The International Shippers and Freight Forwarders Security Code – DRAFT Rev .4
(Security-management Systems for the supply chain)

SOURCE: DNV
STATUS: Draft Rev.4
ACTION: For discussion at the 29-30 September 2003, ITPWG agenda, item 3
## Contents

1. **SCOPE** ................................................................................................................................. 5
   1.1. **GENERAL** ......................................................................................................................... 5
   1.2. **APPLICATION** .................................................................................................................... 5
   1.3. **EXCLUSION** ....................................................................................................................... 5

2. **NORMATIVE REFERENCE** .................................................................................................... 6

3. **TERMS AND DEFINITIONS** ................................................................................................. 6

4. **SECURITY-MANAGEMENT SYSTEM** .................................................................................. 9
   4.1. **GENERAL SYSTEM REQUIREMENTS** ................................................................................ 9
   4.2. **DOCUMENTATION REQUIREMENTS** ................................................................................ 9
   4.2.1. **General** .......................................................................................................................... 9
   4.2.2. **Security Manual** ........................................................................................................... 10
   4.2.3. **Control of documents** ................................................................................................ 10
   4.2.4. **Control of Records** .................................................................................................... 10
   4.3. **MANAGEMENT RESPONSIBILITY** .................................................................................. 10
   4.3.1. **Management commitment** ............................................................................................. 10
   4.3.2. **Security levels** ............................................................................................................. 11
   4.3.3. **Security Policy** ........................................................................................................... 11
   4.3.4. **Security Assessment** ..................................................................................................... 11
   4.4. **ORGANIZATION AND COMMUNICATION** ....................................................................... 12
   4.4.1. **Responsibility and authority** .......................................................................................... 12
   4.4.2. **Company Security Officer** ............................................................................................ 12
   4.4.2.1. **Internal communication** ............................................................................................ 12
   4.4.2.2. **External Communication** ........................................................................................... 12

5. **SECURITY-MANAGEMENT** .................................................................................................. 12
   5.1. **GENERAL REQUIREMENTS** ........................................................................................... 12
   5.1.1. **Procedural security** ......................................................................................................... 12
   5.1.2. **Human Resources** ......................................................................................................... 13
   5.1.3. **Physical Security** ......................................................................................................... 14
   5.1.4. **Information Security** .................................................................................................... 14
   5.2. **SPECIFIC REQUIREMENTS TO STUFFERS AND PACKERS** .................................................. 14
   5.2.1. **Procedural security** ......................................................................................................... 14
   5.2.1.4. **Emergency response measures are defined** .................................................................. 15
   5.2.2. **Physical security** ......................................................................................................... 15
   5.2.3. **Access Controls** ............................................................................................................ 16
   5.3. **SPECIFIC REQUIREMENTS TO WAREHOUSES, STORAGE AREAS AND TERMINALS** .......... 16
   5.3.1. **Procedural security** ......................................................................................................... 16
   5.3.2. **Physical security** ......................................................................................................... 17
   5.3.3. **Access Controls** ............................................................................................................ 17
   5.4. **SPECIFIC REQUIREMENTS TO FORWARDERS AND TRANSPORTERS** ............................. 18
   5.4.1. **Procedural security** ......................................................................................................... 18
   5.4.2. **Physical security** ......................................................................................................... 18
   5.5. **SPECIFIC REQUIREMENTS TO INFORMATION PROCESSORS** ........................................ 19
   5.5.1. **Procedural security** ......................................................................................................... 19
   5.5.2. **Access Controls** ............................................................................................................ 19

6. **MEASUREMENT, ANALYSES AND IMPROVEMENT** .............................................................. 20
   6.1. **GENERAL** ....................................................................................................................... 20
   6.2. **INTERNAL AUDITS** ......................................................................................................... 20
   6.3. **MEASURING AND MONITORING** .................................................................................... 21
   6.4. **CORRECTIVE AND PREVENTIVE ACTION** ..................................................................... 21
   6.4.1. **Corrective action** .......................................................................................................... 21
   6.4.2. **Preventive action** ........................................................................................................... 21
   6.5. **SECURITY RECORDS** ....................................................................................................... 21
   6.6. **MANAGEMENT REVIEWS** ............................................................................................... 22
   6.6.1. **General** ......................................................................................................................... 22
   6.6.2. **Review of the Security-management System** .................................................................. 22
   6.7. **CONTINUAL IMPROVEMENT** ........................................................................................... 22
Introduction

0.1 Overview

As concern grows that combating security threats is becoming more and more important to countries, the logistic world is gaining an increasing awareness that:

- not only elements of the logistic chain can be used by terrorists to cause direct harm to life, property or the environment,
- also direct terrorist intervention in the international supply chain could create serious delays in the supply chain and hence cause considerable economic damage,
- and increased security in the supply chain will reduce other losses like theft and damage.

Whereas a number of unilateral or sectoral initiatives have been implemented or are under development to improve the security of (parts of) the supply chain this Code intends to provide a more holistic approach to supply chain security whilst maintaining the efficiency of world trade and the achievements in trade facilitation.

This Code defines auditable requirements to security-management and the security of an organisation’s premises, and is applicable to each step of the supply chain. The Code covers on a generic basis current national regulations and guidelines like C-TPAT, StairSec® etc.

Port facilities and ships, as defined in the International Ships and Port Facilities Code (ISPS-Code), part A and B, together with the revised and amended Chapter XI of the SOLAS 74 convention, are excluded since security requirements for these steps of the supply chain are already well defined herein.

Achieving sound security performance requires organisational commitment to a systematic approach and to the continuous improvement of the Security-management System.

