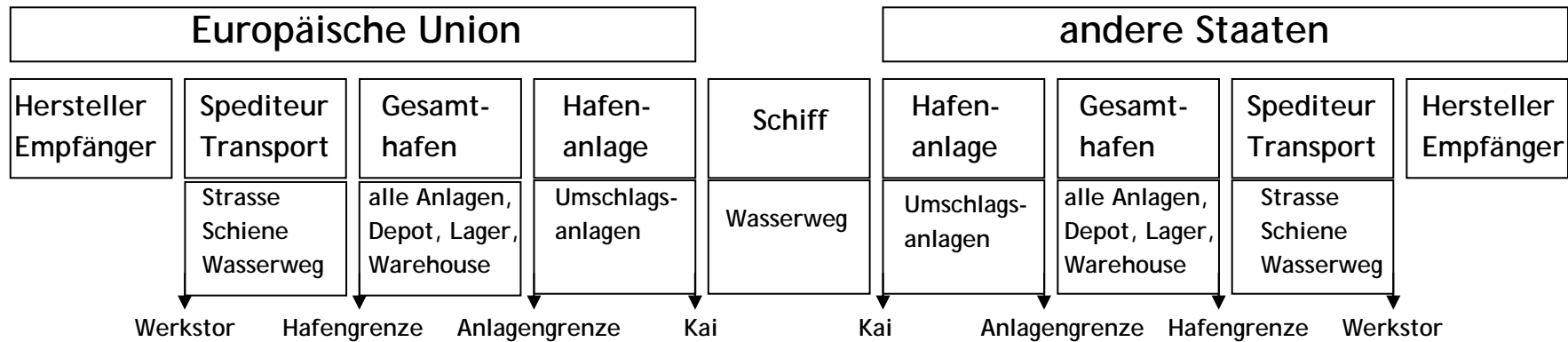
Je nach Interessenlage und Schutzziel wurden und werden Sicherheitsmaßnahmen und –standards zum Teil weltweit, aber auch regional begrenzt und isoliert voneinander entwickelt, in internationales oder nationales Recht überführt oder als Industriestandard bzw. Kundenanforderung quasi verbindlich.

*(Manfred F. Boes, Präsident FIATA)*

# Authorised Economic Operator (AEO)

- Beantragung des Status "Zugelassener Wirtschaftsbeteiligter" (Authorised Economic Operator) ab:
  - 1 Januar 2008 von
  - an der "Supply Chain" beteiligten Unternehmen mit Sitz in der EU
- Drei mögliche Kategorien:
  - Customs (C)
  - Safety and Security (S)
  - Full (F) – eine Kombination
- Um den Status zu erlangen, müssen jeweils bestimmte Kriterien erfüllt werden
- Eine ISO 28000 Zertifizierung muss vom Hauptzollamt zur Erfüllung der jeweiligen Kriterien anerkannt werden

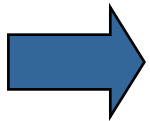
# Verschiedene Sicherheitsinitiativen



CSI				←→		←→			
ISPS				←→					
SST						←→			
TAPA		←→						←→	
C-TPAT	←→ USA			←→					
EU Trans	←→								
ISO 28000	←→								

