UNDERSTANDING THE **SUPPLY CHAIN SECURITY** CERTIFICATION STANDARDS

A DISCUSSION ABOUT THE CHALLENGES, IMPACTS AND OPPORTUNITIES FOR THE SECURITY OF SUPPLY CHAIN MANAGEMENT SYSTEMS

**JUNE 2012**

**AUTHORS**

Chris Yau  
Supply Chain Security Project Manager and Senior Manager,  
Products & Services Development, SGS

Ivan Yiu Wah Ha  
China/Hong Kong Product Manager, SGS Hong Kong
ABSTRACT

The purpose of this document is to introduce various standards and their certification programmes for supply chain security. It will also provide an overview of the similarities and differences of the various standards. This document is not intended to be a full explanation of the available standards, but instead it is to promote understanding of the standards and their benefits to organisations doing business at a domestic or international level within the supply chain.

CONTENTS

I. EXECUTIVE SUMMARY ..................................................................................................................... 1
II. SUPPLY CHAIN SECURITY ........................................................................................................... 2
III. SUPPLY CHAIN SECURITY CERTIFICATION PROGRAMMES .................................................. 4
IV. GLOBAL SOLUTIONS FOR ENSURING THE SECURITY OF SUPPLY CHAINS ....................... 6
V. CONCLUSION ............................................................................................................................... 13
During the last two decades there has been a boom in the high-tech industry. Most new products to market now include at least one high technology component. This drives high product value and leads to an increased interest, and associated threat, from international crime groups. According to the European Union, the theft of high-value, high-risk products moving in supply chains across Europe costs businesses in excess of €8.2 billion per year.* In 2011, the number of incidents that had a loss value of €100 000 or more (and/or incidents in which violence or the threat of violence was involved) doubled that of 2010. In the same period the average loss value per incident almost tripled – from €81 068 to €237 275. The variety of the type of incidents was also an important factor with theft from facilities, robberies, fraud, and hijacking all increasing in 2011. **

The globalisation of world markets and the tremendous growth of international trade have highlighted the need to specifically protect high-tech products, as well as other high value products, as they move through the supply chain. Over the past ten years, as the legal and regulatory environments have evolved, organisations have started to address the need for heightened security within global supply chains.

The International Organisation for Standardisation (ISO) has specifically developed a standard dedicated to supply chain security management systems: ISO 28000 Specifications for Security Management Systems for the Supply Chain. The Transported Asset Protection Association (TAPA) has developed their own standards for high-tech and high value products, including TAPA Freight Security Requirements (FSR), TAPA Trucking Security Requirements (TSR) and TAPA Air Cargo Security Standards (TACSS). The US Customs & Border Protection has also developed the Customs-Trade Partnership Against Terrorism (C-TPAT) programme.

With regulations increasing, security threatened, and the need for the rapid exchange of information concerning the transport of goods from manufacturing through to the final point of sale, there has never been a better time than now to reinforce existing security systems or create new ones backed by effective risk and quality management principles. Certifying your warehousing facilities and transit operations increases your security rating for the handling of high-value and high-risk products.

*IIS Annual Report 2012

I. EXECUTIVE SUMMARY

* www.tapaemea.com

** 2012 Annual Report 2012
According to a study published by TAPA in February 2012, the top five most frequently stolen goods were:

1. Non-electronics (eg toys, auto parts, construction materials, etc)
2. Electronics
3. Premium good and beverages
4. Metals
5. Clothing and footwear

These goods share some common “attractions” for cargo thefts:

- Manageable size (easy to steal)
- High value (worth the effort)
- Non-identifiable (easy to re-sell)

There are several ways that these goods are typically stolen, including from the logistics warehouses, manufacturers’ warehouses or production lines, truck hijacking, or posing as internal staff, etc.

Cargo security is no longer merely the responsibility of the logistics companies, but one that extends throughout the complete supply chain.

Cargo security is no longer merely the responsibility of the logistics companies, but one that extends throughout the complete supply chain. ‘Supply Chain’, by definition, is the entire value-chain from the manufacturer to the receiving end (including: trucking, airports and ports, train terminals, custom warehouses, etc). Any one of these links could present an opportunity for theft. The effective management of all these links forms the basis of ‘Supply Chain Security’.