The general purpose of this Code is to provide assistance to organizations implementing or improving a Security-management System. In addition this Code is a document, open for public distribution, which contains requirements to which an organization may be audited for certification/authorization purposes or for self assessment purposes.

In addition this Code contains in Annex A examples, descriptions, options and checklists that aid in the assessment of an SMS, which is a document that is to be treated as confidential at all times and shall not be distributed outside the organisation of customs, other national authorities charged with supply chain security or other recognised independent 3rd party certification bodies.

A Security-management System provides order and consistency for organizations to address security concerns through the allocation of resources, assignment of responsibilities, ongoing evaluation of practices, procedures and processes, and active utilisation of inputs from security authorities and other stakeholders in the supply chain.

Therefore the development and maintenance of a Security-management System is an ongoing and interactive process.

Security-management is an integral part of an organisation’s overall management system. The structure, responsibilities, practices, procedures, processes, practical measures and resources for implementing security policies, objectives and targets can be coordinated with existing efforts in other areas (e.g. operations, finance, quality, occupational health and safety, environmental care)

Key principles for managers implementing or enhancing a Security-management System include, but are not limited to, the following.

- Recognise that security-management is among the highest corporate priorities.
- Establish and maintain communication with internal and external interested parties
- Determining and meeting the legislative requirements towards security further down the supply chain.
- Develop management and employee commitment to security, with clear assignments of accountability and responsibility.
- Provide appropriate and sufficient resources, including training, to achieve the required security levels.
- Establish a management process to audit and review the Security-management System and to identify opportunities for improvement of the system.
- Encourage contractors and suppliers to establish their own Security-management System.
Organizations can consider the following different uses of this Code.

- To obtain authorization, through certification by its national custom organisation, to supervise its own security activities as part of their trusted trader agreement, upon which cargo, processed by such organisation is considered cargo with a reduced risk by customs.

- To obtain authorization, through certification by an independent third party which has been duly authorised by its custom organisation or other authority, designated with security enforcement, to supervise its own security activities as part of their trusted trader agreement, through which cargo, processed by such organisation is considered cargo with a reduced risk by customs;

- Use this Code in contractual agreements with partners, contactors or suppliers to achieve a supply secure chain from door to door.

- To initiate or improve its Security-management System

This Code can be used by organizations of any size and dealing with any part of the supply chain.

Where it is recognised that there are significant differences between the different actors in the supply chain this Code is defining generic requirements to the handing and transportation of closed Cargo Transportation Units (CTU’s) only and is explicitly excluding port facilities and vessels, which are covered already by the ISPS-Code.

The Code defines:

i. General requirements, applicable to all companies. In addition it defines

ii. Specific requirements to Stuffers and Packers, applicable to companies which are engaged in the stuffing, stowing or packing of CTU’s or the (re)consolidation of LCL-cargo into one CTU.

iii. Specific requirements to Warehouses, Storage Areas and Terminals, applicable to companies which are engaged in the storage of cargo or CTU’s in warehouses, stores, depots, terminals etc.

iv. Specific requirements to Forwarders and Transporters, applicable to companies which are engaged in the transportation of CTU’s by road, rail or inland waterway.

v. Specific requirements to Information Processors, applicable to companies which are engaged in generating, processing, forwarding and storage of documents and data about cargo moving along the supply chain.

It is possible that specialised companies, due to their type of operation, only need to meet one specific set of requirements. However, most companies need to meet two or more of these specific sets of requirements, depending the type of their operation.

- Manufacturers would typically need to comply with specific requirements under i., ii. and iv. above.
- Integrated operators with i., ii. iii. and iv. above,
- Whilst e.g. agents and brokers would only need to comply to the requirements under iv above.

0.2 Compatibility with other management systems

This Code has been aligned as nearly as possible with ISO 9001: 2000 and ISO 14001:1996 in order to enhance the compatibility of the Code with these two standards for the benefit of the user community.

This Code is also aligned with the requirements from the ISPS-Code to create a seamless interface between the different steps in the supply chain.
This Code does not include requirements specific to other management systems, such as those particular to quality management, environmental management, occupational health and safety management, financial management or risk management. However, this International Standard enables an organization to harmonize or integrate its own quality management system with related management system requirements. It is possible for an organization to adapt its existing management system(s) in order to establish a Security-management System that complies with the requirements of this Code.

0.3 Appendixes to this Code

To this International Shippers and Freight Forwarders Security Code (ISFFS-Code) the following appendixes are attached:

Appendix A: ISFFS-Code: Guidelines and Checklists (confidential) \textit{To be developed}

Appendix B: General requirements for bodies operating assessment and certification of Security-management Systems which comply with the ISFFS-Code

Appendix C: Requirements to ISFFS-Code auditors.
1. Scope

1.1. General

This Code specifies requirements for the development and implementation of security-management systems, where an organization, being an integrated part of the supply chain, possibly in coordination with other management systems:

- wishes to demonstrate through certification to its clients, its supply chain partners or to the authorities, responsible for supply chain security, its ability to keep the supply chain free from security breach
- wishes to obtain authorization from its customs organization, or other authorities, responsible for supply chain security, where needed through certification by an authorized independent third party, to perform verifications, checks and other measures which ensure that its cargo is free and remains free from security breach, as part of a trusted trader partnership
- wishes to use the requirements from the Code as a voluntary, internal management tool to develop, implement or improve its Security-management System.

1.2. Application

This Code contains requirements to the security of cargo, being it general cargo, dry or wet bulk, which is entered into and transported along the supply chain in closed Cargo Transportation Units (CTU;s) such as containers and closed road- or rail vehicles, which are transported by road, rail or inland waterways\(^1\).