# Inhalt

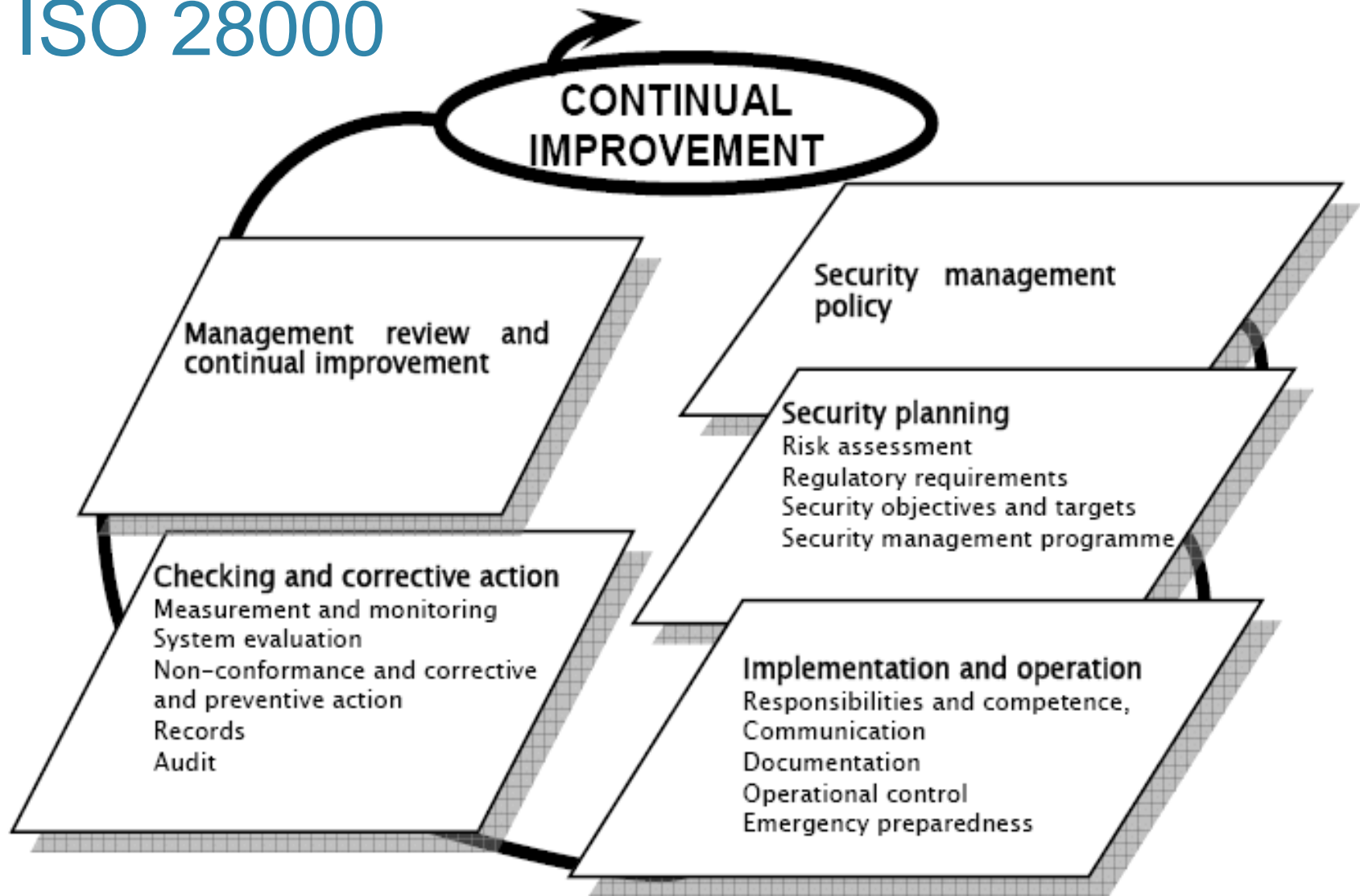
- Ein Szenario
- Ganzheitliche Sicherheitskonzepte
- AEO und andere Sicherheitsanforderungen



## Anforderungen der ISO 28000

- Die ISO 28000 Zertifizierung
- GLC Hilfsmittel

# ISO 28000



# Beispiel eines Programms

Security Objective	Reduction of risk level			
Security Target	Reduction of risk level tampering cargo unit from medium to low by implementing additional risk control measures			
Time Frame	3 months			
Measures	Responsibilities	Resources	Time frame	Completed (date)
Installation of motion detection systems interacting with lights and CCTV	Manager Storage	External supplier 30.000,-- €	01.03. - 15.04	
Development of a procedure for inspection and maintenance of the equipment	Manager Maintenance	4 man days	01.03. - 15.04	
Implementation of the procedure for inspection and maintenance of the equipment	Manager Maintenance	1 man day for familiarization	15.04. - 15.05.	
Training staff for operation and maintenance of the equipment	Manager Training	4 man days	15.04. - 20.04.	
Verification of progress (Date)	Grade of achievement %	Responsible Person	Comments	

# Inhalt

- Ein Szenario
- Ganzheitliche Sicherheitskonzepte
- Anforderungen der ISO 28000
- ➔ Die ISO 28000 Zertifizierung
- GLC Hilfsmittel