Our experience shows that the most effective security systems are those that successfully combine an organisation’s security requirements with the parameters of the applicable regulations, whether they are local, regional or global. Furthermore, these security management systems are able to identify the most severe risk areas and allocate additional or a higher proportion of resources to those areas accordingly. In this manner, security management systems are integrated into the overall management system of an organisation and add value to the bottom line by protecting brand reputation and ensuring customer satisfaction. As with all management systems, at the heart of an effective security management system is the process of continual improvement.

The TAPA FSR and C-TPAT are two of the most notable supply chain security standards. The former targets warehouses and logistics companies whereas the latter aims at manufacturers shipping to the US. There are strengths and weaknesses in these standards. For instance, if you are a manufacturer that does not ship to the US, then currently there is no applicable certifiable (or auditable) security standard suitable for you. However, there are many buyers such as Walmart or Philips, who still perform audits of their suppliers and include security as one of the aspects.

In order to run a security management programme properly three factors are essential:

1. Risk assessment.

Risk assessment is the process by which an organisation identifies potential threats in order to manage decisions, such as the amount of control needed (eg CCTVs, gates, extra lighting, more patrols, etc), the competency and training needs of staff, the resources needed to prepare for an emergency or critical scenario, etc. Without a risk assessment, controls are implemented without justification for their adequacy and sufficiency, and can be over or under-implemented.

2. Management system elements.

A complete management system consists of more than just the operational practices. It includes other supporting requirements such as document control (to help you manage your documentation), objectives and targets (to ensure that you achieve continual improvement), internal auditing (to ensure you monitor your system), structure and responsibility (to define clearly the authority and responsibility), and corrective and preventive actions (to ensure incidents and shortcomings are handled systematically). These system elements provide the “tools” and platform to manage security issues, and ensure the security system is continually improved.


The PDCA cycle is the process of modern management thinking. In many organisations, operational practices are simply executed without subsequent monitoring. A typical example would be installing an advanced CCTV system (DO) in a low-risk residential estate without any risk assessment (PLAN) to justify the installation, and no maintenance and inspection of the videos (CHECK). In a PDCA security system, operational practices are seen as the controls to mitigate the previously identified risks, with the subsequent monitoring to ensure the practices are executed effectively.
SUPPLY CHAIN SECURITY STANDARDS – KEY MILESTONES

2001
C-TPAT program launched by the US Customs and Border Protection

2002
MOU agreed with 3 TAPA audit bodies (SGS, QMI and BVQI)

2005
• First TAPA TSR version developed
• FSR 2005 version deployed

2006
• TSR 2006 version deployed
• ISO/PAS 28001:2006 good practices guideline published

2007
• FSR 2007 version deployed
• ISO 28000 standard introduced

2009
FSR 2009 version deployed

2011
FSR 2011 version deployed

2012
• TSR 2012 version deployed
• TACSS introduced
SGS offers a wide portfolio of supply chain security solutions, including customised audits and certifications that can reinforce your security management systems and protect your brands and products as they make their way through global supply chains. We perform audits and certifications against all global and regional security requirements. Our core supply chain security certifications include the following:

**ISO 28000**
In 2007, the ISO published the ISO 28000 Specifications for Security Management Systems for the Supply Chain standard. The standard specifies the requirements for a supply chain security management system, linking security management to many other aspects of business management. These include all activities controlled or influenced by organisations that have an impact on supply chain security, including transportation of these goods along the supply chain. It uses a PDCA model and risk assessment to determine the corresponding control measures, resource provisions and training needs, etc.

ISO 28000:2007 certification applies to all organisations that would like to implement a security management system and integrate this into their overall quality management system, including small companies or large multinationals in the manufacturing, service, storage or transportation sector.

