



# SUPPLY CHAIN SECURITY, MANAGEMENT SYSTEMS, AND THE ROLE OF THE ASSURANCE PROVIDER

**March 2009**

Prepared on behalf of LRQA  
[www.supplychain.lrqa.com](http://www.supplychain.lrqa.com)  
[www.businessassurance.com/supplychain](http://www.businessassurance.com/supplychain)

By Dr. Andrew Grainger  
Director, Trade Facilitation Consulting Limited  
[www.tradefacilitation.co.uk](http://www.tradefacilitation.co.uk)

## Summary

This white paper sets out to show how standardised management systems can be utilised to help underpin newly emerging security initiatives as well as manage the risks inherent in today's global supply chain operations.

In the years following September 11th 2001 there has been an avalanche in supply chain security-motivated initiatives. These include, amongst others: the World Customs Organisation's (WCO) SAFE framework, the International Maritime Organisation's (IMO) International Ship and Port Facility Security (ISPS) Code, The International Air Transport Association (IATA), EU regulations from Transport & Energy (DGTREN) and Taxation & Customs Union (DG TAXUD), and the Transported Asset Protection Association's (TAPA) Freight Security Requirements. These initiatives are in addition to an already extensive palette of safety and security-related controls and procedures that companies need to comply with.

Organisations with any significant scale of operation rely on management systems to implement their management objectives and monitor their performance. Increasingly, businesses are looking to ISO 28000 'Specification for security management systems for the supply chain' to address their security-related requirements. ISO 28000 is a standardised system that has been specifically developed to manage an organisation's supply chain security needs – including the requirement to comply with regulatory set rules and procedures – and can be easily merged with existing management systems (such as quality, environment and health and safety).

Independent, third-party certification provides a means for businesses to show stakeholders such as clients and regulators that they have robust security management systems in place. The value of certificates issued by assurance providers can be particularly high in countries where it confers exemptions from regulatory requirements or when viewed as equivalent with official authorisations. At present ISO 28000 does not have that status in most of the newly-introduced security programmes. However, some legislative developments (for example the European Union's Authorised Economic Operator (AEO) suggest that wider recognition of ISO 28000 certification will be available.

A range of business benefits can be associated with effectively and efficiently managing supply chain security through the use of an ISO 28000 system. Typically, these benefits include: reduced cost of damages and losses; regulatory compliance; undisrupted and reliable operations; increased protection and security of assets, goods, and products; enhanced value for end-customers; and efficient and effective control procedures resulting in the development or protection of competitive advantages.

One of the major benefits associated with ISO 28000 is that it provides a means of tying together all regulatory compliance requirements into one single system. As such, it can help reduce the costs associated with what some call 'security spaghetti'<sup>1</sup>

Companies are usually aware of where risks within their own operations lie. Management systems such as ISO 28000 enable them to apply an effective control regime to their own organisation. This is considerably more effective than any arms-length inspection arrangement. Moreover, unlike government executive agencies, companies can enforce their security objectives system-wide and irrespective of national borders.

Once significant numbers of businesses choose to implement security management systems like ISO 28000, it is foreseeable that resource-savings for society and governments can materialise. Official recognition of ISO 28000 certificates will confer a number of benefits to government executive agencies. The most significant of these benefits are government resource savings

---

<sup>1</sup> Grainger (2007) 'Supply chain security: adding to a complex operational and institutional environment', World Customs Journal, Vol 1, Issue 2, September (see Annex 2)

related to reduced requirements of direct intervention into business operations through inspections or controls, as well as an unambiguous split between certification and law enforcement.

Further benefits to government, by accepting ISO 28000 certificates, will include a risk-based and targeted control practice which is unrestricted by national borders. Recognition of ISO 28000 certificates as equivalent to official certificates can reduce the regulatory burden suffered by businesses and reduces transaction costs between business and government.

ISO 28000 provides a powerful and flexible tool for businesses to manage their security requirements. Independent assurance and certifications provide confidence in that system and once recognised by authorities, it can serve as a vehicle to reduce regulatory complexity within the area of supply chain security, as well as actively manage overall security risks.

ISO 28000 can also contribute to 'customs to customs' mutual recognition initiatives by establishing a common framework from which to manage security requirements; and therefore encourage confidence in the development of a universal global security requirement.

## **Disclaimer**

Lloyd's Register, its affiliates and subsidiaries and their respective officers, employees or agents are, individually and collectively, referred to in this clause as the 'Lloyd's Register Group'. The Lloyd's Register Group assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register Group entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.

# 1. Introduction

Over the last few years, especially in response to the terrorist attacks in the USA on September 11, 2001, there has been an avalanche of supply chain security-motivated initiatives. These are in addition to an already extensive palette of safety and security-related controls that companies need to comply with. Many of these controls and procedures are not necessarily regulatory driven and have their roots within the company's own safety and security objectives. The challenge for businesses and government executive agencies is to meet security objectives without unnecessarily escalating costs or compromising on tightened security aspirations.

Most companies with any significant scale of operation rely on the use of management systems to implement management objectives. They are used extensively in supply chain management practice. ISO 28000 is a standardised system that has been specifically developed to meet an organisation's supply chain security needs, including the requirement to comply with regulatory set rules and procedures. System certification by independent assurance providers gives confidence to others that the organisation is actively managing its security requirements in compliance to its security policy.

This paper has four aims:

1. To help public and private sector interest groups gain an understanding of management systems' functionality and their reliance on assurance principles.
2. To show how ISO 28000 serves as an umbrella system that provides an effective and efficient vehicle for safeguarding compliance with a wide set of security objectives, including those set by government authorities.
3. To build a case for recognising that ISO 28000 security management system specification is the way organisations can establish alignment with regulatory-defined security requirements.
4. To show how the services of assurance providers fit into the field of supply chain security.

As such the paper is structured into nine sections:

<b>Section 1</b>	-	<b>Introduction</b>
<b>Section 2</b>	-	<b>The supply chain security environment</b>
<b>Section 3</b>	-	<b>Management systems</b>
<b>Section 4</b>	-	<b>The ISO 28000 system</b>
<b>Section 5</b>	-	<b>Assurance and certification</b>
<b>Section 6</b>	-	<b>Managing SC security requirements through ISO 28000</b>
<b>Section 7</b>	-	<b>Business and government drivers</b>
<b>Section 8</b>	-	<b>Benefits conferred by using the services of assurance providers</b>
<b>Section 9</b>	-	<b>Conclusion</b>

## 2. The supply chain security environment

The recent flood of supply chain security-motivated initiatives has international as well as regional and national manifestations. International initiatives include, amongst others: the WCO's SAFE framework, the IMO's International Ship and Port Facility Security Code (ISPS), Aviation security requirements as set forward by e.g. IATA, and the Transported Asset Protection Association's (TAPA) Freight Security Requirements. Examples of recent regional and national initiatives include the European Union's Security Amendment to the Customs Code and its Authorised Economic Operator (AEO) concept, the USA's Customs and Trade Partnership Against Terrorism (C-TPAT), the USA's Container Security Initiative (CSI) and Secure Freight Initiative (SFI), plus many more supply chain security-focused programmes in countries such as Japan, Singapore, Australia, and China.