Security of cargo includes the security of data about that cargo.

The first part of chapter 5 of this Code defines requirements which are generic and are intended to be applicable to all organizations, regardless of type, size and services provided.

The second part of chapter 5 of this Code contains specific requirements for the security of each of the four fundamental process steps of the supply chain i.e.:

- Stuffers and Packers
- Wharehouses, Storage Areas and Terminals.
- Forwarders and Transporters
- Information Processors.

1.3. Exclusion

Although this Code describes requirements to security management of all steps in the supply chain, from original shipper to final addressee, the Code does not apply to storage and handling of CTU’s in the perimeter of port facilities and on board passenger vessels, cargo vessels > 500 gross ton, high speed craft and mobile offshore rigs, since the security-management of these parts of the supply chain are adequately covered through the compulsory implementation of the International Ships and Port Facilities Code (ISPS-Code), part A and B, together with a revision and amendment of Chapter XI of the SOLAS 74 convention.

\(^1\) Transportation of closed CTU’s by inland waterways may also cover (short-) sea transport of closed CTU’s by vessels, not covered by Chapter XI of the SOLAS 74 convention and the ISPS-Code.
2. Normative Reference

Although this Code addresses supply chain security as a separate issue, it is based on the same management system fundamentals as described in ISO 9000:2000 and on which, ISO 9001:2000 and ISO 14001:1996 are based.

The Code complies with the principles set out in the “High level guidelines for co-operative arrangements between WCO Members and the private sector” to increase supply chain security, as adopted by the WCO council in its general assembly in June 2003 and serves to define more detailed requirements to specific business levels.

National standards and guidelines on supply chain security, like C-TPAT and StairSec® are incorporated in full in this Code.

The requirements of this Code are formulated such that port facilities, which comply with the ISPS Code can be confident that cargo, entering their perimeter from a supply chain which is officially confirmed to comply with this Code, is free from security breach.

3. Terms and definitions

The following terms and definitions are applicable to this Code:

3.1. Re. the Security-management System

3.1.1. Security-management System
Set of interrelated or interacting elements to establish a security policy, objectives and measures to achieve those objectives

3.1.2. Top management
A person or a group of persons who directs and controls an organization at the highest level

3.1.3. Organization
Group of people, premises and facilities with an arrangement of responsibilities, authorities and relationships

3.1.4. Supplier
Organization or person that provides a product or service, including sub-contractors

3.1.5. Process
Set of interrelated or interacting activities which transforms inputs into outputs

3.1.6. Procedure
Specified way to carry out an activity or a process

3.1.7. Requirement
Need or expectation that is stated, generally implied or obligatory

3.1.8. Nonconformity
Non-fulfilment of a requirement

3.1.9. Corrective action
Action to eliminate the cause of a detected nonconformity or other undesirable situation

3.1.10. Preventive action
Action to eliminate the cause of a potential nonconformity or other undesirable situation

3.1.11. Security manual
Document specifying the quality management system of an organization
3.1.12. Record
Document stating results achieved or providing evidence of activities performed

3.1.13. Verification
Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

3.1.14. Audit
Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extend to which audit criteria are fulfilled

3.1.15. Audit criteria
Set of policies, procedures or requirements used as a reference

3.1.16. Audit evidence
Records, statements of fact or other information which are relevant to the audit criteria and verifiable

3.1.17. Corrective action
Action to eliminate the cause of a detected nonconformity or other undesirable situation

3.1.18. Certification
A system leading to a written document issued by a party which is duly authorised to do so, confirming that assessments which comply to defined procedures, have revealed that a system is, or has remained, in conformance with a defined standard.

3.1.19. Authorised certification body
An independent third party organisation which has obtained authorization from a designated authority to verify and confirm, through certification, that an organisation complies with the requirements of this Code. Such authorization will only be issued upon verification and confirmation of compliance with appendix B to this Code

3.2. Re. the Supply Chain

3.2.1. Supply chain
the entirety of processes, process steps, organizations and suppliers to get a product moved across international borders from the manufacturer to the point of delivery, as defined by the purchaser

3.2.2. Closed Cargo Transportation Unit (CTU)
any container or closed means of conveyance intended for transport of cargo via road, rail or inland waterways, used in international traffic, of which the interior cannot be accessed other than by visibly damaging its bottom, sides, fronts, top, door or locks, or by breaking its seals.

3.2.3. Premises
Something that is built, installed, or established to serve as an area or location for the processing, storage or handling of cargo and/or CTU’s

3.2.4. Restricted area
An area which after a risk assessment of an organization’s processes and facilities is considered to contain a high risk to physical or information security

3.2.5. Prolonged stop
A period of time during which the means of conveyance is left unattended long enough for unauthorised persons to intrude the CTU.

3.2.6. Inland waterways
Waterways trafficked by barges or inland cargo vessels.
3.2.7. Inland Cargo Vessels
All cargo vessels, excluded by IMO’s International Ships and Port Facilities Code (ISPS-Code), part A and B, together with a revision and amendment of Chapter XI of the SOLAS 74 convention

3.3. Re. Security
3.3.1. Physical Security
absence of danger that the characteristics of cargo in a secure area or a CTU are illegally changed including measures taken to guard against sabotage, escape, attack, or other crime. This danger includes i.a.:
• infiltration with weapons or any other dangerous substances and devices intended to harm people, property or the environment and which are not authorized,
• infiltration with other unauthorised cargo or passengers or
• theft of or damage to cargo

3.3.2. Information Security
absence of danger that information in a document (paper or electronic) is accessed, distributed or changed without proper authorization including measures taken to guard against espionage, sabotage or other crime.