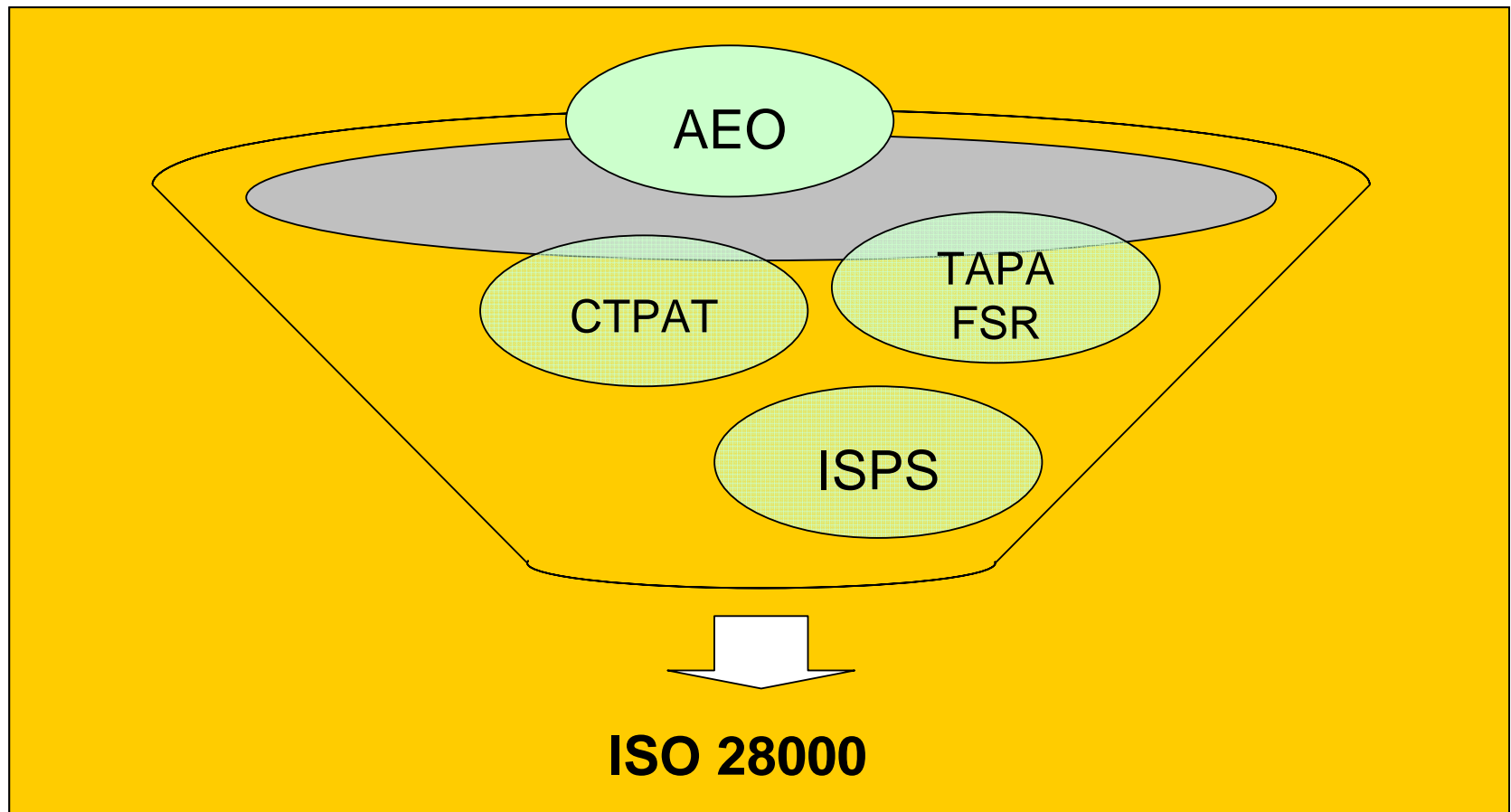
# Vorteile einer ISO 28000 Implementierung

- systematischer Ansatz zur Reduzierung von Diebstahl, Vandalismus, Unterschlagung, etc.
- implementieren Sie durch den Risikoanalyseansatz KOSTENEFFEKTIVE Sicherheitsmaßnahmen
- erhöht die Sicherheit bei allen Lager- und Behandlungsprozessen
- verbessert das Sicherheitsrating für die Behandlung von hochwertigen Waren und / oder Risikoprodukten
- fördert die Vertrauensbildung bei Ihren Kunden
- stärkt Grundwerte Ihres Unternehmens

# Vorteile einer ISO 28000 Implementierung

- senkt ihre Haftpflichtrisiken
- Firmen-interne Sicherheitsstandards über Benchmarking einführen
- unterstützt ihre Kommunikationsstrategie und verstärkt den Einsatz ihrer Mitarbeiter im Bereich Sicherheit
- bündeln sie die in der Logistikkette (Lieferkette) bereits vorhandenen Sicherheitsstandards in einem ganzheitlichen Managementsystem (unter Beachtung von z.B. AEO, C-TPAT, TAPA, etc.)

# Vorteile einer ISO 28000 Implementierung

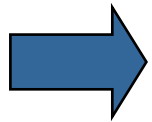


# Vorteile einer ISO 28000 Zertifizierung

- präsentieren Sie sich gegenüber ihren Geschäftspartnern als professioneller „sicherer Partner“
- bei bereits vorliegender Zertifizierung (Qualität / Umwelt) vermeiden sie Mehrfachaudits und deren Kosten
- AEO (Zugelassener Wirtschaftsbeteiligter)
- sehr gut mit TAPA kombinierbar
- öffentlicher Kompetenznachweis (public relations)
- Verbesserung der Zuverlässigkeit der Lieferkette
- Verbesserung der Sicherheit der Lieferkette (EU KOM)