However, security concerns in business operations are nothing new. Most businesses will already have put in place systems to address security-specific issues. To give a few examples, deployed management systems are likely to cover areas as diverse as: product quality; the safety of products and assets; the physical handling of goods; payment and financial arrangements; the prevention of theft and pilferage; and the misuse of goods, equipment, and infrastructure by criminals. Furthermore, there are a wide range of regulations with security components that have been in place well before recent acts of terrorism gave rise to current policy concerns. Businesses need to ensure that they comply with the legislatively set rules and procedures. In most countries it is easy to count 30 or more regulatory initiatives that have security dimensions. To give an example of regulatory complexity Figure 1 shows the UK case based on research first published by SITPRO, the UK trade facilitation agency<sup>2</sup>. The resulting complexity and overlap is described by some as 'security spaghetti'<sup>3</sup>, and is a cause for concern in both policy and business circles where the added cost of compliance threatens to undermine economic performance.

- Animal Health Controls and Licensing
- Authorised Economic Operator
- Aviation: "Known Shipper"
- Bio Terrorism Controls
- Carcinogenic substances - Import Licences
- Compliance with specified Health and Safety procedures for the handling of goods
- Container Security Initiative (CSI)
- Customs and Trade Partnership Against Terrorism (USA)
- Customs Pre-notifications (Security)
- Dangerous Goods Declarations (Air)
- Dangerous Goods Declarations (Rail)
- Dangerous Goods Declarations (Road)
- Dangerous Goods Declarations (Sea)
- Export Controls (End-use and Destination)
- Export Controls (Precursor Drugs)
- Export Controls (Technology, Dual-use & Military)
- Financial crime and terrorist financing, restrictions and controls
- Food and Hygiene Controls
- Formal Cooperation Agreements between Businesses and Executive Agencies (including MoUs)
- Immigration (outward) - as proposed under eBorders
- Immigration Controls (passengers)
- Immigration Controls (vehicle operators)
- Maritime: ISPS Code and SOLAS Convention
- Medical Equipment Licensing
- Medicines and Drugs Licensing
- Plant Health Controls and Certificates
- Prior Ship-notification
- Road Operator Licensing
- Rough Diamond Certificate
- Secure Freight Initiative (cargo scanning of US bound traffic)
- Secure Operator (DG Transport)
- TAPA-FSR
- Use of additional scanning equipment (e.g. x-ray scanners, scanning for radioactive materials, scanning for explosives, etc.)

**Figure 1: Example – Security initiatives as applicable to UK traders<sup>4</sup>**

<sup>2</sup> SITPRO and Grainger (2008), A UK Review of Security Initiatives in International Trade, SITPRO: London

<sup>3</sup> Grainger (2007) 'Supply chain security: adding to a complex operational and institutional environment', World Customs Journal, Vol 1, Issue 2, September (see Annex 2)

<sup>4</sup> Adapted from: SITPRO and Grainger (2008), A UK Review of Security Initiatives in International Trade, SITPRO: London

The considerable overlap of regulatory activity is a significant source of burden for most businesses involved in international trade operations. Their challenge is to enhance their management systems to ensure continued regulatory compliance and improve security performance without inflating costs. Similarly, government executives responsible for enforcing safety and security in international trade (e.g. customs, department for transport, border protection, immigration, health) face their operational challenges, too. Most of the newly emerging security regimes require them to expand the control focus to cover the entire supply chain. However, unlike the national borders over which government executive agencies have direct power, the supply chain is a construct that is defined by fluid arrangements between contracting business parties. Adding to the enforcement challenge is that no two supply chains are alike and operational practices from one company to the next vary considerably.

Given the diversity in operational practices as well as in the sources of security-related risk, one size seldom fits all. Businesses often complain about the regulator's failure to sufficiently accommodate prevailing business practices and argue that overly prescriptive regulatory approaches to supply chain security can prove expensive to implement and may compromise the desired outcome of tightened-up security. In contrast, the desire to tighten up security without increasing the compliance burden can be achieved by integrating regulatory requirements into businesses' management systems.

### 3. Management systems

Most businesses already draw on some form of **management system** to manage their supply chain, including associated security requirements. The security requirements addressed by these systems are likely to extend well beyond those set by the regulator. For example, a soft-drink manufacturer with a global reputation to protect is likely to impose a very stringent quality regime across all stages of its supply chain, ranging from suppliers of ingredients to bottling plants and distributors. While it is not feasible to physically check and test each bottle before it is delivered to the customer or stand over the shoulder of each and every staff member, management systems are designed to ensure that any contaminants are not introduced in the first place. System specifications are likely to cover areas as diverse as staff hygiene, the way within which machines are operated, product consistency and quality, safeguards for intellectual property rights, and the security of facilities and computer systems.

At present, numerous off-the-shelf management system standards are available, which have been designed to meet specific business management and compliance objectives. Apart from the ISO 28000 system for supply chain security, other systems include: the ISO 9000 series, focusing on quality; ISO 14001, focusing on the environment; ISO 14064, focusing on greenhouse gas emissions; ISO 22000 focusing on food safety in supply chain operations; and ISO 27001, focusing on IT security. Outside of the ISO standards, OHSAS 18001 applies to the areas of health and safety planning, BS 25999 is the new standard related to business continuity management and PAS 2050, the new carbon footprinting for products specification, has just been launched. Each of these systems are designed to give companies confidence that they meet the set management objectives within the areas for which the systems are designed. Independent, third-party certification provides confidence to others that the certified company meets set system specifications.

The physical manifestation of a management system can take shape in multiple formats. A basic system is likely to consist of a series of manuals which set out specifications for operations, management, and control. The leading principle is a risk identification & risk analysis process, which is regularly reviewed and updated. More sophisticated management systems are often embedded within a company's wider corporate (IT) infrastructure. They are likely to include detailed specifications for management and administrative procedures and are supported by the extensive use of information technology. Where deployed, infrastructure also enables staff, business units, suppliers, and customers to share information and performance or control measures on a real-time basis. For many multinational companies such systems often have

global proportions, covering most theatres of operation and tying-in the majority of their facilities, suppliers, and customers irrespective of national boundaries. The system allows top management to maintain an integral overview of the company's performance against set objectives.

Once the management system has been implemented most companies will choose to engage the services of independent assurance companies. These assurance providers will usually conduct an **initial assessment** and check that systems specifications are met. This is then followed-up by periodic **surveillance visits**. Where management systems are based on international or national standards – such as ISO 9000 for quality or ISO 28000 for supply chain security – companies will most likely ask the assurance provider to certify the management systems. Certificates provide confidence to others (for example, partnered businesses up and down the supply chain or the regulator) that relevant requirements are met. Most of the reputable assurance providers conducting certification seek to become **accredited** by governing official bodies or a government agency such as the United Kingdom's Accreditation Service (UKAS).

In some instances the assurance concept is taken one step further. In the European Union **notified bodies** – officially-approved independent assurance providers – are appointed by the Competent Authority to audit and inspect management systems in order to safeguard compliance with legislatively-defined directives. For example, faulty electrical appliances could be a source of considerable danger to consumers. The role of notified bodies is to assure that goods carrying officially required certificates or marks – such as the European Union's "CE" mark – are compliant with the specifications set by legislation. Other areas where notified bodies are endorsed by regulators to assure compliance with legislation include products as diverse as: pressure vessels, medical devices, toys (to protect children from small parts and toxic materials); furniture (to regulate product flammability and potential for toxic smoke); and spectacle frames, zips, and buttons (to protect wearers from skin contact with toxic nickel in alloys).