**TAPA FSR**
This standard is published by TAPA, an association of security professionals and related business partners from high technology companies. The standard is aimed at addressing the security threats that are common to the technology industry. It applies to any organisation with high value goods stored in warehouses and distribution centres, who utilise their own or sub-contracted transportation systems or freight forwarders. Companies in the pharmaceutical, clothing, tobacco, large retail business, or high-tech industry should use this standard to safeguard their warehouses, in addition to any transportation providers.

FSR addresses the nature by which high-tech products and materials are handled, warehoused and transported as they move across the world. It specifies the minimum acceptable security standards of these assets when they are travelling throughout the supply chain and the methods to be used in maintaining those standards.

The FSR standard determines the most suitable classification to be applied to the supply chain security. Classification “A” contains the most security requirements, with up to 77 criteria in the checklist; classification “C” contains the least, with only 41 criteria.

An updated version of FSR is expected to be published in 2013.

<table>
<thead>
<tr>
<th>FSR CLASSIFICATION</th>
<th>A*</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of criteria to meet/Number of mandatory requirements</td>
<td>77/23</td>
<td>68/23</td>
<td>41/9</td>
</tr>
<tr>
<td>Independent auditor needed</td>
<td>Yes for 1st year. Self-assessment in the 2nd year.</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Passing score</td>
<td>(1) 60% overall score in the checklist, and (2) 60% in section 1-5 of the checklist, and (3) A “1” in every mandatory questions in the checklist</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Description of data: 77/23 means 77 requirements of which 23 mandatory
The TSR standard has been established to ensure the safe and secure transportation of any assets of TAPA members throughout the world. The TSR specifies the minimum acceptable standards for security throughout the supply chain utilising trucking and associated operations, and the methods needed to maintain those standards. It also outlines the process and specification for suppliers to achieve compliance for their trucking operations.

The TSR standard determines the most suitable classification to be applied to the transportation security. Classification “1” contains the most security requirements, whereas classification “3” contains the least.

It is the intention of TAPA members to select suppliers that meet or exceed TSR compliance requirements. The TSR may be used in conjunction with other TAPA freight security requirements.

### TSR LEVELS

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of criteria to meet/ Number of mandatory requirements</strong></td>
<td>69 / 69</td>
<td>59 / 34</td>
<td>36/22</td>
</tr>
<tr>
<td><strong>Passing score</strong></td>
<td>100%</td>
<td>80%</td>
<td>60%</td>
</tr>
</tbody>
</table>

* Description of data: 36/22 means 36 requirements of which 22 mandatory

### TAPA TACSS

The TAPA TACSS is a certifiable security program for the protection of air cargo during temporary storage, handling and transportation. It specifies the minimum acceptable standard for ground handlers and operations.

Historically, air cargo handlers would be certified to FSR if they choose to pursue a security program. After TACSS was published, air cargo handlers may choose to use FSR or TACSS. From Jan 1, 2013, all air cargo handlers may only be certified against TACSS. Existing FSR-certified air cargo handlers whose certificates expire after Dec 31, 2012 may only be renewed to TACSS.

### TACSS LEVELS

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of criteria to meet/ Number of mandatory requirements</strong></td>
<td>100/100</td>
<td>54/54</td>
</tr>
<tr>
<td><strong>Passing score</strong></td>
<td>100%</td>
<td></td>
</tr>
</tbody>
</table>

* Description of data: 54/54 means 54 requirements of which 54 are mandatory

### C-TPAT

C-TPAT is a US government-business initiative programme designed to increase security at US borders. SGS provides a supply chain security audit tool based on C-TPAT requirements for security. The standard assesses an organisation’s security processes, identifies corrective actions and establishes improvement plans to address weaknesses. It can also assess a customer’s compliance with C-TPAT through periodic auditing of its commercial processes. In addition, the standard can be used to evaluate the compliance of security systems and procedures of prospective or contracted third-party suppliers, manufacturers, freight forwarders and similar service providers with the customer’s security requirements, based on a risk assessment of the entire supply chain.
IV. GLOBAL SOLUTIONS FOR ENSURING THE SECURITY OF YOUR SUPPLY CHAIN

WHY ISO 28000?

