BUSINESS ALLIANCE FOR SECURE COMMERCE

BASC International Norm and Standards Implementation Guide

Version 6 - 2022



World BASC Organization
www.wbasco.org

Miami, Florida.
United States of America

Design and Layout:
World BASC Organization

BUSINESS ALLIANCE FOR SECURE COMMERCE

BASC International Norm and Standards Implementation Guide

Version 6 – 2022

Effective Date: March 2, 2022

BUSINESS ALLIANCE FOR SECURE COMMERCE

BASC International Norm Implementation Guide

Control and Security Management System (CSMS)

Version 6 – 2022

Effective Date: March 2, 2022

TABLE OF CONTENTS

• INTRODUCTION

The Implementation Guides for the BASC International Norm V.6-2022 and the BASC International Standards are tools whose purpose is to help the company put into operation the BASC Control and Security Management System (CSMS).

Generally, companies that seek to ensure their processes by meeting security requirements need guidance to implement a management system, in particular the BASC CSMS, which is developed within the framework of the supply chain and other national and international trade processes.

The Implementation Guides are practical documents that contribute to the proper implementation and compliance with the BASC CSMS addressing relevant recommendations, approaches and considerations. These guides do not constitute mandatory requirements that must be evidenced for conformity in the BASC Certification.

This document is the result of the collaboration of many individuals at WBO organization including:

WBO Board of Directors 2021-23: Emilio Aguiar (BASC Ecuador), President; Ricardo Sanabria (BASC Colombia), Vice President; Patricia Siles (BASC Peru), Secretary; Armando Rivas (BASC Dominican Republic), Treasurer; and Álvaro Alpízar, Vocal.

WBO Technical Committee 2021-23: Fermin Cuza, WBO International President; Executive Directors: Giomar Gonzalez, BASC Panama; Luis Bernard Benjumea, BASC Colombia; Omar Castellanos, BASC Dominican Republic; Fabrizio Muñoz, BASC Guayaquil; Cesar Venegas, BASC Peru; Jorge Wellmann, BASC Guatemala; María Andrea Caldas, WBO Certifications Coordinator, and Luis Renella, WBO Director of Operations.

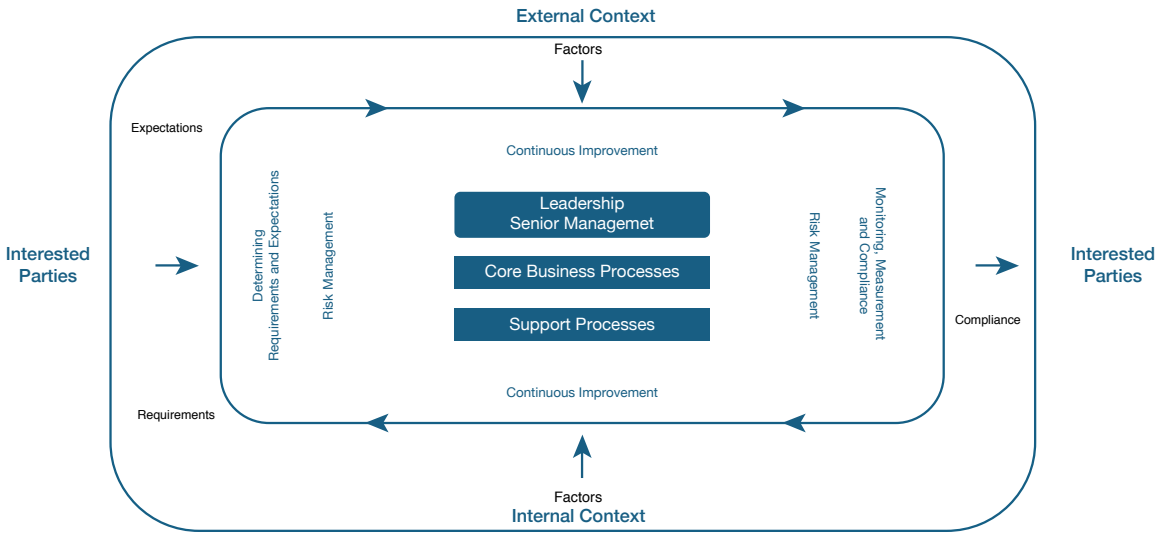
English Homologation: Bradd Skinner and Luis Renella.