Management systems are an essential feature in modern day supply chain management practices. They help bring down costs while ensuring that suppliers meet set requirements. For example, in quality controls the classic management choice lies between inspection and assurance. In a supply chain where every consignment needs to be physically checked for quality defects – for instance, whether a procured car windscreen can be readily assembled into a car body – transaction costs between contracting parties will be very high. However, in a relationship where suppliers and customers work together to raise quality by using a quality control management system (e.g. ISO 9001), the requirement to check each and every delivery is significantly reduced. Rather than inspecting each windscreen, management focus shifts to how production and quality defects are eliminated. The stronger management systems are, the lower the risk of quality breaches and exposure to costly inspection requirements. It is not much of a leap to consider how such a management system can be extended to help tighten-up supply chain security and give governments the confidence that companies are actively managing security within their supply chain. This is the underlying motive that led to the development of ISO 28000.

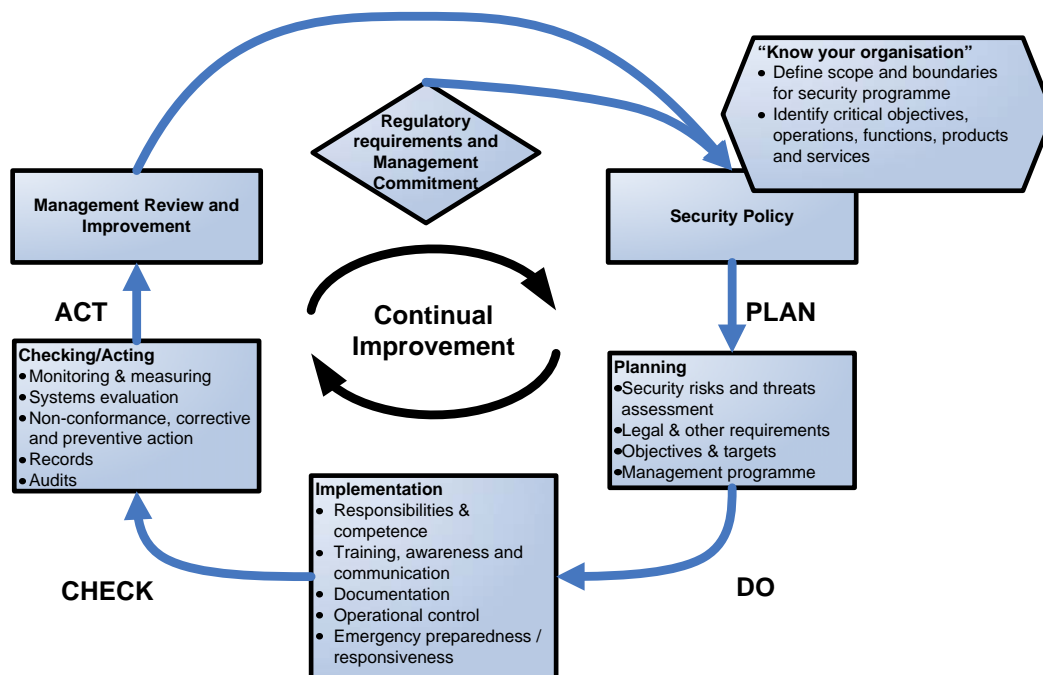
## 4. The ISO 28000 system

ISO 28000:2007 is an international management system standard that specifies the requirements for security management systems. It was developed under the authority of the International Organisation for Standards (ISO) through a close collaboration with relevant stakeholders as a response to growing industrial demand for a security management system standard. ISO 28000 specifications reflect, amongst others, those set by the WCO's SAFE framework, the European Union's Authorised Economic Operator programme (AEO), the USA's Customs-Trade Partnership against Terrorism (C-TPAT), the IMO's International Ship and Port Facility Security (ISPS) Code, and the high-tech industry's Transported Asset Protection Association (TAPA). ISO 28000 is a risk based management system standard which is based on the "Plan-Do-Check-Act" (Figure 2) method safeguarding the organisation's commitment to "continual improvement".

The ISO 28000 management system can be applied to any size or type of organisation that plays a part in supply chain operations, from raw material supply, manufacturing, transport and logistics through to point of sale or end user. ISO 28000 is also able to accommodate sector and activity specific risks. For example, tightly monitored supply chains designed for goods with strategic and military applications or medical use have very different requirements from non-sensitive goods with comparatively lower risk implications. Similarly, intermediaries, such as transport and logistics operators, are likely to have very different security requirements to manufacturers or distributors. Depending on the markets in which the company operates it is likely that users of the ISO 28000 standard will also want to tie-in compliance with other security programmes, such as AEO, C-TPAT, and TAPA.

ISO 28000 begins with the organisation's commitment to authorising a security management policy. This provides the organisation with a framework that enables specific security and management objectives, targets, and programmes to be adhered to. Considering the magnitude of varying operational practices and the number of stakeholders in any organisation, implementation of ISO 28000 is frequently preceded by a review exercise that seeks to establish and document current supply chain management practices and areas of risk – sometimes referred to as a "know your organisation and its environment" review.

Implementation of the security policy normally requires clear communication from senior management on the system's objectives for the entire organisation as well as for the organisation's suppliers and customers. Implementation also entails extensive training, competence building, and awareness programmes. Moreover, successful implementation is dependent on ensuring that key information (such as performance measurement criteria) is communicated and acted upon. This includes organisation-wide awareness of the set management objectives, regulatory requirements, and the consequences resulting from implementation failure.



**Figure 2: The application of Plan-Do-Check-Act principles in ISO 28000**

Once commitment by senior management to the security policy has been achieved, subsequent “**Plan**” activities typically involve: the assessment of risks and regulatory requirements (including a risk management framework); the setting of security objectives and targets; and the development of a management programme. “**Do**” activities address: responsibilities and competence; training; communications; documentation; operational control of identified risks; and emergency preparedness. “**Check**” within the ISO 28000 system involves activities such as: measurement and monitoring; system evaluations; taking corrective or preventive actions in areas of non-conformity; the keeping of records; and periodic systems audits (usually every six months).

Successful implementation of the ISO 28000 system provides a circle of “continual improvement” in which findings from **Plan**, **Do**, and **Check** steps are used to inform actions. Thus, the “**Act**” step encompasses a permanent commitment to reviewing the system’s performance. For example, one review finding might be that the organisation’s exposure to security risks has changed. Subsequently, the organisation’s risk management framework would have to be amended to ensure that the objectives set by the organisation’s security policy continue to be met. However, the “continual improvement” principle also gives rise to fine-tuning the company’s operations and security management – for instance by striving to reduce costs or by setting more ambitious security management and performance objectives.

## 5. Assurance and certification

A key feature in any ISO 28000 system implementation is the use of assurance providers to review systems once they are implemented, conduct periodic audits, and to issue a certificate of compliance. When certifying an ISO 28000 system, assurance providers are required to take a two-stage approach (Figure 3). The **first stage** sets out to identify whether supply chain security risks are identified and accurately assessed, the policies, processes, and procedures set by the ISO 28000 implementation are in place and put into practice. During the stage-one visit, the certifier will also collect information about the company's organisation, processes, and activities. Certifiers will then look at the nature and scale of operations, including how far up or down the supply chain the implementation has taken effect, and where the boundaries of control lie.

In the **second stage** of the certification process, the certifying body looks at how the ISO 28000 management system has been put in place. The assessment team aims to confirm whether or not the implemented policies, processes, and procedures are effective. The guiding audit question at this stage is whether the implemented system is fit for purpose. Areas reviewed also include whether there are any gaps in control and whether implementation objectives have been met. A certificate is issued once the assurance provider is satisfied that all the requirements of stage one and stage two assessments are met. Subsequent to the issuing of the certificate, third party assurance providers are compelled to conduct periodic surveillance visits – usually on a six-monthly basis. Reports on findings are communicated to the appropriate managers. Where the certifiers identify areas of **nonconformity**, companies are obliged to remedy these within a specified time-frame.