ISO 28000:2007 certification provides the following benefits:

- Allows security to be managed as a process so that the effectiveness of security management can be measured and improved
- Allows management to focus resources and efforts on areas with high-risk concerns (through a security risk assessment)
- Allows management to benchmark its security management efforts with international standards
- Demonstrates to stakeholders the commitment to enforce systematic security management

ISO 28000:2007 uses a pragmatic approach in which the risk levels of your supply chain operations are identified.

ISO 28000:2007 uses a more pragmatic approach in which the risk levels of your supply chain operations are identified. It enables your organisation to perform a risk assessment with supporting management tools (e.g., document controls, key performance indicators, internal audits and training) and applies the controls in accordance with the risk involved.

The framework of ISO 28000:2007 is structurally very similar to ISO 14001:2004 Environmental Management Systems (EMS) standard. The environmental aspects identification and evaluation process in EMS is analogous to security risk assessment in security management.

HOW DOES THE ISO 28000 AUDIT PROCESS WORK?

The ISO 28000:2007 certification process consists of six steps:

Step A – SGS provides you with a proposal based on the size and nature of your organisation. You can then proceed with the audit by accepting the proposal.

Step B – You may ask SGS to perform a ‘pre-audit’ to give an indication of the readiness of your organisation for the audit. This stage is optional, yet it is often found useful in identifying any weaknesses in your systems and in building confidence before the formal audit.

Step C – The first part of the formal audit is the ‘Stage 1 – Readiness Review’. This lets us evaluate the compliance of your documented system with the requirements of the standard to better understand the nature of your organisation, to plan the rest of the audit as effectively as possible and to initially examine key elements of the system. You will receive a report after this stage identifying any concerns or observed non-compliances so that you can take immediate action if required.

Step D – This is ‘Stage 2’ of the initial audit process. The audit includes interviews with you and your colleagues and examination of records. Observation of your working practices determines how compliant your actual processes are with the standard and with your own documentation system. At the end of this stage, we will present the findings of the audit classified as either major or minor non-conformances along with other observations and opportunities for improvement. Once you have addressed the non-conformities, a technical review of the audit will then be conducted by an authorised SGS Certification Manager to confirm the issuance of a certificate.

Step E – Our surveillance visits will be scheduled at either six or twelve month intervals depending on the contract. During the visits, we review the implementation of the action plan addressing the past non-conformities and examine certain mandatory and other selected parts of the system in line with an audit plan that we provide you before each visit.

Step F – Shortly before the third anniversary of the initial certification, our routine visit will be extended to enable a re-certification audit. Surveillance visits will then continue, as before, on a 3-year cycle.

ISO 28000:2007 CERTIFICATION PROCESS

<table>
<thead>
<tr>
<th>ASSESSMENT AND CERTIFICATION</th>
<th>ANNUAL SURVEILLANCE VISITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>STEP A Agree Contract</td>
<td>Certificate Issue on Completion of Successful Audit</td>
</tr>
<tr>
<td>STEP B Optional Pre-Audit</td>
<td></td>
</tr>
<tr>
<td>STEP C Stage 1 Audit</td>
<td></td>
</tr>
<tr>
<td>STEP D Stage 2 Audit</td>
<td></td>
</tr>
<tr>
<td>Action and Closure of Identified Non-Conformities</td>
<td>Action and Closure of Identified Non-Conformities</td>
</tr>
<tr>
<td>STEP E Surveillance Visits</td>
<td></td>
</tr>
<tr>
<td>STEP F Recertification Audit</td>
<td>Certification Cycle Typically 3 years</td>
</tr>
</tbody>
</table>
MAIN AUDIT

INITIAL AUDIT STAGE 1
Onsite evaluation of SCS MS documentation, scope, resources and preparedness for Stage 2

INITIAL AUDIT STAGE 2
Onsite evaluation of the implementation and effectiveness of SCS MS

Closing meeting and confirmation of any non-conformities

Initial audit corrections and corrective action completed

Corrective action not completed or not satisfactory

No certificate issued

Corrections and corrective action evidence assessed by certification body by documented evidence or revisit. Successful close out documented

Independent certification review completed

Certification decision made by certification body

Ongoing surveillance audits (see Surveillance Audits flow chart)

No non-conformities raised

Corrective action not completed or not satisfactory

No certificate issued
SURVEILLANCE AUDITS

To ensure continuous improvement, a series of surveillance audits are scheduled, with a minimum of one per year.