• COMPANY CONTEXT

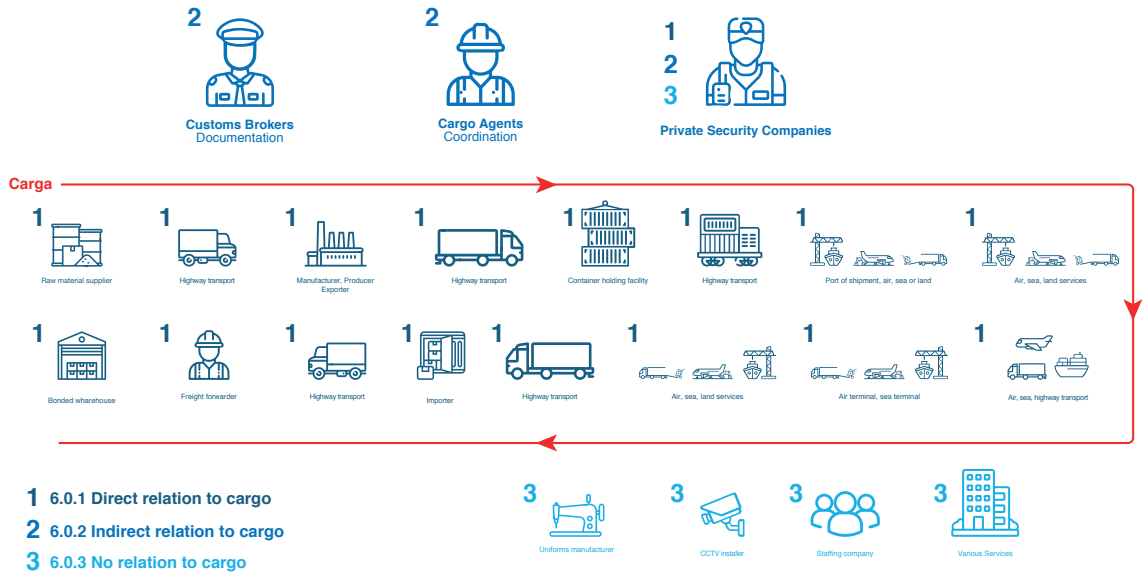
- Understanding the company and its context

The context of the organization is the combination of internal and external factors that can have an effect on the company's approach to developing and achieving its objectives. The internal context are aspects related to the values, culture, knowledge, performance of the company, among others. The external context includes the legal, technological, competitive, commercial, cultural, social, and economic environment, among others, whether local, national, regional, or international. For the above, one can use different tools such as Global BASC, or any other that one considers appropriate to diagram the supply chains with the greatest impact, including business partners and stakeholders based on risk management.

Context graph



Supply Chain graph



- Understanding the needs and expectations of interested parties

The identified interested parties of the company can be internal (Shareholders, board of directors, owners, collaborators, among others) or external (Regulatory entities, business associates - clients, suppliers and third parties linked to the supply chain, competitors, community, among others), according to the impact on the scope of the BASC CSMS and the supply chain.

The company can identify needs and expectations through meetings, surveys, experiences, among other methodologies.

- Process approach

The process-based approach is a basic management principle and fundamental to obtaining the results expected by the company.

Each identified process should be analyzed to determine and document the requirements established in the BASC Standard, through a record, procedure or characterization.

• LEADERSHIP

- Leadership and commitment

Leadership is understood as a behavior and personal commitment, whose purpose is to direct and positively influence the behavior of others to achieve certain objectives.

Senior management should demonstrate its leadership and commitment to the CSMS by informing employees about the most significant aspects of the BASC CSMS and its results, promoting regular meetings with process leaders to review the performance and achievements of the CSMS, participating in forums and meetings related to the CSMS, assigning personnel and financial resources for the implementation, maintenance and improvements of the CSMS, among others.

When elaborating the code of ethics and conduct, the company should consider its vision, mission, values, prohibited behaviors, collaborator responsibility, compliance with the law, and avoiding conflicts of interest, among others.

- Control and security management policy

The Control and Security Management Policy is the tool used by senior management to establish the main axes of the BASC CSMS. This should include the strategic foundations and the guidelines that will serve as a reference to achieve compliance with the objectives of the CSMS.