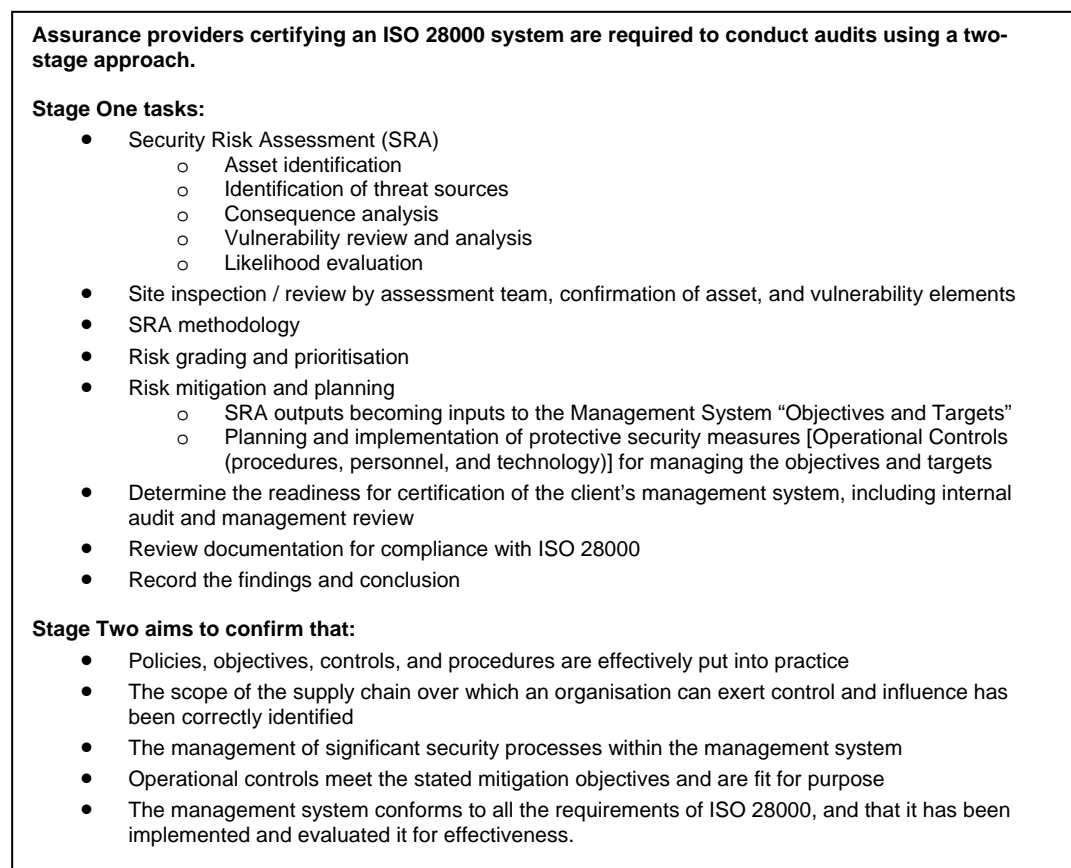
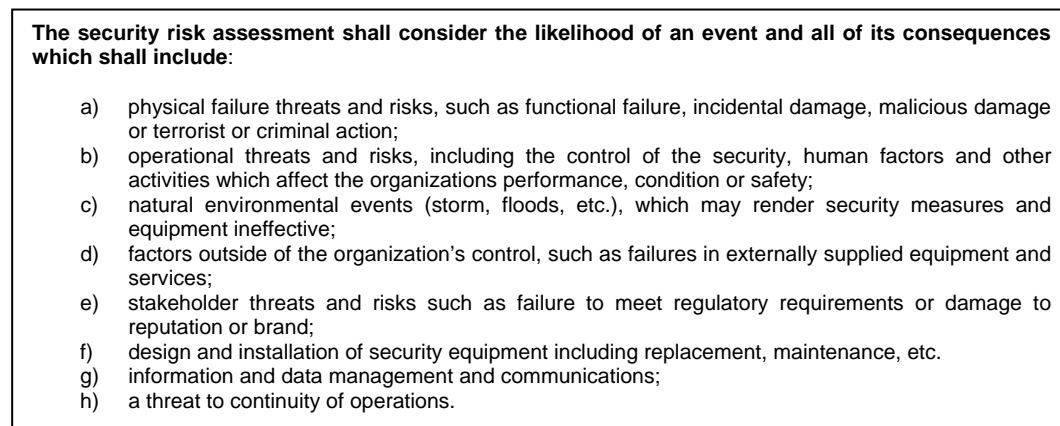


Figure 3: ISO 28000 certification tasks and aims

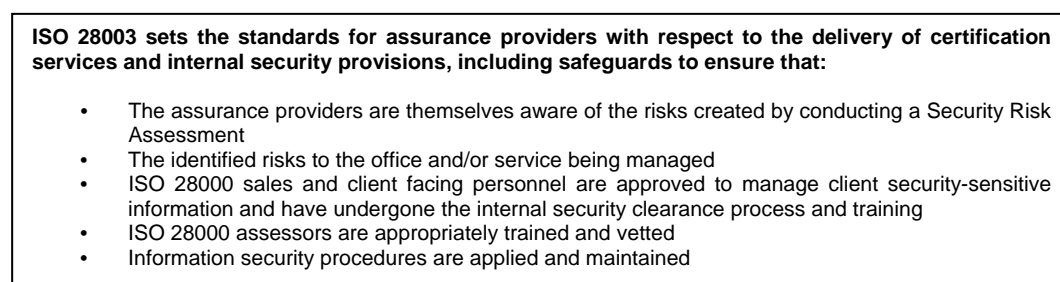
A focal point in any assurance visit is the **security risk assessment (SRA)** in which the assurance provider is required to take into account security objectives and potential sources of risks (Figure 4) as well as how risks are managed by the organisation. For example, a soft-drink

manufacturer will want to make sure that no toxic ingredients – accidentally or on purpose – contaminate its products. Identified risks can thus be sector specific – such as the food and drinks industry – and risks can be activity-related – for instance the person in charge of mixing the ingredients. Certification does not guarantee that contamination of goods will not occur. However, certification does provide assurance that the company has a system in place that recognises sources of threat and has put responsible **risk management** measures in place – such as risk based sampling and random spot checks – to reduce and prevent the risk of contamination from happening.



**Figure 4: ISO 28000 security risk assessment considerations**

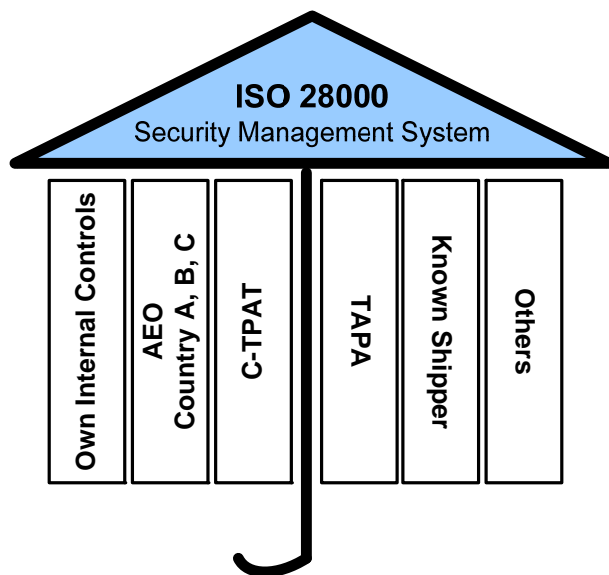
To standardise the method of verification against the international standard and to safeguard the integrity of certificates awarded against it, most reputable assurance providers will seek to be accredited to provide ISO 28000 assessment services. They would achieve this by following the requirements of ISO 28003 'Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems'. This provides a standardised framework of guidelines for certification by assurance providers. It addresses the delivery of certification services, including the assurance provider's integrity, capabilities, and professional competencies. In principle, ISO 28003 provides a framework for public bodies (such as UKAS) to regulate the assurance industry. (Figure 5).