Following issuance of the certification, ongoing pre-planned surveillance audits occur a minimum of once per year.

A surveillance audit report is completed and detailed findings during the audit and non-conformities are documented.

Non-conformities raised

Correction and corrective action must be taken and verified by the auditor either by a re-visit or documented evidence.

- No correction and corrective action taken or not effective
  - Decision made on suspension or withdrawal of the certificate

Correction and corrective action acceptable

Continuing Surveillance visits

Re-Certification every 3 years

Minor non-conformity raised

Correction and corrective action plan submitted and verified. Full verification of the corrective action completed at the next due visit.

- No correction or corrective action plan submitted
  - Decision taken on suspension or withdrawal of the certificate

No non-conformities raised

Correction and corrective action plan submitted and verified. Full verification of the corrective action completed at the next due visit.

- No correction or corrective action plan submitted
  - Decision taken on suspension or withdrawal of the certificate
WHY TAPA FSR?

Any TAPA certification provides the following benefits*:

• Recognised globally as the industry standard for cargo facility and transport security
• Enables you to use the latest cargo crime intelligence from IIS to avoid incident ‘hotspots’, protect your goods in transit and, if required, to report and trace stolen property
• Ensures your requirements to reduce crime are regularly consulted at the highest level of relevant government departments and with law enforcement agencies
• Allows sharing of best practice and networking with like-minded companies
• Provides you with a monthly newsletter

In addition to the general TAPA benefits, the following benefits are particular to FSR:

• Enables partnership with high-tech buyers (eg Intel, Infineon, HP, Nokia, etc)
• Allows your organisation to be more marketable
• Increases security ratings for the handling of high-value/high-risk products
• Demonstrates concern and capability to service customers’ security expectations
• Opens your organisation to TAPA member supply chain management business
• Helps build a management system that is up-to-date with the very latest technological and organisational safety requirements
• Reduces insurance liability exposure
• Supports the communications strategy, reinforcing the core values of a company and demonstrating employees’ on-going commitments to security

HOW DOES THE FSR CLASSIFICATION PROCESS WORK?

The certification process for TAPA FSR consists of five steps:

Step A - SGS provides you with a proposal based on the size and nature of your organisation. You can then proceed with the audit by accepting the proposal.

Step B – You may ask SGS to perform a ‘pre-audit’ to give an indication of the readiness of your organisation for the audit. This stage is optional, yet it is often found useful in identifying any weaknesses in your systems and in building confidence before the formal audit.

Step C – This is the initial audit process. The audit includes interviews with you and your colleagues and examination of records and physical security measures. Observation of your working practices determines how compliant your actual processes are with the standard and with your own documentation system. At the end of this stage, we will present the findings of the audit in the TAPA scoring spreadsheet that also shows non-conformances along with other observations and opportunities for improvement. When you have demonstrated the 60% minimum score, and have addressed any zero scored mandatory items, a technical review of the audit will then be conducted by an authorised SGS Certification Manager to confirm the issuance of a certificate.

Step D – Review of your internal audit. One year after the initial audit by SGS, you submit your annual internal audit to us and we review this for continued compliance with the FSR standard.

Step E – Shortly before the second anniversary of the initial certification, we will visit again to verify continuing compliance, and then renew your certificate.

WHY TAPA TSR?

In addition to the general TAPA benefits (as stated above under TAPA FSR), the following benefits are particular to TSR:

• Enables partnership and increases business opportunities with global freight forwarders (eg CEVA, Schenker, DHL, etc)
• Enhances drivers’ sense of security in the line of duty
• Improves drivers’ job satisfaction (if they are aware that their operational practices are in line with an industrial best practice)
• Enables better load utilisation (and hence profitability) when transporting high value/high risk products (many buyers allow full load only if the service provider is TSR certified)

HOW DOES THE TSR CLASSIFICATION PROCESS WORK?