- Policy communication

The company should guarantee adequate internal and external communication of the Control and Security Management Policy so that the message from senior management is known and understood by employees and stakeholders at all levels of the company.

This policy should be made available to interested parties (internal and external) relevant and pertinent to the company's CSMS, through websites, publications within the facilities, mass mailings to customers and suppliers, among others.

- Objectives of the BASC CSMS

The objectives of the CSMS constitute one of the main ways to achieve goals and improvement of the CSMS. The objectives of the CSMS will carry out the general guidelines set by the Control and Security Management Policy, therefore they should be consistent with the strategic direction of the company.

- Company responsibility and authority

Roles and responsibilities are defined by senior management. Collaborators should know what their role is in the CSMS and in the processes that comprise it. They should also know what the authority is to perform the assigned functions.

To maintain the documented information of the responsibility and authority of the personnel that have an impact on the CSMS, the following documents should be implemented: Organization and functions manual, description of job profiles, process files, and appointment certificates, among others. The responsibility and authority information should be included in previously established procedures where applicable.

• PLANNING

- Risk management

The procedure should consider the use of risk matrixes, Global BASC or other tools that it considers pertinent for the management of the risks identified by processes.

a) Risk criteria and identification

To determine risk criteria, the company should:

- Specify the amount and type of risk that it's willing to take to achieve the objectives of the BASC CSMS.
- Assess the importance of risk to support decision-making in risk management.
- Align with the risk management framework and adapt to the purpose and scope specified in the BASC CSMS.
- Reflect the values, objectives and resources of the company and be

consistent with the policies and statements about the BASC CSMS.
- Be reviewed and amended if necessary.

Risk identification responds to the need to recognize and describe the threats or vulnerabilities that can help or prevent a company from achieving its objectives. This risk identification must be process based, considering the scope and context of the company and the commitments established in its policy, objectives and with interested parties.

b) Risk analysis

The purpose of risk analysis is to understand its nature and characteristics, identifying the level of impact it has on the BASC CSMS processes. Risk analysis involves a detailed consideration of uncertainty, sources of risk, consequences, probabilities, events, scenarios, controls, and their effectiveness. An event can have multiple causes and consequences and can affect multiple processes.

Risk Factor (RF) is the mathematical result of multiplying the Probability (P) and Impact (I) factors. The probability (P) is the possibility that the risk happens or materializes in a specific period and the impact (I) is the expected result before the materialization of the risk, whether tangible or intangible and related to security in the BASC CSMS.

c) Risk evaluation

The purpose of risk evaluation is to support decision-making and involves comparing the results of the risk analysis against established criteria to determine when further action is required.

d) Risk treatment

Risk treatment involves an interactive process of:

- formulating and selecting options;
- planning and implementing;
- evaluating the effectiveness;
- deciding if the residual risk is acceptable; and
- if not acceptable, performing additional treatment.

Addressing the risk is understood as the set of actions that the company proposes for the treatment of an identified, analyzed and valued risk.

Options to treat the risk may involve one or more of the following alternatives:

- avoid the risk by deciding not to start or continue with the activity that generates the risk;
- accept or increase risk in search of an opportunity;
- eliminate the source of risk;
- modify probability;
- modify consequences;
- risk sharing (for example: through contracts, purchase of insurance);
- retain the risk based on an informed decision.

Source: ISO 31000

e) Response planning

In executing exercises and drills, it should be considered in the planning that these do not become a risk or may affect the continuity of the business.

Business continuity requires processes and resources developed to manage the risks related to the business and its nature, considering the Recovery Time Objective (RTO) and the Maximum Tolerable Period of Disruption (MTPD) due to an interruption from a business or strategic team perspective.

Event response should be considered as improvement actions, treating their causes, determining actions and verifying their effectiveness.

Source: ISO 22301

f) Follow-up

The purpose of monitoring and follow-up is to ensure the effectiveness of the applied method for risk management in the aforementioned stages. This methodology should be carried out periodically or at least once a year, including its planning, collection of data and sources, analysis of information, recording of results, actions and conclusions.

g) Reviews

As part of the risk management review process, the company should consider a report that includes the results of the methodology, the allocation of resources, review of results, residual risk, conclusions and decision-making in this regard.

h) Communication

Risk management communication should include all relevant stakeholders who are responsible for the organization, considering digital, physical and other methods that are necessary to ensure effectiveness and receipt of the information.