**Figure 5: ISO 28003 provisions**

## 6. Managing supply chain security requirements through ISO 28000

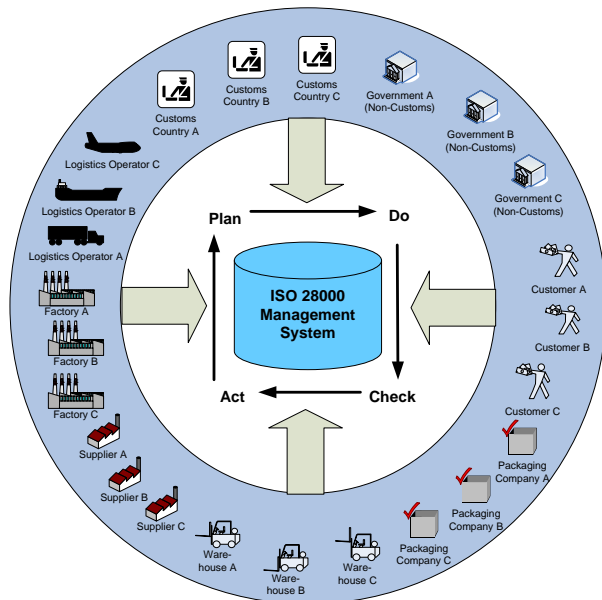
Assurance providers are receiving increasing numbers of enquiries from companies that are considering ISO 28000 implementation and subsequent certification. Their interest is sparked by identifying ISO 28000 as a global security solution that can stand alongside other corporate infrastructure elements (such as accounting, quality, and supply chain relationship systems). Security requirements normally include the implementation of the company's own specific security measures. Amongst others, these are likely to include issues like product integrity and ensuring that goods or assets are not stolen or misappropriated<sup>5</sup>. In addition to the company's own supply chain security requirements, the ISO 28000 management system is also seen as a vehicle to ensure that those security specifications set by the regulator and other external bodies are met. Depending on the organisation's needs, such specifications are likely to include the legislatively-defined security programmes in each of the countries within which the company operates, such as AEO, C-TPAT, TAPA, and the IATA "known shipper" (Figure 6). Thus, ISO 28000 provides a means for managing different regulatory requirements under one single umbrella.



**Figure 6: ISO 28000 as an umbrella system for regulatory compliance.**

By drawing on the company's corporate infrastructure (such as accounting, quality, and supply chain relationship systems), a well-integrated security system can also ensure that relevant information from across the supply chain is always up-to-date and easily accessible (Figure 7). For instance, most organisations with multiple locations use an extensive electronic infrastructure to keep track of operational activities in real-time. This information then feeds into the continual review cycle of supply chain security-related risks and management (following the Plan-Do-Check-Act principles). Reporting infrastructure can also be utilised to generate automatic reports to the relevant regulatory authorities where mandated by legislation or business-government partnership agreements.

<sup>5</sup> For example, spare parts certified for use in aircraft are known to be targets for criminals who seek to replace them with inferior non-certified parts.



**Figure 7: Capturing information across the supply chain**

As outlined earlier, another feature of ISO 28000 is that its security specifications reflect, amongst others, those set by the WCO's SAFE framework, the European Unions' AEO, the USA's C-TPAT, and the IMO's ISPS code. Where companies choose to adopt and implement the ISO 28000 system, they must ensure regulatory requirements and specifications *are met* – as this is a requirement of the Standard (section 4.3.2):

#### 4.3.2 Legal, statutory and other security regulatory requirements

The organization shall establish, implement and maintain a procedure

- a) to identify and have access to the applicable legal requirements and other requirements to which the organization subscribes related to its security threat and risks, and
- b) to determine how these requirements apply to its security threats and risks.

The organization shall keep this information up-to-date. It shall communicate relevant information on legal and other requirements to its employees and other relevant third parties including contractors.

Text extract from ISO 28000: 2007

As such, ISO 28000 can therefore be seen as a means of ensuring relevant security programmes to which the organisation subscribes are complied with, i.e. C-TPAT or AEO.

Moreover, if the ISO 28000 solution is integrated or linked with other corporate infrastructure and management procedures, the effort involved in managing regulatory compliance can be significantly reduced. To give one example of this, Figure 8 sets out the European Union's AEO (Security) case. The left column of Figure 7 lists the components that are evaluated by customs administrations when granting the AEO status. Components include: 1) information about the company seeking AEO status; 2) the record of compliance with customs procedures; 3) the quality of record keeping, including commercial and logistics operations; 4) proven financial solvency; and 5) the enforcement of appropriate security and safety standards. While point 5 is fully covered by ISO 28000 security specification, compliance with the remaining AEO components is dependent on consolidating information from the wider corporate infrastructure.

Thus, full compliance with AEO criteria is dependent on the company's security management system's ability to interface with the organisation's wider corporate infrastructure. As outlined in the right column of Figure 8, supporting infrastructure that needs to be linked to the ISO 28000 management system include: accounting and finance systems, customs management systems, quality control systems, relationship management systems, customs warehousing systems, audit reports from accountants and IT systems auditors, credit reports, and professional development and training systems.

Components of AEO Authorisation	Supporting systems, procedures and corporate infrastructure
<b>1. Company Information, including:</b> <ul style="list-style-type: none"> <li>⇒ Annual turnover, profit and losses</li> <li>⇒ Stock capacity</li> <li>⇒ Foreign trade and purchases</li> <li>⇒ Goods received in customs warehouses</li> <li>⇒ Goods used in production</li> <li>⇒ Sales</li> </ul>	<ul style="list-style-type: none"> <li>⇒ Accounting and finance systems</li> <li>⇒ Customs management systems</li> <li>⇒ Customs warehousing systems</li> <li>⇒ Quality controls systems (e.g. ISO 9001)</li> <li>⇒ Relationship (supply chain) management systems</li> </ul>
<b>2. Compliance history, including:</b> <ul style="list-style-type: none"> <li>⇒ Customs transactions</li> <li>⇒ Customs authorisations</li> <li>⇒ Declarations</li> <li>⇒ Irregularities</li> </ul>	<ul style="list-style-type: none"> <li>⇒ Customs management systems</li> <li>⇒ Customs warehousing systems</li> <li>⇒ Relationship (supply chain) management systems – where logistics is managed by third parties</li> <li>⇒ Accounting and finance systems</li> </ul>
<b>3. Accounting and logistics systems, including:</b> <ul style="list-style-type: none"> <li>⇒ Quality of accounting records and systems</li> <li>⇒ Access, quality and documentation of electronic systems and data</li> <li>⇒ Internal control systems and procedures</li> <li>⇒ Management of the supply chain, including the movement, production and storage of goods</li> <li>⇒ Record keeping and data management</li> <li>⇒ Back-up, recovery, fall-back and archival options</li> <li>⇒ Information Security</li> </ul>	<ul style="list-style-type: none"> <li>⇒ Verification, assessment and certification by an independent quality assurance provider</li> <li>⇒ Audits by accountants and tax advisors</li> <li>⇒ Reviews and audits by systems and IT specialists and systems auditors</li> <li>⇒ Professional development and training systems</li> <li>⇒ Elements of the ISO 9001 management systems</li> <li>⇒ Elements of ISO 28000</li> </ul>
<b>4. Financial Solvency</b>	<ul style="list-style-type: none"> <li>⇒ Accounting and finance systems</li> <li>⇒ Credit reports</li> <li>⇒ Due diligence checks</li> </ul>
<b>5. Safety and security, including:</b> <ul style="list-style-type: none"> <li>⇒ Self assessment</li> <li>⇒ Entry and access to premises</li> <li>⇒ Cargo security</li> <li>⇒ Logistical processing</li> <li>⇒ Supervision and control of transport operations (incoming and outgoing goods)</li> <li>⇒ Storage, production and loading of goods</li> <li>⇒ Security of business partners</li> <li>⇒ Personnel security</li> <li>⇒ Security training</li> </ul>	<ul style="list-style-type: none"> <li>⇒ Covered in full by ISO 28000 specifications, drawing in wider corporate infrastructure where applicable</li> <li>⇒ Elements of ISO 9001</li> </ul>