3.3.3. Tamper
any act, object, or practice that interferes with another's rights or interests by being offensive, annoying, dangerous, obstructive, or unhealthful

3.3.4. Security level 1
the level for which minimum appropriate protective security measures shall be maintained at all times.

3.3.5. Security level 2
the level for which appropriate protective security measures, additional to those required for security level 1, shall be maintained for a period of time as a result of heightened risk of a security incident.

3.3.6. Security level 3
the level for which further specific protective security measures shall be maintained, additional to those required for security level 1 and 2, for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

3.3.7. Company security officer
the person designated by the organisation for ensuring that a security assessment is carried out; that a Security-management System is developed, where appropriate submitted for approval, and thereafter implemented and maintained and who liaises with the designated authorities.

3.3.8. Designated authority
The body which, by its government, has been assigned the responsibility to set security levels, and to police compliance with security requirements in the country where the organization is based. For transporters and forwarders this may include bodies which by their governments have been assigned with the responsibility to set security levels and to police compliance with security requirements in the country of destination or transit for CTU’s
4. Security-management system

4.1. General system requirements

The organization shall establish, document, implement and maintain a Security-management System and continually improve its effectiveness in accordance with the requirements of this Code.

The organization shall
a) comply in full to the requirements of this Code, including section 5.1 to 5.5 of this Code as far as these are applicable to the organization’s processes.
b) identify through a security assessment any other security risk in its processes or facilities, as far as not catered for by the provisions of this Code, and include appropriate measures to achieve effective control over these risks in its Security-management System.
c) monitor, measure, guard and analyze these processes and facilities

d) ensure the availability of resources and information necessary to support the security and monitoring of these processes and facilities, and
e) implement actions necessary to achieve planned results and continual improvement of these processes and facilities

Processes and facilities shall be managed by the organization in accordance with the requirements of this Code.
Where an organization chooses to outsource any part of its activities, and this has an effect on the security of the supply chain, the organization shall ensure proper control over such activities. Control of such outsourced activities shall be identified within the Security-management System.

4.2. Documentation requirements

4.2.1. General

The Security-management System shall include
a) documented statements of a Security policy and Security objectives,
b) a documented security risk assessment (see 4.1.b)
c) a Security manual,
d) documented procedures as required by this Code,
e) documents needed by the organization to ensure the effective planning, operation and control of the security of its processes and facilities, and
f) records required by this Code (see 4.2.4).

NOTE 1. Where the term “documented procedure” appears within this Code, this means that the procedure is established, documented, implemented and maintained.
NOTE 2. The extent of the Security-management System documentation can differ from one organization to another due to a) the size of organization and type of activities, b) the complexity of processes, their interactions and the facilities, and c) the competence of personnel.
Its volume shall not obstruct effective implementation of security procedures.
NOTE 3 The documentation can be in any form or type of medium.
4.2.2. Security Manual

The organization shall establish and maintain a Security manual that includes
a) the scope of the Security-management System, including a clear description of the processes which the organization undertakes.
b) the documented procedures, established for all 3 security levels, in the Security-management System, or reference to them.
c) a description of the interaction between the processes and the facilities covered by the Security-management System, and
d) a description of the interaction between the designated authorities and the organization.

4.2.3. Control of documents

Documents required by the Security-management System shall be controlled. Records are a special type of document and shall be controlled according to the requirements given in 4.2.4.
A documented procedure shall be established to define the controls needed
a) to approve documents for adequacy prior to issue,
b) to review and update as necessary and re-approve documents,
c) to ensure that changes and the current revision status of documents are identified,
d) to ensure that documents are subject to information security measures,
e) to ensure that relevant versions of applicable documents are available at points of use,
f) to ensure that documents of external origin are identified and their distribution controlled, and
g) to prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose.

4.2.4. Control of Records

Records shall be established and maintained to provide evidence of conformity to requirements and of the effective operation of the Security-management System. Records shall remain legible, readily identifiable and retrievable. A documented procedure shall be established to define the controls needed for the identification, storage, protection, security retrieval, retention time and disposition of records.

4.3. Management responsibility

4.3.1. Management commitment

Top management shall provide evidence of its commitment to the development and implementation of the Security-management System and continually improving its effectiveness by
a) communicating to the organization the importance of security awareness as well as meeting statutory and regulatory requirements,
b) establishing the Security policy,
c) ensuring that Security objectives are established,
d) conducting management reviews,
e) ensuring the availability of resources, and
f) providing means for raising the alarm in case of security threats or security incidents
g) ensuring adequate response after an alarm has been raised
h) effective information-management regarding security issues and developments
4.3.2. Security levels

When an organization receives notification on a change in security level top management shall immediately ensure that appropriate procedures for the changed security level are adhered to and where necessary brought in compliance with the instructions from the designated authority. They shall ensure that such changes are communicated effectively and efficiently to relevant parts of the organization.

Note: The designated authorities shall set security level 2 and/or 3 and provide guidance for protection from security threats. Factors which are considered in setting the appropriate security level include:
- the degree that the threat information is credible;
- the degree that the threat information is corroborated;
- the degree that the threat information is specific or imminent; and
- the potential consequences of such a security incident.

Designated authorities, when they set security level 3, shall issue, as necessary, appropriate instructions and shall provide security related information to organizations that may be affected.

4.3.3. Security Policy

Top management shall ensure that the Security policy
a) is appropriate to the purpose of the organization,
b) includes a commitment to comply with requirements and continually improve the effectiveness of the Security-management System,
c) provides a framework for establishing and reviewing Security objectives,
d) is communicated and understood within the organization, and
e) is reviewed for continuing suitability.