Risk management communication should be timely and ensure that relevant information is collected, consolidated, synthesized and shared, where appropriate, and that feedback is provided and improvements made.

- Legal requirements

Legal requirements are recognized as compliance obligations established in laws, regulations, codes, statutes, agreements or other binding documents that are applicable to the company and the sector in which it operates, in accordance with the legislation of each country.

Legal requirements should be identified and managed. The company must apply due diligence procedures, including permits or operating requirements, collaboration agreements between interested parties, in accordance with the processes declared in the scope of the BASC CSMS.

The company should use a matrix of legal and regulatory requirements or any other tool which takes into consideration, but not limited to, the following: the responsible institution, a brief description, evidence of compliance, expiration, consequences of non-compliance and renewal.

It is important to specify that WBO and BASC Chapters' regulatory requirements apply.

• SUPPORT

- Forecasts

The company should allocate a budget approved by senior management, as well as have the necessary resources to implement, maintain and continuously improve the BASC CSMS.

- Personnel

To establish staff competency requirements, the company should implement a job description or manual, and should conduct regular performance appraisals.

The company should periodically review and update the risk management criteria to determine critical positions, generating objective evidence of said review.

The establishment of critical positions allows the company to define responsibilities associated with the risks of each process. Critical functions are those that require exhaustive controls such as access to cargo, classified information, and sensitive sites among others, based on the criteria determined by the company, according to its risks. The company will determine, according to the activities it develops, the criticality of its personnel.

- Infrastructure

Infrastructure is understood as the set of facilities, equipment, support services and technology necessary for the operation of the company. Once the necessary infrastructure has been established, one will need to carry out any required maintenance or renovation.

The company should maintain up-to-date records of the equipment or work tools provided to personnel for the performance of their duties and responsibilities.

- Control and security manual

The Control and Security Manual establishes how the company understands its context, the needs and expectations of the interested parties, the scope, justification for the exclusions to the requirements of the BASC Security Standard that do not apply, as well as the way in which the company complies with each of

the requirements of the BASC International Norm and Standards.

The company should periodically review the BASC Control and Security Manual and maintain records of said review and any modifications made thereto.

- Document control

The company should establish procedures that contemplate the guidelines for the control of its documents. This document control procedure should be approved and reviewed at least yearly, ensuring its integrity and the way in which it will be made available to interested parties. The Master document list should consider the version of the document, the process to which it applies, date of approval, person responsible for compliance, among others.

- Control de registros

La empresa podría establecer procedimientos que contemplen los lineamientos para el control de sus registros. Durante el tiempo de retención, los registros deben permitir evidencia objetiva durante el período que abarque la operación o servicio, considerando las disposiciones legales relacionadas y el SGCS BASC. También aplica para registros fílmicos.

• PERFORMANCE EVALUATION

- General

The documented procedure should contain, at a minimum, the objective, the person responsible for supervision, the person(s) responsible for execution, terms and definitions, the development of activities, the necessary records to demonstrate compliance, and the control of changes.

The internal audit cycle (delivery of the report, communication of the result, implementation of actions and verification of the effectiveness) should be carried out before the expiration date of the annual certification so that it can be presented as evidence of completion prior to the BASC audit. Likewise, it is advisable for the company to carry out the internal audits with sufficient time before the BASC audit in order to complete the cycle of corrective actions as far in advance as possible.

The task of the internal auditor is to demonstrate compliance with the

requirements of the BASC International Norm and Standards. To do this, the evidence obtained should be established and recorded in the "Auditor's Notes".

- Internal audit program

In its internal audit program, the company should consider at least the following aspects: objectives, scope, people in charge, records, management and monitoring of results, review and improvement of the program.

- Selection and evaluation of the audit team

The company determines the competencies of internal auditors (training, education, experience and skills).

As part of the training process, the BASC International Norm and Standard interpretation course, internal auditor course and risk management course should be considered.

In order to periodically evaluate the validity of the competencies of the internal auditors, the company should establish a methodology that considers their registration and activities carried out regarding the BASC CSMS.

- Management review

Reviews of the BASC CSMS should be convened and conducted by senior management and should be carried out before the expiration date of the annual certification, in order to be able to present the evidence in the BASC audit. It should be preserved through a record.