**Figure 8: AEO authorisation and supporting infrastructure**

## 7. Business and government drivers

Although the ISO 28000 management system is still relatively new, there are a number of compelling business and policy drivers for its implementation by businesses. These deserve further consideration. Primary business objectives tend to vary from organisation to organisation, but usually include the desire to secure market share, improve competitiveness, safeguard returns on capital deployed, reduce costs, and increase value in the hands of the customer. Subsequent supply chain security objectives thus include: regulatory compliance; uninterrupted operations; increased protection and security of assets, goods, and products; enhanced value for end-customers (those that have specific security requirements); efficient and effective control procedures; as well as the development or protection of competitive advantages – especially where security measures are associated with commercial incentives such as reduced interference from government executives or lower insurance premiums.

To recap, the considerable number of security-related controls and procedures has already been highlighted within this paper in Section 1. As shown in Figure 1, it is easy to count more than 30 initiatives with security compliance elements. Direct compliance costs with each of these initiatives take form in the costs of managing systems, collecting information, and making declarations. There are also indirect cost elements which are associated with foregone business opportunities and reduced competitiveness, especially where failure to comply leads to operational disruptions. Although compliance costs without extensive regulatory reform are unlikely to be eliminated, tying all security compliance needs and regulatory scheme requirements into one management system – such as ISO 28000 – can yield synergies and economies of scale which can reduce the direct costs to compliance burden.

The use of a robust security management system encompassing regulatory compliance operations can also ensure that conformity breaches are minimised, effectively reducing exposure to the indirect cost of compliance. Further benefits might be found where the security management system includes compliance operations with security procedures that confer preferential treatment – such as the EU's AEO status or C-TPAT. Preferential treatment might include fast-track customs clearance, lower risk scorings and exposure to physical inspections, and access to customs simplified procedures<sup>6</sup>.

Another business driver for investment into a security management system such as ISO 28000 is the desire to increase the protection and security of assets, goods, people and products. This is likely to be of specific concern to businesses that are particularly exposed to criminal elements or work in high-risk environments. Beyond regulatory compliance, as outlined in Section 4, the Plan-Do-Check-Act principles underlying ISO 28000 provide a means to actively take control of risk mitigation and reduce it through continual improvement. Commercial benefits will vary from company to company, but are likely to include a reduction in pilferage and reduced misuse of company resources.

For some companies, compliance with set security provisions might also be a conditional term in commercial contracts. For instance, a company manufacturing high value or sensitive goods – such as consumer electronics or pharmaceuticals – is likely to pose strict security specifications upon its logistics service providers. If this logistics service provider has a robust system in place that accommodates these specifications, it will have a competitive edge over rival logistics service providers.

Some anecdotal evidence also suggests that insurance premiums can be significantly reduced where underwriters are satisfied that management systems help to reduce the volume of claims and exposure to risk. Therefore the existence of a certified security management system such as ISO 28000 may be viewed favourably by underwriters.

---

<sup>6</sup> In most countries access to customs simplified procedures (for instance inland clearance) is conditional on some form of authorisation. Security considerations – often linked to deposits or bonds – play a significant role when granting these authorisations.

There are also a range of intangible business benefits that can stimulate investment into security management systems. These will be unique to each and every company. However, one consistent theme is the company's desire to put procedures in place that can minimise exposure to public or shareholder repercussions, for instance where a company inadvertently aids terrorist or criminal activity. A robust security management system like ISO 28000 provides a framework that minimises exposure to such risk and subsequent repercussions. A related business driver is the desire to establish an audit trail of all security-related activities. This can have significant value in events where security performance is under dispute – be it by partnering companies up and down the supply chain, insurance companies, or by the regulator.

Another theme amongst intangible business drivers is the ISO 28000 system's ability to incorporate new regulatory requirements. Political pressures to regulate and public perception of risks constantly changes. Subsequently it is conceivable that regulators might decide to introduce emergency measures at short notice. Companies that have a functioning security management system are better positioned to respond to such rapid changes in the regulatory environment than those that do not. Potentially this ability can provide a significant competitive advantage.

### **Government drivers**

Governments' desire to enhance supply chain security can be equally diverse. Security is a fundamental public good, essential for prosperity and stability in any society. Policy makers are faced with the challenge of carefully balancing public and political demands for tighter security (bearing in mind the perceived ongoing threat from terrorists) against available resources, the capabilities of government executive agencies, and the potentially disruptive impacts of becoming overly heavy handed (or prescriptive) in enforcing security-related controls. Adding to their challenge are ever-rising volumes in goods traded and the trend for global procurement and outsourcing initiatives<sup>6</sup>

To this end executive agencies are required to rethink traditional inspection-based methods. Risk management and partnership are key themes in security initiatives that are based on the WCO's SAFE Framework. They are also key features in programmes like the European Union's AEO and the USA's C-TPAT. The underlying idea is to provide incentives to trustworthy and low-risk traders and refocus resources to target high-risk areas. As outlined above, good security programmes create an incentive for businesses to actively manage security objectives and reduce their risk scores. As long as government executive agencies have the capacity to differentiate and give incentives to traders who perform well, businesses have an incentive to make investments into the security area. In the long-term, once a significant number of businesses choose to tighten-up their internal controls, government resource savings ought to materialise.

A further government benefit from business investments into systems like ISO 28000 is that security-related issues become an active feature in supply chain management. Companies are usually very aware of where risks within their own operations lie. Management systems such as ISO 28000 enable them to apply a bespoke control regime. This is likely to be considerably more effective than any arms-length inspection arrangement. Moreover, unlike government executive agencies, companies can enforce their security objectives system-wide and irrespective of national borders. Subsequently, control objectives are less limited by national sovereignty issues.

## 8. Benefits conferred by using the services of assurance providers

The use of independent assurance providers to verify, assess, and certify ISO 28000 management systems can confer a range of additional benefits that extend beyond those described in Section 7. As outlined in Sections 4 and 5, assurance providers are primarily engaged to conduct system audits and to provide external verification through certification. They may also be employed at the pre-implementation stage to conduct a gap analysis and help companies identify areas that can benefit from improvements. However, reputable assurance providers subscribing to ISO 28003 do not provide consulting services that directly relate to the implementation of ISO 28000 systems as this can easily lead to conflicts of interest and undermine the integrity of ISO 28000 certificates.

