JBW Group International
Information Assurance

Supply Chain Security and ISO 28000

Insight Brief **June 2009**

What if there was a way to reduce risks to the supply chain that also helped meet regulatory requirements and streamlined supply chain operations?

Security of the supply chain has always been a concern of transport, logistics and manufacturing companies. Concerns about theft, damage and shipment integrity intensify as the value per pound of cargo increases. Add the threat of organized crime, piracy and terrorism, and security of the supply chain becomes critical to business survival.

A Bit of Background

The transportation of goods in the global economy, driven largely by outsourcing of services, has never been more complex. Sources of raw materials, components, component assembly, and finished products are global in nature and therefore require a global supply chain. As this global dependence has intensified, the value of goods shipped has also increased. High value products such as electronics and pharmaceuticals account for a sizeable percentage of transported goods. A thirty-pound box of microprocessors valued at tens of thousands of dollars would typically be insured for less than $300 by freight carrier insurers.[1]

The threat of terrorism, smuggling (drugs, weapons, human trafficking), preservation of brand integrity, product safety and other threats have mandated the increase in regulation and cooperation between nations. Requirements of the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI), the Transported Asset Protection Association (TAPA) and others are some examples of regulation designed to address threats to the supply chain. These are complemented by the drive for increased surveillance and inspection.

One topic addressed at the 2009 International Transportation Forum[2] sponsored by the Organization of Economic Cooperation and Development (OECD) highlighted the challenges of improving security of the supply chain with increasingly scarce resources by using a risk-based model for policy appraisal and development.

ISO 28000

ISO 28000:2007 – *Specification for security management systems for the supply chain,* offers a framework for providing effective physical security management through a system that identifies security threats, assesses risk, establishes objectives for implementing controls and continuously improves the physical security of the organization.

Security Management System Elements

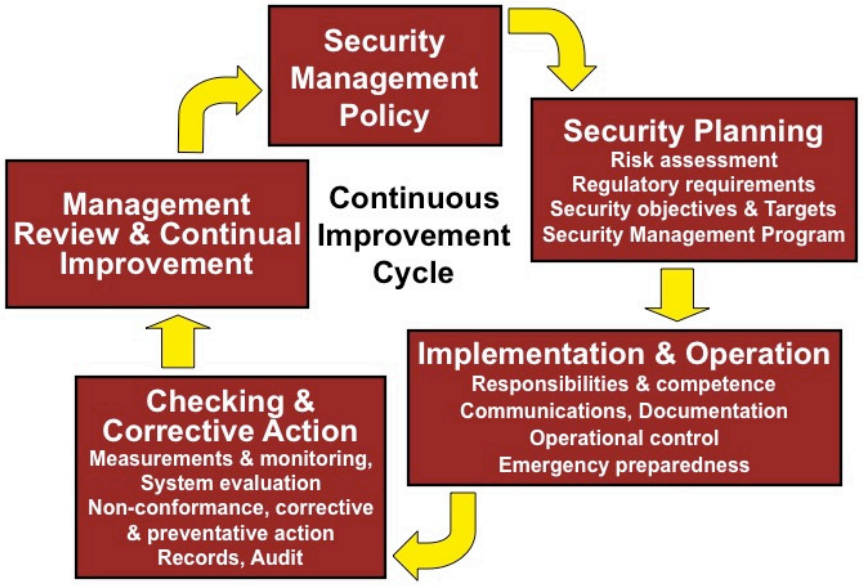
There are five key elements that are critical to the development of a Security Management System (SMS):

- Security Management Policy
- Security Planning
- Implementation & Operation
- Checking & Corrective Action
- Management Review & Continual Improvement

continued on page 2

continued from page 1

Components of a Security Management System using ISO 28000



Security Management Policy and Security Planning

A conformant physical security management system (SMS) requires the organization to have an overall security management policy, authorized by executive management. The SMS must also have a process for assessing the security environment in which it operates and for determining if adequate security measures are in place. This examination of the operational environment includes regulatory requirements as well as the physical, natural and human hazards and specific industry requirements. ISO 28000 articulates a strategy for assessment of risk and determining countermeasures as a core component of providing physical security for the organization.

Implementation and Operation

ISO 28000 identifies requirements for implementing and operating a SMS, including organizational (security) structure, authorized personnel responsible for security management, assessing and maintaining competence of personnel and training for personnel responsible for security.

Checking and Corrective Action

Corrective and preventative actions, based on monitoring and evaluation of the SMS, must be implemented to address any security-related failures and address in a timely fashion any non-conformities that are discovered.