Senior management should have objective evidence of the aspects related to the BASC CSMS and give priority attention to evaluating and analyzing the aspects in which deviations are evident.

• IMPROVEMENT

- General

The objective of improvement management is for the organization to have the ability to identify important aspects that can directly affect the effectiveness of the

BASC CSMS and after a careful analysis implement actions to ensure compliance with it; this means strengthening risk management through the actions implemented, achieving compliance with the established objectives and, consequently, with the declared Control and Security Management Policy.

- Correction

There are critical events or unusual activities in the operation that can directly affect the integrity of the processes and that should be controlled and/or mitigated immediately and with available resources.

- Corrective action

The company should apply any methodology for root cause analysis (5 whys, fishbone, brainstorming, among others). This analysis can lead to identifying other deviations in the CSMS that should also be treated.

- Improvement actions

The company should constantly identify and implement improvements in its activities as a result of verification exercises or audits, as well as during the daily performance of its operations.

BUSINESS ALLIANCE FOR SECURE COMMERCE

Implementation Guide BASC International Standards

Control and Security Management System (CSMS)

Version 6 – 2022

Effective date: March 2, 2022

TABLE OF CONTENTS

• INTRODUCTION

The Implementation Guides for the BASC International Norm V.6-2022 and the BASC International Standards are tools whose purpose is to help the company put into operation the BASC Control and Security Management System (CSMS).

Generally, companies that seek to ensure their processes by meeting security requirements need guidance to implement a management system, in particular the BASC CSMS, which is developed within the framework of the supply chain and other national and international trade processes.

The Implementation Guides are practical documents that contribute to the proper implementation and compliance with the BASC CSMS addressing relevant recommendations, approaches and considerations. These guides do not constitute mandatory requirements that must be evidenced for conformity in the BASC Certification.

This document is the result of the collaboration of many individuals at WBO organization including:

WBO Board of Directors 2021-23: Emilio Aguiar (BASC Ecuador), President; Ricardo Sanabria (BASC Colombia), Vice President; Patricia Siles (BASC Peru), Secretary; Armando Rivas (BASC Dominican Republic), Treasurer; and Álvaro Alpízar, Vocal.

WBO Technical Committee 2021-23: Fermin Cuza, WBO International President; Executive Directors: Giomar Gonzalez, BASC Panama; Luis Bernard Benjumea, BASC Colombia; Omar Castellanos, BASC Dominican Republic; Fabrizio Muñoz, BASC Guayaquil; Cesar Venegas, BASC Peru; Jorge Wellmann, BASC Guatemala; María Andrea Caldas, WBO Certifications Coordinator, and Luis Renella, WBO Director of Operations.

English Homologation: Bradd Skinner and Luis Renella.