A TSR audit process typically consists of four elements:

Step A – Once the contract has been agreed upon, SGS will define an audit programme based on the agreed TSR level checklist

Step B – SGS conducts the audit. Auditors will follow the audit protocol as per the agreed TSR level and vehicles / routes concerned

Step C – On completion of the audit, we will provide the scored audit checklist that will also be submitted to the SGS technical reviewer to review and approve prior to sending the final report and certificate. During the audit, we will also make recommendations for future improvement

Step D – Ongoing monitoring audits will be performed if required

* www.tapaemea.com
WHY TAPA TACSS?
In addition to the general TAPA benefits (as stated above under TAPA FSR), the following benefits are particular to TACSS:
- TACSS is the result of the collective wisdom and experience of numerous air cargo handling practitioners in the industry and government supply chain security programs
- TACSS requirements anticipate existing and emerging threats to air cargo including theft, pilferage, tampering, and intentional use of cargo for terrorist purposes
- TACSS is compatible with, and could be used in conjunction with, other TAPA standards (FSR and TSR) as well as other security program such as ISO 28000

HOW DOES THE TACSS CERTIFICATION PROCESS WORK?
A TACSS audit process typically consists of four elements:
Step A – You (the air cargo handling service provider) will determine your security level by completing the risk assessment questionnaire found on the TAPA website or provided by SGS.
Step B – SGS, after reviewing the risk assessment questionnaire and security level, will provide you with a proposal. Once the proposal has been agreed upon, SGS will schedule and plan the audit.
Step C – SGS conducts the audit. Auditors follow the audit protocol corresponding to security level. Every requirement (except for those officially waived by TAPA) must be met. If a requirement is not met, corrective actions must be implemented within 60 days.
Step D – On completion of the audit, we provide the scored audit checklist that also be submitted to the SGS technical reviewer to review and approve prior to sending the final report and certificate to you. During the audit, we will also make recommendations for future improvement.
Step E – You will perform a self-assessment using the TACSS checklist within 12 months of the first audit and submit the completed checklist (with corresponding corrective actions if needed) to SGS.
Step F – Steps A to D will be repeated before the end of the 36th month of the first audit.
Step G – You will perform a self-assessment every 24 months afterwards and submit the completed checklist (with corresponding corrective actions if needed) to SGS.

WHY C-TPAT?
C-TPAT certification provides the following benefits:
- Compliance with customer requirements
- Fast-lane custom clearing (C-TPAT)
- Reduced cargo loss
- Enhanced social responsibility
- Improved competitive advantage

HOW DOES THE C-TPAT AUDIT PROCESS WORK?
The total score for the C-TPAT criteria is 362 (100%); however, certification is granted to a specific facility location for a C-TPAT audit score of 60% or higher and all mandatory items scoring at least a “1”. The supplier can, in accordance with the audit result, continually improve the security system and the buyer can easily identify the risk level of their suppliers.

<table>
<thead>
<tr>
<th>ACHIEVEMENT LEVEL</th>
<th>SCORES ON CHECKLIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>&gt;80%</td>
</tr>
<tr>
<td>Level 2</td>
<td>&gt;67%</td>
</tr>
<tr>
<td>Level 3</td>
<td>&gt;60%</td>
</tr>
<tr>
<td>Level 4</td>
<td>&lt; 60%</td>
</tr>
</tbody>
</table>
AUTHORISED ECONOMIC OPERATOR (AEO)

The European Commission has adopted this regulation with the intent of increasing security for shipments entering or leaving the EU and providing greater facilitation for compliant operators, introducing a framework for better risk analysis of goods crossing EU borders. Trade facilitation measures include the electronic exchange of advance information between traders and customs authorities on all goods entering or leaving the EU. The regulation also requires customs authorities to exchange information electronically on exports in order to speed up export procedures. Compliance with AEO can be greatly assisted through ISO 28000 or TAPA certification.