4.3.4. Security Assessment

The security assessment is an essential and integral part of the process of developing and updating the Security-management System and is the delegated responsibility of the Company Security Officer.

The security assessment shall be carried out by the organisation. Assistance by a qualified third party is not permitted when this third party, or any of its affiliates or subsidiaries, is involved in the evaluation of the assessment.

The security assessments shall periodically be reviewed and updated, taking account of changing threats and/or minor changes in the organisation or its facilities and shall always be reviewed and updated when major changes to the organisation or its facilities take place.

The security assessment shall include, at least, the following elements:

a) identification and evaluation of facilities, process steps and documents which are important to protect;
b) identification of possible threats and vulnerabilities to these facilities, process steps and documents and the likelihood of their occurrence, in order to establish and prioritize security measures and define restricted areas, also taking into account other actors in the supply chain

c) identification of weaknesses, including human factors in the facilities, policies and procedures.
d) identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability. This should include considering the application and/or installation of (additional) equipment for radar scanning, heartbeat detection, CO2-detection, scanning of nuclear substances, differentiation of screening and scanning percentages, operational changes in CCTV-control regarding frequency and coverage at the different security levels.

Upon completion of the security assessment, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each threat and vulnerability, found during the
assessment, and a description of counter measures that could be used to address each threat and vulnerability. The report shall be protected from unauthorized access or disclosure.

Designated authorities or their authorised certification bodies may allow a security assessment to cover more than one organisation if the organisations location, operation, equipment, and design of its facilities are similar. Any authorised certification body, which allows such an arrangement, shall communicate this to their designated authority.

4.4. Organization and communication

4.4.1. Responsibility and authority

Top management shall ensure that responsibilities and authorities regarding functions, pertinent to security, are defined and communicated within the organization.

4.4.2. Company Security Officer

Top management shall appoint a member of management who, irrespective of other responsibilities, shall have responsibility and authority that includes

a) ensuring that processes and provisions needed for the Security-management System are established, implemented and maintained,

b) reporting to top management on the performance of the Security-management System and any need for improvement, and

c) ensuring the promotion of security awareness throughout the organization and with its suppliers,

Top management can appoint one or more deputies. Appointment must be in writing and be communicated to the relevant parties.

4.4.2.1. Internal communication

The responsibility of the company security officer includes that appropriate communication processes are implemented within the organization and that communication takes place regarding the effectiveness of the Security-management System.

4.4.2.2. External Communication

The responsibility of the company security officer includes identification of and liaison with external parties including other parties in the supply chain on matters relating to the Security-management System.

Clear and concise procedures should be established to assure that changes in security level are being promulgated rapidly and security incidents are reported instantly to the designated authorities. A list of contact points and emergency response services should be available at relevant locations in the organization.

5. Security-management

5.1. General requirements

These general requirements are applicable to all organizations who want to apply this standard, independent of size and type of processes in their operation.

5.1.1. Procedural security

The organization shall have documented procedures in place which describe:

5.1.1.1. For security level 1
a. How deviations from normal operating procedures are reported and investigated within the organization and how responsibilities for this are defined.

b. how customs and other relevant law enforcement bodies are notified in cases where anomalies or illegal activities are detected, or suspected

c. how overages/shortages, including unmanifested materials, shall be detected and how these are reported to customs, other law enforcement bodies clients and other appropriate parties in the market

d. how suppliers are classified according to the security risk they may constitute to the supply chain.

e. how dangerous goods and other hazardous cargo, including nuclear substances, are recorded / documented

f. how random, unannounced security verification of areas in control of the organization and within the supply chain are performed and who decides where and when these verifications take place.

g. who shall be authorized to break seals for inspection purposes and re-seal the CTU before further handling and how information about such change of seal shall be processed.

5.1.1.2. For security level 2

a. how the use of suppliers is limited to those which have worked for the organization more than 2 years without any security incidents.

b. how intensified random, unannounced security verifications of areas in control of the organization and within the supply chain are performed and who decides where and when.

c. how the response will be to any security threat and breaches

5.1.1.3. For security level 3

a. how the organization shall respond to level 3 security incidents

b. how to evacuate its premises

5.1.2. Human Resources

The organization shall have documented procedures in place which, with due regard for (where relevant) applicable privacy legislation, shall describe:

5.1.2.1. For security level 1

a. in detail the tasks and responsibilities of personnel assigned security duties

b. how employees, including sub-contracted staff are screened and interviewed prior to employment

c. how analysis is carried out to define which personnel performs security sensitive duties.

d. how the background of employees, including sub-contracted staff, which perform security sensitive tasks is annually checked. These checks shall be routinely done when relocating personnel to security sensitive positions within the organization

e. how all employees, including sub-contracted staff, are trained and educated to recognize conspiracies, breaches of cargo and/or information integrity and unauthorized access.

f. how a security awareness program shall be implemented and provided to employees and sub-contracted staff, including the recognition of internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should offer incentives for active employee participation in security controls and verifications.