Independent verification by a trusted assurance provider helps give confidence to managers that their procedures and operations match set objectives. Moreover, certification provides confidence to others that the audited company actively manages its security requirements. This aspect is of significance where companies share responsibilities for supply chain operations and each member within the supply chain needs to have confidence in others doing “their bit”. Another benefit of note is that audit reports and recommendations can provide businesses with valuable external feedback that highlight areas where improvements can be made or where areas of risk remain. This allows organisations to make informed decisions about their security policies and help prioritise management resources.

Independent certification also provides a vehicle for businesses to show regulators that they have robust security management systems in place. The regulator’s confidence in the company’s ability of actively managing security can potentially lead to lower risk scores, hence a more light-handed approach in regulatory enforcement. Certificates by independent assurance providers can be a useful instrument in securing that confidence. The value of certificates issued by assurance providers can be particularly high in countries where it confers exemptions from regulatory requirements or is viewed as equivalent with official authorisations. At present, ISO 28000 does not have that status; though feedback gained from customs officers who have shadowed assurance companies is favourable.

Provisions within the EU customs legislation are also favourable towards recognising ISO 28000 certificates as supporting evidence in an AEO application. For example, the EU’s Customs Regulation’s Implementing Provisions (2454/93/EEC, as amended) implies that where the criteria for issuing ISO 28000 certificates are identical or correspond to those laid down in customs legislation, they may be taken as equivalent. Moreover, the regulation also states that issuing customs authorities may accept conclusions provided by an expert (such as an independent assurance provider) (Figure 9).

Article 14k(4): “If the applicant, established in the Community, is the holder of an internationally recognised security and/or safety certificate issued on the basis of international conventions, of a security and/or safety certificate issued on the basis of Community legislation, of an International Standard of the International Organisation for Standardisation, or of a European Standard of the European Standards Organisation, the criteria provided for in paragraph 1[setting out security and safety conditions] shall be deemed to be met to the extent that the criteria for issuing these certificates are identical or correspond to those laid down in this Regulation”.

Article 14n(2): “The issuing customs authority may accept conclusions provided by an expert in the relevant fields referred to in Articles 14i, 14j and 14k in respect of the conditions and criteria referred to in those Articles respectively. The expert shall not be related to the applicant”.

**Figure 9: Extract from the European Union’s Customs Regulation Implementing Provisions (2454/93/EEC, as amended)**

Official recognition of ISO 28000 certificates could confer a number of benefits to government executive agencies. The most significant one would be the considerable resource savings resulting from recognising ISO 28000 as equivalent to official security authorisations. For government agencies keeping tight regulatory controls on the assurance industry is less resource intensive than checking-up on each and every business that seeks security authorisation. But even where ISO 28000 is not recognised in full, the acceptance of ISO 28000 certificates as supporting evidence means that bodies such as customs could choose to relax some of the rigor when processing applications and issuing authorisations.

Unlike most government executive agencies, assurance companies have existing relationships with their clients (e.g. gained through ISO 9000 or similar assurance visits). Consequently, they are intimately familiar with their client's corporate infrastructure. Such detailed knowledge of a company can significantly reduce the time and effort required to conduct assurance operations. Official bodies in a traditional arms-length relationship are unlikely to have the capacity or capability to get involved with the organisation at such a level of detail.

Moreover, assurance companies are not restricted by national borders. This is important where companies operate global supply chains; such organisations are likely to use one management system irrespective of location. Unlike government agencies, assurance companies can examine the management system and thereby the supply chain in its entirety. ISO 28000's inbuilt 'continuous improvement' also ensures that regulatory compliance is not aimed at meeting the lowest common denominator prevalent in 'one-size-fits-all' and check-list type regulatory approaches. As such, it is likely to prove superior in terms of security when compared to the practice of simply collating self-declarations that underlie some of the newly introduced security regimes.

Recognition of ISO 28000 certificates as equivalent to official certificates can also reduce the regulatory burden suffered by business. As outlined in Sections 4 and 6, most businesses are familiar in managing their operations through the use of management systems. Transaction costs between the business and the regulator are likely to be minimised in instances where evidence of ISO 28000 certification is sufficient for proving regulatory compliance. In contrast, transaction costs between the business and the regulator will be significantly higher where compliance specifications require detailed reporting (or declarations) for every type of business activity.

## **9. Conclusion**

This paper has covered a lot of ground, setting out the supply chain security environment and its regulatory challenges, the use of management systems to implement company objectives, and the ISO 28000 system to meet supply chain security requirements. This paper has also looked at the role played by assurance providers in ISO 28000 certification as well as set out how businesses can use ISO 28000 when managing their security requirements. This is followed by an overview of drivers that push businesses and government administrations towards ISO 28000 as well as the benefits derived from using independent assurance providers.

A number of issues are highlighted. Businesses face an avalanche of supply chain security initiatives for which they need to devise management systems. ISO 28000 is a standardised system designed to help businesses take managerial control over their security requirements, providing them with tools to actively reduce security risks, and tighten up their performance. The ISO 28000 system is also suited for tying-in regulatory compliance and thus offers a vehicle to ensure that regulatory requirements – in addition to the company's own requirements – are fully met. The Plan-Do-Check-Act principle ensures that identified risks and procedures are continuously reviewed.

Independent assurance and certification provides confidence to management as well as to others that the ISO 28000 system meets the requirements for which it has been implemented. Many business drivers have stimulated interest in the ISO 28000 system. Among others, these include: regulatory compliance; uninterrupted operations; increased protection and security of assets, goods, people and products; enhanced value for end-customers (those that have specific security requirements); efficient and effective control procedures; as well as the development or protection of competitive advantages.

The desire to actively manage and increase supply chain security also matches policy objectives that underlie many of the more recent security programmes sponsored by government organisations – such as those falling under the WCO’s SAFE framework. Independent third-party certification enables businesses to show regulators that they have robust security management systems in place. At present, ISO 28000 does not have any official recognition, though this might change as regulators become more familiar and confident with ISO 28000 and how businesses use management systems. To safeguard the ISO 28000 standard and the value of certificates, ISO 28003 can provide a basis for regulating assurance providers (through accreditation by official bodies like, UKAS).

Management systems can be tailored to suit business needs and to target the company’s specific sources of risk. Such an approach promises a significant reduction in transaction costs between business and government as well as help tighten-up overall security. One further advantage is that unlike regulatory authorities, assurance providers are not bound by national jurisdictions and can take a global view towards a specific company’s exposure to security risks and implemented security measures.

Although ISO 28000 standard is still relatively young, LRQA believes that it provides a powerful and flexible tool for businesses to manage their own security requirements. Assurance and certification provides confidence in the system. When recognised by authorities, ISO 28000 will serve as a tool to reduce regulatory complexity within the area of supply chain security as well as reduce overall security risks.

The assurance principle is tried and tested and based on years of experience. Adopting the principle of underpinning an organisation’s security needs and objectives by integrating them into a management system specifically designed to continually address those requirements, would seem to make logical sense.