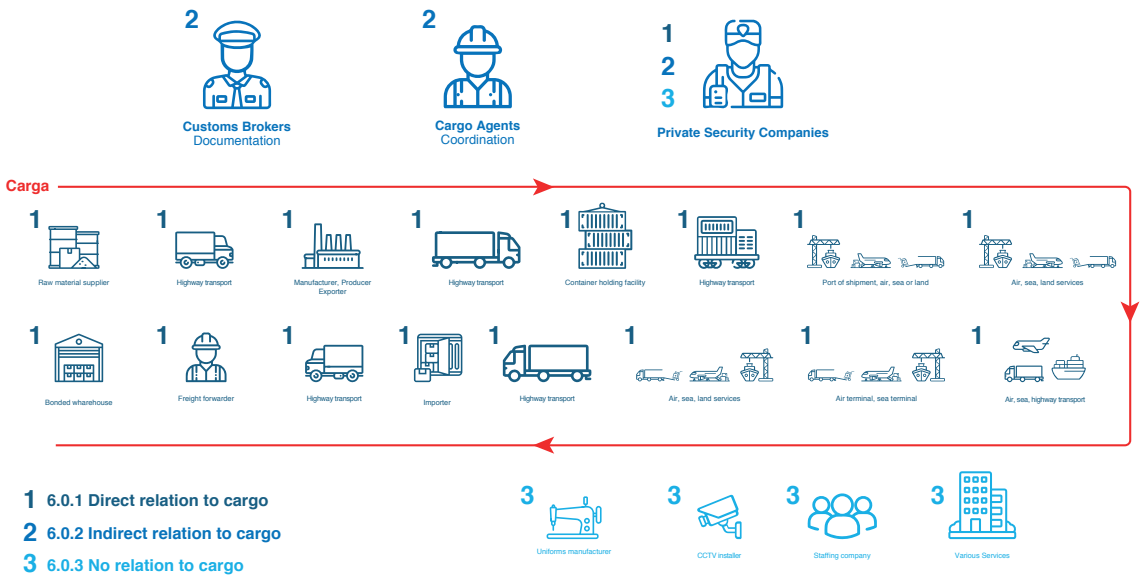
• BUSINESS PARTNERS

- Business partners requirements

Different sectors of business partners pose different types and degrees of risk; therefore,they should be treated differently in the selection, evaluation and contracting procedures, as well as in the company's risk management.

The third parties linked in the supply chain are those companies subcontracted by a supplier of products or services contracted by the BASC company linked in the supply chain; this linkage should define how the contracted supplier will secure the supply chain.

Supply chain graph



Once the business partners have been defined, criteria should be established with assessments according to risk to determine the level of criticality. It is suggested to adopt aspects related to responsibility, management, cargo information and the management of security seals, among others.

The security agreement formalizes a commitment of the business partner to implement and maintain controls that minimize the risks to which the company is

exposed, due to the product or service that it receives or delivers. For the preparation of security agreements, the company should first define the risks to which it is exposed when establishing the relationship with the business partner, according to the commercial sector.

To verify compliance with security agreements, companies should carry out second-party audits; this is a process carried out by the company to business partners, whose audit criteria are the controls implemented and commitments to minimize risks.

- Prevention of money laundering and financing of terrorism

Among the national and international lists, one can consider OFAC (Office of Foreign Assets Control), Clinton, United Nations (UN) List, European Union, Canadian List, FBI, local information lists of judicial process in execution, which are binding to business associates, among others.

The company can expand the information of negative press references (adverse media) on the reputation of companies and their members, as evaluation elements. The verification should be done for the shareholders, signatories, legal representative, attorneys-in-fact, board of directors, and management team of the company. When the business associate is a natural person, at a minimum, their criminal record should be checked. The legislation in force in each country should be taken into account, in accordance with the provisions of the Financial Analysis Units, for the prevention of crimes related to money laundering and terrorism.

The documented procedure should specify how the company will determine, based on the scope of the certification, the suspicious operations that could occur in the processes declared for the BASC CSMS. The company should periodically monitor for indications of suspicious operations according to the requirements mentioned in the criteria.

Reporting a suspicious operation does not require certainty of criminal activity, nor its type or that the resources involved come from such activities. Reports must be made to the relevant authority of each country.

• SECURITY OF CARGO UNITS AND CARGO TRANSPORT UNITS

- General

The individual performing the inspection should acquire the necessary training, experience and skill to be competent in carrying out this task. The inspection is focused on detecting hidden compartments, or in other words, points where illegal elements such as weapons, drugs, or cash can be hidden.

Each company is responsible for verifying cargo units and vehicles. Inspections in warehouses or cargo lots are directed in most cases to detect possible leaks, odors or traces of polluting elements. Each link in the chain should implement its own controls and have traceability of its operation.

The company should establish criteria for rejecting cargo units, such as dents, irregular structures, odors, undeclared repairs or welds, among others, in coordination with the shipping companies or warehouses, depending on the nature of the product to be transported and its requirements, among others. When suspicious repairs or modifications are identified, the company can perform a more intensive inspection with additional controls such as the use of technology or canines before rejecting the unit.

- Inspection of the cargo units

As the requirement of the Standard mentions, the inspection of the cargo unit should not be limited to the points that are listed.

In the case of refrigerated cargo units, also referred to as reefer containers, the inspection should include, in addition to the criteria listed in the requirement, the following:

- Roofs, which have thermal insulation devices.
- Welding, glue and rivets to detect alterations.
- Ventilation holes.
- The condenser and its quick opening mechanism; electrical control boxes; compressor and battery area, among others.

The company should consider factors related to the handling of air cargo during the palletizing and depalletizing processes, as well as ramp operations, when applicable.

- Inspection of cargo transport units

When cargo units are inspected, inspection of cargo transportation units should also be considered. This inspection is also focused on verifying the integrity of the transport unit and detecting hidden compartments, or in other words, points where potentially illegal elements can be hidden.