5.1.2.2. For security level 2

a. how security awareness programs, which are ran within the organization, shall be intensified.

b. how relocation of personnel within the organization shall be authorized

c. how additional resources are introduced and organized

5.1.2.3. For security level 3
a. how security performance of employees and suppliers is monitored, corrected and documented.
b. how training and selection program will be revised as a result of performance monitoring.
c. how additional resources are introduced and organized
d. which critical key functions have been identified and defined to handle emergency response

5.1.3. Physical Security

The organization shall have made provisions which ensure that:

5.1.3.1. For all security levels
a. internal / external two way communication systems to contact internal and/or external security personnel are in place and operational at all times, including, where applicable, procedures which prevent impersonation

5.1.4. Information Security

The organization shall have documented procedures in place which ensure that:

5.1.4.1. For all security levels
a. the organizations security procedures are kept confidential and are not distributed outside the organization without authorization of the company security officer.
b. obsolete document are destroyed under secure conditions.

5.2. Specific Requirements to Stuffers and Packers

These specific requirements are applicable to all organizations who, as (part of) their operation are engaged in the stuffing, packing, loading, re-loading or consolidating and consecutive sealing of CTU’s, independent of their size and type of processes of this operation.

5.2.1. Procedural security

The organization shall have documented procedures in place which ensure that:

5.2.1.1. For security level 1
a. only the designated company security officer or one of his designated deputies, shall be physically present during loading/unloading of the CTU and supervise the introduction or removal of cargo into/from the CTU to prevent that:
   • CTU’s are infiltrated with unauthorized weapons or any other dangerous substances and devices intended to harm people, property or the environment,
   • other unauthorised cargo or passengers are entered into the CTU
   • cargo is stolen.
b. when a deputy to the designated security officer is employed by a sub-contracting company, such sub-contracting company shall be authorized by the designated authorities, based on confirmed compliance with this Code.
c. the supervision, as per 5.2.1.1.a, includes inspection of empty or partially loaded CTU’s to detect any security breach, immediately before loading.
d. this supervision shall be uninterrupted from the start of the inspection until the CTU is sealed.
e. this supervision shall include verification that seals on received CTU’s are intact and conform the appropriate records.
f. marking, weighing, counting and documenting of cargo entering the CTU is properly performed

g. all cargo is compliant with its documentation and manifests
h. the designated security officer (or his deputies) shall seal the closed CTU with an approved tamper proof seal immediately upon loading and properly record the data of this seal.

i. cargo is properly stuffed in accordance with the IMO/IL/O/UN ECE Guidelines for Packing of Cargo Transport Units (1997 edition) to prevent cargo damage during transport

j. adequate maintenance and calibration of any security pertinent equipment

5.2.1.2. For security level 2

a. the organization shall supervise the introduction or removal of cargo into/from the CTU without using suppliers personnel for this supervision.

b. intensified search is carried out and intensified use of equipment is implemented

5.2.1.3. For security level 3

5.2.1.4. Emergency response measures are defined

5.2.2. Physical security

For restricted areas the organization shall have documented procedures in place and/or physical provisions made which ensure that:

5.2.2.1. For security level 1

a. buildings containing restricted areas should be constructed of materials, which resist unlawful entry and protect against outside intrusion of unauthorized persons and goods.

b. restricted areas, situated outside are surrounded by perimeter fences which comply to the legal and statutory requirements

c. external and internal doors, windows, gates and fences of restricted areas are provided with locking devices

d. restricted areas, both inside and outside are provided with adequate lighting

e. restricted areas are equipped with intrusion alarms

f. parking areas for private vehicles are well separated from restricted areas

5.2.2.2. For security level 2

a. restricted areas are patrolled by guards, dogs and/or closed TV-circuits.
5.2.2.3. **For security level 3**
   a. as indicated by the designated authorities specific CTU’s are separated, will not be stuffed or loaded, be moved to a designated area outside the premises or put under continuous monitoring by guards or TV-cameras.

5.2.3. **Access Controls**
The organization shall have documented procedures in place and/or physical provisions made which ensure that:

5.2.3.1. **For security level 1**
   a. unauthorized access to facilities is prevented
   b. controls include positive identification and recording of all employees, suppliers, visitors, and vendors on site.
   c. visitors are not allowed to move around the facilities without accompaniment of an employee
   d. unauthorized / unidentified persons are challenged
   e. authorization to access restricted areas shall be recorded and evidence shall be worn clearly visible at all times
   f. security Codes, cards and/or keys shall only be submitted to authorized persons for which records shall be held.
   g. upon termination of engagement at the premises security Codes, cards and/or keys shall be returned to the organization for which records shall be held.

5.2.3.2. **For security level 2**
   a. only goods for which properly authorized documents, such as purchase orders, manifests etc. are available shall be allowed to enter the premises after visual inspection.
   b. persons and goods will be screened and/or scanned randomly
   c. the identification of lorries, entering or leaving the premises, and their drivers and passengers shall be recorded

5.2.3.3. **For security level 3**
   a. visitors or vendors will not be allowed to enter the premises unless special authorization is provided by the recognized authority for response to a security incident.
   b. security Codes, cards and/or and keys (with their locks) for restricted areas shall be changed and only redistributed to persons authorized to access the restricted area.

5.3. **Specific Requirements to Warehouses, Storage Areas and Terminals**
These specific requirements are applicable to all organizations who, as (part of) their operation are engaged in the storage of cargo and/or sealed CTU’s in warehouses, on storage areas and terminals, independent of nature and size.