**Lloyd’s Register Quality Assurance Ltd.**

Hiramford, Middlemarch Office Village, Siskin Drive, Coventry CV3 4FJ, United Kingdom

**Lloyd’s Register Quality Assurance is a member of the Lloyd’s Register Group**

Copyright 2009. Lloyd’s Register Quality Assurance Ltd. All rights reserved



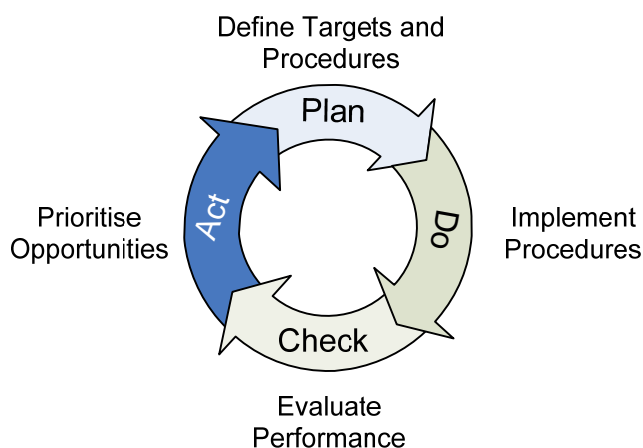
**LIFE MATTERS**

# Annex 1

## Plan-Do-Check-Act:

### The four cornerstones in ISO management systems

Robust management systems are based on the “**Plan – Do – Check – Act**” principle, which underpins any ISO management system standard (Figure 1). The “Plan – Do – Check – Act” principle provides businesses with a vehicle to better understand their own operations and supply chain management practices, set management objectives (including regulatory compliance), identify scope for improvement (for example, tighter security and better performance), and reduce costs.



**Figure 1: The “Plan–Do–Check–Act” principles**

The “**Plan**” step, described at its most basic, is about defining targets and procedures to meet set management objectives – such as tightened security and regulatory compliance within an ISO 28000 management system. Given the complexity of relationships and practices in most supply chains, the “Plan” step often starts with the mapping of existing business processes, supply chain linkages, and operational practices. “Plan” tasks, tools, and components underpinning any management system will typically include the following:

- A preliminary gap and risk analysis to review existing operational and management practices as well as to identify system requirements and management objectives
- Flowcharts drawn out to describe the step-by-step progression of a product as it moves through the organisation as well as interactions with suppliers and customers
- A management team assigned to critically evaluate whether and how system-wide improvements can be found and implemented
- A list of management priorities, applying the 80/20 rule for quick wins and best focus of resources
- An evaluation matrix to help measure performance and provide a benchmark for improvements
- Cause and effect diagrams drawn to help analyse reasons why problems occur and develop remedies

The “**Do**” step, described at its most basic is about implementing procedures to meet the set management objectives. “Do” tools underpinning any management system are likely to include:

- Training – on the job or through external providers – to ensure specified system requirements are understood and applied
- Pilot projects and experiments designed to test whether pre-designed systems deliver the expected outcome and whether they require any further tweaking
- The employment of “champions” and team leaders to provide staff running operations with instant support and make changes where the management system needs to be improved
- Conflict resolution mechanisms to help resolve issues between teams and entities up and down the supply chain as conflicting or competing interests are frequently at work

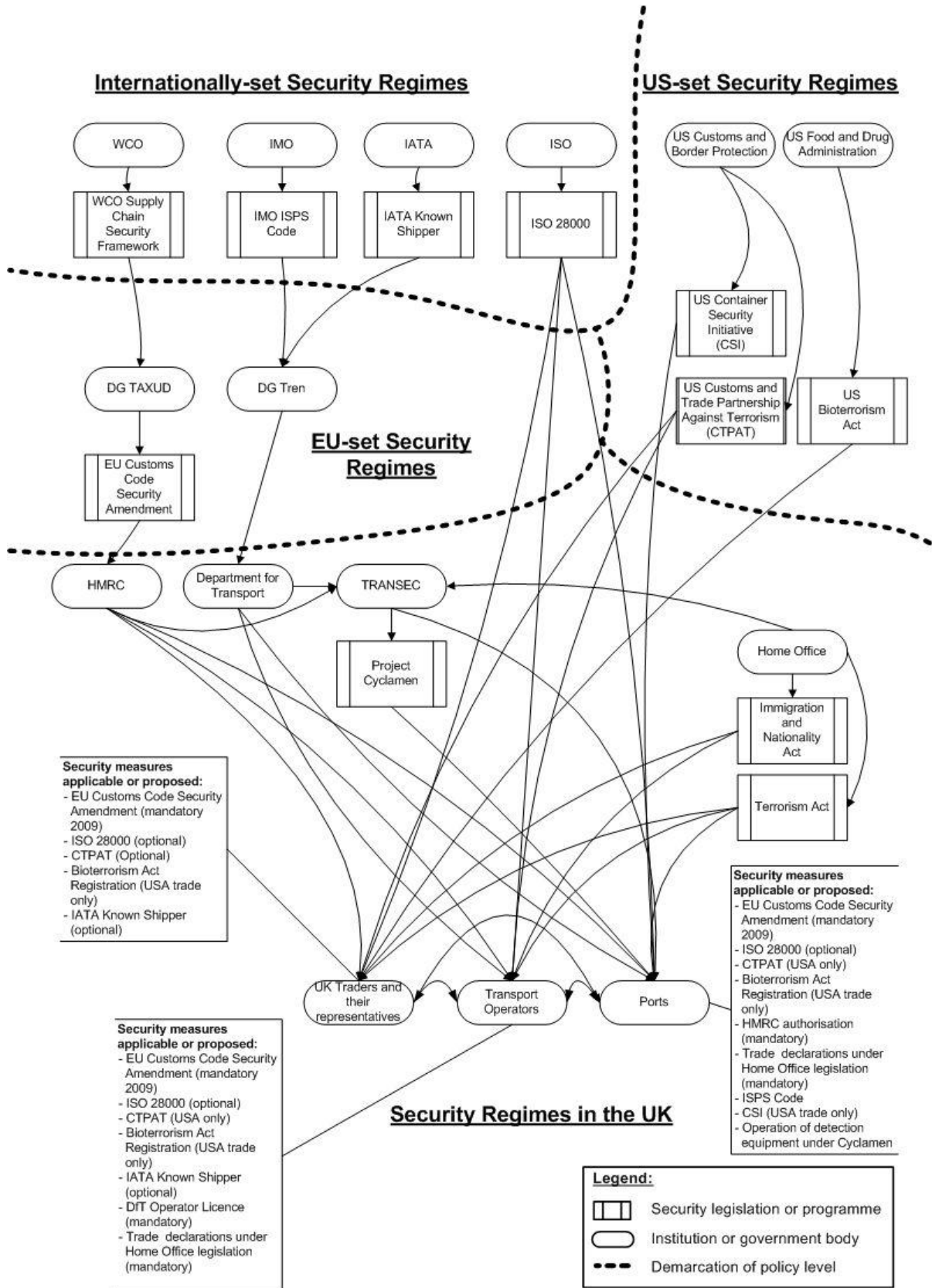
The “**Check**” step, described at its most basic is about evaluating the performance of the management system. “Check” tools are likely to include:

- Data worksheets to track important outputs from any supply chain or process
- Control charts to measure data and assess whether performance is consistent
- Key Performance Indicators (KPIs) and benchmarks used to measure factors that directly or indirectly influence the effectiveness of the process
- Graphs which plot process results over time as well as highlight any changes

The “**Act**” step, described at its most basic, is about acting on what has been discovered in previous steps and prioritise areas for improvement. As such, the Plan-Do-Check-Act principle ensures a virtuous circle of continuous improvement. “Act” features are likely to include:

- Process maps setting out (for all to see) how processes fit together
- Process standardisation to ensure that the processes within the system become comparable
- Formal training to ensure that everyone across the supply chain meets the specifications set by the management system.

# Annex 2 - Security Spaghetti - An illustrative example



Grainger, "Supply chain security: adding to a complex operational and institutional environment"  
 World Customs Journal, Volume 1, Number 2, September 2007