As mentioned in the requirement of the Standard, the inspection of the cargo transport unit should not be limited to the points that are listed.

- Cross contamination prevention and agricultural safety

The introduction of contaminants into the supply chain should be avoided. The company should verify that the cargo unit is free of pests, remains of waste and residues through controls during the inspection process.

When receiving and handling of empty containers, the company should carry out an internal and external verification of the container to ensure that it is free of any pest contamination.

The company should establish the means to apply this procedure during container loading and unloading operations.

- Traceability of cargo units and cargo transport units

Based on risk management, the company should include the following points in the documented procedure: authorized overnight stays, closure/sealing of the cargo unit with high security seals (ISO17712), authorized cargo personnel, photographic or film evidence, the proper record keeping, the timely reporting status, among others.

The driver should verify the integrity of the security seals installed at each overnight point and authorized stops along the route.

- Security seals

The company should contemplate in the documented procedure the inspection, storage, inventory, verification of the installation, protection and replacement of security seals. Likewise, it is important that this procedure considers:

- Maintaining records when it is necessary to replace a seal during transit, including the communication mechanisms and the reason for which it was replaced.
- Notifying incidents to shipping companies, customs authorities and other relevant interested parties, when there are anomalies in the handling of the corresponding seals and records.
- Documenting corrective actions when alterations, manipulations or incorrect numbers of seals are identified in the records.

If the cargo is examined by the authorities, consider the following actions:

- Documenting the replacement seal number.
- Immediately notifying the appropriate party of the replacement seal number when a seal is broken, indicating who broke it and why.

The company should ensure that the security seals have the certificates that guarantee that they have passed the tests required by ISO 17712.

Source: ISO 17712

- Route control

Route control refers to rigorous, real-time control over all areas of transportation and allows constant visibility on the transport of goods during the transfer processes between point-to-point routes.

To carry out route control, a good practice is to establish a schedule of approximate travel times; one could also establish "geofences", using a vehicle control tools that allows one to draw a virtual border perimeter to define geographic areas of interest, which allow the company to receive real-time notifications every time one of its GPS-enabled transportation mechanisms enters or leaves said territory.

It is important for the company to carry out periodic and random inspections without prior notice according to the identified risks, mainly considering places where cargo transport units are most vulnerable and maintaining evidence for the verification that the integrity of the units was verified.

- SECURITY IN CARGO HANDLING PROCESSES AND OTHER PROCESSES DEFINED IN THE SCOPE OF THE CSMS

Cargo handling processes are to be understood as the activities applied by the company to maintain the integrity of the cargo during production, manufacturing, packing, packaging, handling of the documentation handling and verification of the cargo.

- Parameters and criteria

The documented procedure should include operational controls at each point established for cargo handling. These points may be located in the company's own facilities or may belong to a business partner (producer, consolidation yard, collection center or third-party plants where these cargo handling processes are carried out).It is important to take into consideration the handling of the cargo at different points for filling a single cargo unit. Traceability is an integral part of the procedure in order to adequately respond to events and should include the documentary, photographic and/or film records (generated by the company or by its business partners), how the information is maintained / backed up and retention period.

- Raw material, packing and packaging material control

The documented procedure should include the identification of the person directly responsible for custody and inventory of the raw material, the packing and packaging material, as well as other elements to facilitate their storage and handling (pallets, etc.). Also, it should consider the essential traceability records defined for their control and management, including procedures in case of theft or loss of any of these materials, considering the respective report to the authorities, indicating the relevant information for proper identification (security coding, production dates, lot number, etc.). Consider methods for the proper disposal or destruction and safety checks of residues and waste at the time of exiting the facility's access point.

- Chemical Precursors and controlled substances

Chemical precursors and controlled substances are substances for commercial and industrial use that can be diverted from legally permitted use, to be used for illicit purposes. The documented procedure should consider risk management, in accordance with the applicable legislation (permits and authorizations), identifying those responsible for its custody and inventory, the traceability records that show

the operational controls applied to its proper management, as well as the procedures in case of theft, loss, or incidents, considering the timely reporting to the authorities. It should comply with environmental safety, work risk or other applicable regulations according to the legislation of each country.