# Inhalt

- Ein Szenario
- Ganzheitliche Sicherheitskonzepte
- Anforderungen der ISO 28000
- Die ISO 28000 Zertifizierung



GLC Hilfsmittel

# GLC Hilfsmittel

- **Checkliste zu ISO 28000**
  - Bestandsaufnahme
  - Sinnvoll bei der Implementierung aller ISO 28000-Anforderungen
- **To-Do List für Logistikunternehmen**
  - anwendbar, wenn ISO 9001 und ISO 14001 bereits implementiert sind
  - Auflistung aller neuen Schritte und Elemente
- **Leitlinien zur Implementierung von ISO 28000**
  - Development of a documented Security Management System
  - Step by Step Approach for Development and Implementation

Step By Step Approach for the Development and Implementation of a Security Management System

Steps	Activities
4. Identification of legal and other regulatory requirements	<p>4.1 Analyze the organizations supply chain activities for relevance with legal and other requirements</p> <ul style="list-style-type: none"> <li>- consider the results of risk identification, risk assessment and risk management</li> <li>- take into account best practices and guidelines issued in codes and by industrial associations</li> <li>- utilize available media to get access to information (e.g. internet, publications, rulebook, code, Standard)</li> <li>- identify and register legal and other requirements</li> <li>- specify which of the requirements apply where</li> <li>- decide where the documentation (rulebook, text, summary or analysis) of the requirements to be kept</li> <li>- decide who in the organization needs to have the information</li> </ul> <p>4.2 Establish, implement and maintain measures to monitor and control the application of legal requirements, rules and regulations</p> <p>4.3 Establish, implement and maintain measures to monitor legal developments and to analyse new requirements or changes to existing requirements for relevance for the own organization.</p>
5. Definition of the organization's security policy, with security objectives	<p>5.1 Formulate and document the security policy of the organization</p> <ul style="list-style-type: none"> <li>- ensure relevance of policy and the general objectives defined therein to the activities of the organization</li> <li>- reflect to the threats and security risks of the organization</li> <li>- be consistent with other organizational policies and with the company's overall threat and risk management framework</li> <li>- state clearly the overall broad security management objectives,</li> <li>- include a commitment to continual improvement of the security management system with its policy, processes and activities</li> <li>- include a commitment to comply with current applicable legislation, regulatory and statutory requirements and with other requirements to which the organization subscribes</li> <li>- consider general requirements of the stakeholders</li> <li>- include the involvement of employees and their contribution to the organization's security management system</li> <li>- include the relationship of contractors, stakeholders and other external persons for the enhancement of the overall security</li> </ul> <p>5.2 Endorse the security policy by signature of top management</p> <p>5.3 Implement and maintain the policy</p> <ul style="list-style-type: none"> <li>- consider issuing a detailed security policy for internal use and additionally a summarized non confidential version for external distribution</li> <li>- communicate the policy to all relevant employees and third parties including contractors and visitors</li> <li>- make the policy available to stakeholders and other parties where appropriate</li> </ul> <p>5.4 Derive and document quantified (where practicable) security management objectives</p> <ul style="list-style-type: none"> <li>- Communicate objectives to all relevant employees and third parties with the intent that these persons are made aware of their individual obligations</li> </ul> <p>5.5 Derive and document security management targets from the objectives</p> <ul style="list-style-type: none"> <li>- Ensure that these targets are specific, measurable, achievable, relevant, time-based (where practicable) and detailed enough to an appropriate level</li> <li>- Communicate targets to all relevant employees and third parties with the intent that these persons are made aware of their individual obligations</li> </ul>

Germanischer Lloyd © Version 01/2007  
The use of this document does not automatically qualify for successful certification. 4 / 10

# GL/GLC – Ihr Partner!

- **Kompetenz und Erfahrung in Sicherheit, Logistik und Transport**
  - weltweit führend in der ISPS-Zertifizierung (Schiffs- und Hafensicherheit)
  - eine der vier weltweiten TAPA-Zertifizierer
  - Globale Logistikerfahrung eingebracht bei der Entwicklung der eigenen Standards CCQI und CTQI
- **internationale Aktivitäten**
- **guter Ruf der GLC Zertifizierung im gesamten Markt**
- **hochqualifizierte, kompetente und unabhängige Auditoren**
- **Partnerschaftliche Zusammenarbeit zwischen GLC und Kunden**

# Kontakt

- **Wilhelm Loskot**
- **Abteilungsleiter "Schifffahrt und Logistik"**
  
- **Tel: +49 . (0)40 . 36149 - 593**
- **Fax: +49 . (0)40 . 36149 - 650**
- **Mobil: +49 . (0)172 . 451 77 41**
- **wilhelm.loskot@gl-group.com**

**Internet: [www.gl-group.com/glc](http://www.gl-group.com/glc)**

Vielen Dank für Ihre Aufmerksamkeit!