5.3.1. **Procedural security**
The organization shall have documented procedures in place which ensure:

5.3.1.1. **For all security levels**
   a. that all cargo entering the warehouse or storage area is properly marked, weighed counted, documented and inspected for the absence of illegal goods or attributes
   b. that all CTU’s entering the premises are properly sealed and that the seal is compliant to its documentation
   c. that all cargo and CTU’s are compliant with their documentation and manifests
   d. that received containers, when emptied, are sealed again and that such sealing is properly recorded
   e. adequate maintenance and calibration of any security pertinent equipment
5.3.2. Physical security

Warehouses and storage areas for outward bound cargo as well as terminals are identified as restricted areas. For these restricted areas the organization shall have documented procedures in place and/or physical provisions made which ensure that:

5.3.2.1. For security level 1
   a. warehouses should be constructed of materials, which resist unlawful entry and protect against outside intrusion of unauthorized persons and goods.
   b. storage areas and terminals are surrounded by perimeter fences which comply to the legal and statutory requirements
   c. external and internal doors, windows, gates and fences of restricted areas are provided with locking devices
   d. restricted areas, both inside and outside are provided with adequate lighting
   e. international, domestic, high-value, and dangerous goods cargo is marked and segregated within the premises by a safe, caged or otherwise fenced-in area.
   f. restricted areas are equipped with intrusion alarms
   g. parking areas for private vehicles are well segregated from restricted cargo areas

5.3.2.2. For security level 2
   a. restricted areas are patrolled by guards, dogs and/or closed TV-circuits.

5.3.2.3. For security level 3
   a. specific cargoes or CTU’s, as indicated by the designated authorities, are separated, be moved to a designated area outside the premises or put under continuous monitoring by guards or TV-cameras

5.3.3. Access Controls

The organization shall have documented procedures in place and/or physical provisions made which ensure that:

5.3.3.1. For security level 1
   a. unauthorized access to facilities is prevented
   b. controls include positive identification and recording of all employees, suppliers, visitors, and vendors on site.
   c. visitors are not allowed to move around the facilities without accompaniment of an employee
   d. unauthorized / unidentified persons are challenged
   e. authorization to access restricted areas shall be clearly visible
   f. security Codes, cards and/or keys shall only be submitted to authorized persons for which records shall be held.
   g. upon termination of engagement at the premises security Codes, cards and/or keys shall be returned to the organization for which records shall be held.

5.3.3.2. For security level 2
   a. only goods for which properly authorized documents, such as purchase orders, manifests etc. are available shall be allowed to enter the premises after inspection.
   b. persons and goods will be screened and/or scanned randomly
   c. the identification of lorries, entering or leaving the premises, and their drivers and passengers shall be recorded.
5.3.3.3. For security level 3
   a. visitors or vendors will not be allowed to enter the premises unless special authorization is provided by the recognized authority for response to a security incident.
   b. security Codes, cards and/or and keys (with their locks) for restricted areas shall be changed and only redistributed to persons authorized to access the restricted area.

5.4. Specific Requirements to Forwarders and Transporters

These specific requirements are applicable to all organizations who, as (part of) their operation are engaged in the moving of closed CTU’s by road, rail or inland waterway

5.4.1. Procedural security

The organization shall have documented procedures in place which ensure that:

5.4.1.1. For security level 1
   a. only CTU’s are accepted to be loaded on the organizations means of conveyance which are properly marked, and have the correct weight and documentation.
   b. CTU’s, whether loaded or empty, only will be loaded when they are tamper proof sealed and this sealing is properly documented.
   c. CTU’s are moved according to pre-defined schedules, including routes and stops, and unexpected delays and deviations are to be reported to the organization.
   d. origin site shall pre-alert destination site before shipment. Such pre-alert shall contain as a minimum: departure time, expected arrival time, transport companies name, employee name, seal numbers.
   e. security pertinent equipment is properly maintained and calibrated.
   f. before loading, at departure and after each prolonged stop seals are checked for tampering, all readily accessible areas shall be physical searched and internal/external compartments and panels shall be secured. These checks are to be recorded and records are to be kept for one year and be accessible to other actors in the supply chain for verification.

5.4.1.2. For security level 2
   a. at departure the identity of any authorized passenger, other than employees of the organization shall be forwarded to the designated authority at the point of arrival.
   b. receiving site to confirm arrival to origin site within 4 hours after arrival and after verification that the pre-alert details are correct.

5.4.1.3. For security level 3
   a. at departure the identity of all employees of the organization onboard the means of conveyance shall be forwarded to the designated authority at the point of arrival. Passengers, other than own employees are not allowed, unless special arrangements have been made with the designated authorities.

5.4.2. Physical security

The organization shall have documented procedures in place and/or physical provisions made which ensure that:

5.4.2.1. For security level 1
   a. control cabins of means of conveyance, when not manned, are kept locked at all times and only employees of the organization are allowed to have access. Deviations shall be authorized by the organization in advance.
   b. documentation containing cargo information is kept secure in these control cabins.
   c. control cabins are equipped with an intrusion alarm.
d. procedures for reporting when unauthorized personnel, unmanifested materials, or signs of tampering, are discovered.
e. no prolonged stops shall be made at isolated locations where normal social control can not be exercised, unless such location is equipped with adequate lightening and fencing according to the standards set by the designated authorities.

5.4.2.2. For security level 2

a. road and rail vehicles will only make prolonged stops at locations which are equipped with adequate lightening and fencing which meets the standards, as set by the designated authorities;
b. road and rail vehicles shall not be left unattended.
c. vessels and barges shall be kept under constant surveillance, whether en route or boarded alongside and shall have adequate lightening

5.4.2.3. For security level 3

a. areas for prolonged stops shall be permanently patrolled by guards, dogs or supervised by closed TV-circuits
b. specific CTU’s, as indicated by the designated authorities, are separated and will not be transported any further awaiting instructions from the designated authorities

5.5. Specific Requirements to Information Processors

These specific requirements are applicable to all organizations (including brokers, agents etc,) who as (part of) their operation are engaged in the receiving, processing or forwarding of information to customs or other parties in the supply chain.