COMPARISON OF SUPPLY CHAIN SECURITY CERTIFICATION PROGRAMS

<table>
<thead>
<tr>
<th>ISO 28000</th>
<th>TAPA FSR</th>
<th>TAPA TSR</th>
<th>TAPA TACCS</th>
<th>C-TPAT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targeted organisations</strong></td>
<td>Any organisation in a supply chain</td>
<td>Warehouses and logistics companies, usually explicitly required by customers but voluntary certification is OK</td>
<td>Any organisation operating a trucking fleet</td>
<td>Air cargo handling service providers</td>
</tr>
<tr>
<td><strong>Management System?</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Risk assessment required?</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Ease of integration with other management system (i.e. ISO 9001)</strong></td>
<td>Yes</td>
<td>Only the operational procedures</td>
<td>Only the operational procedures</td>
<td>Only the operational procedures</td>
</tr>
<tr>
<td><strong>Applicable to logistic sector</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Applicable to manufacturing sector</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Covering risks other than physical security</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Prescriptive requirements of security practices</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
V. CONCLUSION

Supply chain management services combines the benefits of a business management tool linking supply chain security and business processes with the ability to meet growing global customer requirements for a certified supply chain. Supply chain security demands that organisations demonstrate control over identified threats, and ensures that systems and services meet the requirements of standards set by governments, entities or customers across most major industries in the world. It provides real value to an organisation, irrespective of size and complexity, and levels the playing field for customers and suppliers throughout the supply chain and around the world.

ABOUT THE AUTHORS

Chris Yau
Supply Chain Security Project Manager
and Senior Manager, Products & Services Development, SGS

Chris Yau has 15 years experience in audit against various standards, including quality, environmental, health and safety, hazardous substance process management, information security, IT service management, and supply chain security. He is responsible for developing the ISO 28000 assessment and training service offerings. In his other capacity, Chris is also the product manager for other IT and security related standards.

Ivan Yiu Wah Ha
China/Hong Kong Product Manager,
SGS Hong Kong

Ivan Ha has over 16 years of experience in supply chain quality assurance and security management including consultancy, training and auditing. Ivan has provided training in supply chain security, Lean 6 Sigma, service management, as well as quality management, to many national and international manufacturers and logistic companies. He also has vast auditing experience in C-TPAT, TAPA FSR, TAPA TSR, ISO 9001, TS16949, Service Certification and has performed over 800 audits. Ivan is now responsible for all the supply chain security management and related technical development in the China, Hong Kong region.
ABOUT SGS

SGS is the world’s leading audit and certification body with over 110,000 organisations certified across a wide variety of industry segments. We are also the market leader in the field of transportation and supply chain security, having issued over 600 TAPA certificates*, making us the global leader in TAPA certification. SGS is the first certification body to be awarded the accreditation on ISO 28000 by ANAB (ANSI-ASQ National Accreditation Body, US). We also advise on policies and procedures against both applicable legal requirements and international best practices to identify areas of key bribery risks and ensure anti-corruption compliance within organisations’ supply chains.

Our reputation for technical expertise combined with our worldwide network of auditors, who operate as comfortably in English as they do in their local language, provides for an internationally consistent service across the world. In addition, our Global Key Account Management team oversees all activities, communications and technical interpretations and incorporates a standardised web-based reporting format, making execution faster and your job easier.

SGS performs audits and certifications against all global and regional supply chain security requirements.

SGS is the world’s leading inspection, verification, testing and certification company. Recognized as the global benchmark for quality and integrity, we employ over 70,000 people and operate a network of more than 1,350 offices and laboratories around the world. We are constantly looking beyond customers’ and society’s expectations in order to deliver market leading services wherever they are needed.

Our approach is transparent and logical, which is what makes SGS the ideal independent partner to help you in your quest for continuous improvement. Our experts are selected and trained based on their technical expertise as well as their business acumen, and like all SGS employees their objectivity, ethics and confidentiality are beyond reproach.

FOR MORE INFORMATION, VISIT WWW.SGS.COM/LOGISTICS OR EMAIL SUPPLYCHAINSECURITY@SGS.COM

* 2012