Management Review and Continual Improvement

Oversight by the organization's executive management at regular intervals is required to assure that security management policy, objectives, targets and other elements of the SMS are functioning as intended and consistent with continual improvement. Records generated as part of the operation of the SMS, results of audits and risk assessments, legal and regulatory requirements are submitted for review along with input from interested parties and recommendations for improvement. Output from management review must include guidance for the organization to improve the SMS through changes to policy, controls and other elements of the security management system. ISO 28004:2007 provides corresponding implementation guidance for implementation of ISO 28000.

continued on page 3

continued from page 2

Benefits

A study by University of Virginia[3] researchers analyzing the cost/benefit of implementing Customs-Trade Partnership Against Terror (C-TPAT) requirements identified tangible benefits to organizations that implemented a supply chain security program. Among the benefits:

- Significant decrease in U.S. Customs inspections (up to 42.8%)
- Increase in new customers for transport and logistics companies (35.2%)
- Increase in sales (24.1%)
- Access to the U.S. Customs FAST (Free and Secure Trade) program
- Decreased wait time at the border (Green Lane)
- Decreased supply chain disruptions
- Increased supply chain visibility and improved lead-time predictability

An ISO 28000-conformant security management system will meet the security requirements of C-TPAT, World Customs Organization (WCO) SAFE Framework, Safety of Life at Sea (SOLAS) and other international regulations while providing greater visibility and optimizing the organization's security spend.

ISO 28001

Specific guidance for implementation of a security management system for the supply chain is provided in ISO 28001:2007 – *Best practices for implementing supply chain security, assessments and plans – Requirements and guidelines.* ISO 28001 is intended to assist organizations in establish reasonable levels of security and make better risk-based decisions for protection of the supply chain. Organizations that are in compliance with the WCO SAFE Framework of standards[4] are also in compliance with ISO 28001. In the absence of SAFE Framework compliance, ISO 27001 is an auditable standard containing requirements of a supply chain security process (General Requirements 4 – 5) and guidance for implementing a supply chain security process (Annex A).

A core component of ISO 28000 is planning the organization's security program, including a formal risk assessment and selection of controls and countermeasures. Annex B of ISO 28001 contains an eight-step methodology for security risk assessment and development of countermeasures. This specific methodology is not required for certification to 28001 but is provided as an informative reference for organizations seeking to implement a risk assessment process or refine an existing methodology.

Risk Management

Risk management is the process of identifying threats, vulnerabilities, impact to the organization in the event that a threat exploits a vulnerability, likelihood of such an occurrence and identification of countermeasures sufficient to reduce risk to levels acceptable to executive management. In ISO 28001 Annex B, the risk management methodology is captured in eight steps:

1. Identify all activities within the scope of the security management system (SMS)
2. Identify the security controls and countermeasures in place
3. Identify security threat scenarios
4. Determine the potential impact if the threat scenario actually occurred
5. Determine the likelihood of such an event occurring, given the current controls and countermeasures in place
6. Assess whether the current controls and countermeasures are adequate

continued on page 4

continued from page 3

7. If current controls and countermeasures are not adequate, develop and implement additional controls and countermeasures (develop a security plan)
8. Repeat the process

Executing this methodology at regular intervals and when significant changes occur in the operating environment enables an organization to proactively assess risk and continually improve the security program.

28000 Series

The International Standards Organization released the ISO 28000 series in 2007 to provide requirements and guidance to organizations seeking enhancement to supply chain security and to certification bodies providing audit and certification of supply chain security management systems. Unlike other standards that have been "fast-tracked" for release, the ISO 28000 series is a mature and fully realized set of documents. The series consists of:

- ISO 28000:2007 – *Specification for security management systems for the supply chain*
- ISO 28001:2007 – *Best practices for implementing supply chain security, assessments and plans – Requirements and guidance*
- ISO 28003:2007 – *Requirements for bodies providing audit and certification of supply chain security management systems*
- ISO 28004:2007 – *Guidelines for the implementation of ISO 28000*

Proper implementation and operation of a security management system will provide improved security and deliver tangible benefits.

[1] See Transported Asset Protection Association (TAPA) website at www.tapaonline.org.

[2] The 2009 International Transportation Forum, held in Leipzig, Germany on May 26-29, focused on transport for the global economy in a time of economic downturn. See www.internationaltransportforum.org for more information. The forum "Ensuring a Secure Global Transport System" referenced "Terrorism and International Transport: Towards Risk-Based Security Policy."

[3] The C-TPAT Cost/Benefit Survey was prepared by the University of Virginia Center for Survey Research and the Weldon Cooper Center for Public Service for the U.S. Customs and Border Protection Service in August 2007.

[4] The World Customs Organization (WCO), founded in 1952, is a collaboration of 174 countries' customs administrations. The SAFE Framework was adopted by the organization in 2005. The 2007 version of the SAFE Framework has incorporated detailed provisions concerning Authorized Economic Operators (AEO).

Registrar Requirements

ISO 28003:2007 specifies the requirements for registrars providing audit and certification of supply chain security management systems. Registrars are responsible for assuring that auditors have security clearance, government background checks, and carry tamper-resistant photo identification in addition to having in-depth knowledge of supply chain security, threat identification, risk assessment and mitigation, and incident planning and preparedness.

In addition to supplying highly qualified, vetted auditors, the registrars are required to have controls in place to safeguard the confidentiality, integrity and availability of information in their possession. The registrar requirements contained in ISO 28003 are the most rigorous of any ISO standards requirements to date.

For More Information…

JBW Group International
P.O. Box 19373
Minneapolis,
Minnesota 55419 USA
www.jbwgroup.com
Email: info@jbwgroup.com
1.877.97.27001