5.5.1. Procedural security

The organization shall have documented procedures in place and/or physical provisions made which ensure that:

5.5.1.1. For all security levels

a. complete, legible and accurate documents are submitted timely to customs
b. an analysis is made of the vulnerability of information systems, the relevance to security of data and the implementation of adequate safeguards and firewalls.
c. access authorization protects computer systems and computer data against exchange, loss or introduction of erroneous information
d. security critical information is only accessible to authorized personnel and that the users of this information can be traced back
e. routines exist to securely cope with break downs and secure back-up routines are followed.
f. the transporter or forwarder is informed when during the processing of information it is noted that the progress or movement of CTU’s deviates from pre-defined schedules
g. overages and shortages, as well as other anomalies, observed during the processing of information, are reported not only to the customs, but also to the organization(s) responsible for the processing of the cargo.

5.5.2. Access Controls

The organization shall have documented procedures in place and/or physical provisions made which ensure that:
5.5.2.1. For security level 1 and 2
a. unauthorized access to facilities is prevented
b. controls include positive identification and recording of all employees, suppliers, visitors, and vendors on site.
c. visitors are not allowed to move around the facilities without accompaniment of an employee
d. unauthorized / unidentified persons are challenged
e. security Codes, cards and/or keys shall only be submitted to authorized persons for which records shall be held.
f. upon termination of engagement at the premises security Codes, cards and/or keys shall be returned to the organization for which records shall be held.

5.5.2.2. For security level 3
a. visitors or vendors will not be allowed to enter the premises unless special authorization is provided by the recognized authority for response to a security incident.

6. Measurement, analyses and improvement

6.1. General

The organization shall plan and implement the monitoring, measurement, analysis and improvement processes needed
a) to demonstrate compliance to requirements,
b) to ensure conformity of the Security-management System, and
c) to continually improve the effectiveness of the Security-management System.

This continually improving of the effectiveness of the Security-management System shall be through the use of the Security policy, Security objectives, audit results, analysis of data, reports on security incidents, corrective and preventive actions and management review.

6.2. Internal Audits

The organization shall conduct internal audits at planned intervals to determine whether the Security-management System
a) conforms to the planned arrangements, to the requirements of this Code and to the Security-management System requirements established by the organization, and
b) is effectively implemented and maintained.

Internal audits can include activities which are performed by suppliers.

An audit programme shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods shall be defined. Selection of auditors and conduct of audits shall ensure security, objectivity and impartiality of the audit process.

Auditors shall not audit their own work.

The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.2.4) shall be defined in a documented procedure.

The management responsible for the area being audited shall ensure that actions are taken without delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

NOTE See ISO 19011 as revised for guidance.
6.3. Measuring and Monitoring

The organization shall continuously monitor and, where applicable, measure the implementation and the effectiveness of its Security-management System. This shall demonstrate the ability of the system to maintain the required level of security at all times. When planned results are not achieved, correction and corrective action shall be taken, as appropriate, to ensure conformity to requirements. Evidence of conformity with the acceptance criteria shall be maintained.

6.4. Corrective and preventive action

6.4.1. Corrective action

The organization shall take immediate action to eliminate the causes of nonconformities in order to prevent recurrence. Corrective actions shall be implemented promptly and be appropriate to the effects of the nonconformities encountered.

A documented procedure shall be established to define requirements for
a) reviewing nonconformities (including feedback from the designated authorities),
b) determining the causes of nonconformities,
c) evaluating the need for action to ensure that nonconformities do not recur,
d) determining and implementing action needed,
e) records of the results of action taken (see 4.2.4), and
f) reviewing corrective action taken.

6.4.2. Preventive action

The organization shall determine action to eliminate the causes of potential nonconformities in order to prevent their occurrence. Preventive actions shall be appropriate to the effects of the potential problems.

A documented procedure shall be established to define requirements for
a) determining potential nonconformities and their causes,
b) evaluating the need for action to prevent occurrence of nonconformities,
c) determining and implementing action needed,
d) records of results of action taken (see 4.2.4), and
e) reviewing preventive action taken.

6.5. Security Records

Records are evidence of the ongoing functioning of a Security-management System and should cover as a minimum (but not limited to):

- Information received on any change in security level
- Legislative and regulatory requirements
- Cargo manifests
- Permits
- Security training records
- Initial and periodic employee screening records
- Inspection, maintenance and calibration records
- Audit and Management review reports
- CTU- and seal identity
- Security assessment records
- Non-conformance reports, incident reports, complaints and records on follow-up actions
- Supplier and contractor information
All these records are subject to security information procedures and to the document control requirements in 4.2.4.

6.6. Management Reviews

6.6.1. General

Top management shall review the organization's Security-management System, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the Security-management System, including the Security policy and Security objectives. Records from management reviews shall be maintained (see 4.2.4).

6.6.2. Review of the Security-management System

The input to management review shall include information on
a) results of audits,
\[ \text{d) status of preventive and corrective actions,} \]
\[ \text{e) follow-up actions from previous management reviews,} \]
\[ \text{f) changes that could affect the Security-management System, and} \]
g) recommendations for improvement.
\[ \text{h) feedback from designated authorities on} \]
\[ \text{1. any non-conformities during physical checks} \]
\[ \text{2. changes in regulatory and legislative requirements} \]
\[ \text{3. security information and developments from intelligence networking} \]

6.7. Continual improvement

The output from the management review shall include any decisions and actions related to
a) improvement of the effectiveness of the Security-management System,
b) improvement of facilities
c) resource needs.
that will need to be incorporated in a plan for the coming period.