- Controls in the cargo handling process

The cargo handling processes involve the company's own personnel and also those of its related critical business partners.

Each company carries out different activities that generate essential traceability records that jointly ensure integrity in the handling of cargo and cargo units while in storage. In this context, storage includes different locations or in different points of the same facility where there is direct contact with the loading unit, which on certain occasions is used as a storage unit until the moment of loading for export. It is necessary to identify the participants in the different activities, and they should carry out their activities in pre-determined sites that allow surveillance and traceability, for the assurance of the process, the cargo and cargo units.

Compliance with security agreements constitutes an effective tool for the proper control of these activities carried out by non-BASC certified business partners, to ensure the integrity of the processes.

- Information processing and cargo documents

In the event that the operational coordination activity for the handling of cargo documents and information is carried out by a business partner, the company should maintain direct control to ensure the integrity of the processes. If the business partner is not BASC certified, the security agreement should consider these requirements and the suggested procedures to secure sensitive information.

- Communication of suspicious activities or critical events

When a suspicious or unusual activity occurs that could affect the integrity of the operations, the company should inform the authorities and the BASC Chapter for record keeping, limiting the detail of the information in accordance with current legislation.

If the critical event materializes in any of the processes, the company should inform the pertinent authorities and carry out an in-depth analysis to identify the factors that could have caused the event.

In both cases, the BASC Chapter will cooperate with the company in evaluating the affected processes. It should be noted that the determination of an illicit act or the participation, commission or facilitation of an alleged crime, is an issue that falls solely to the control authorities in accordance with each country's legislation. Communication with the BASC Chapter or its cooperation does not exempt the company from its responsibilities to local authorities. Companies should train and raise awareness of the personnel responsible for communicating these activities.

- Controls in operational processes not related to cargo

Every company handles processes of an operational nature; these processes are part of the scope declared in the BASC CSMS. The company ensures the integrity of the processes and minimizes risks through procedures that involve operational controls, including traceability and information records, considering the storage times of these records for an adequate response to events. This criterion excludes industrial production processes, product formulas and any other sensitive information that does not refer to the scope of the BASC CSMS.

• PERSONNEL SECURITY

- Procedure for personnel management

Personnel is to be understood as direct employees, subcontracted personnel and temporary staff. BASC certified companies should have a code of ethics or conduct that establishes the ethical principles and values of the organization and make it known through awareness and training programs to raise awareness among employees and stakeholders. The company should consider compliance with local legislation.

- Personnel selection

The verifications may include the status of legal records in accordance with current legislation and the consent of the candidates. Official documents should be issued by the corresponding body.

Based on risk management, the verification should apply to subcontracted personnel or business partners (see BASC Standard Chapter 1) that will either directly or indirectly be part of the processes identified according to the scope of the BASC CSMS.

- Personnel hiring

The hiring of personnel is known as the closing phase of recruitment and selection, formalizing the entry of the collaborator into the company.

A good practice in this regard is to create a file for each employee with evidence of the recruitment and selection process. Likewise, this file should contain updated data on the candidate.

The candidate's induction process should include their responsibility and commitment to the BASC CSMS, according to their functions and level of criticality.

The company should verify that the data of the new employee is duly protected, and only accessible to authorized personnel.

- Personnel administration

Maintaining and following up on personnel information is an important aspect for the continuous improvement of the BASC CSMS. The frequency of the monitoring should apply to the level of criticality of the positions held by the employees.

The company should maintain documented information on changes and updates, providing permanent training to maintain the integrity of the CSMS.

If there are significant developments as a result of home visits or tests carried out, the corresponding procedure should be applied, and senior management should be notified.

- Personnel termination procedures

When an employee is terminated, it is important to monitor the resources assigned to him/her, as well as deactivate both physical and technological access at all levels of the organization.

The company should keep documented information on this process as evidence for BASC validations and in accordance with the provisions of local legislation for traceability purposes and possible investigation.

- Education, training, and awareness program

The company should periodically provide security training to employees, as required by their functions and positions, in accordance with the commitments made regarding the BASC CSMS. Newly hired employees should receive this training as part of their job orientation or induction.

This program should include training, education and awareness talks with defined objectives and aligned with the requirements of the BASC International Norm and Standards, in order to demonstrate the effectiveness of its application.

The company should maintain records that evidence the execution of these programs.

• ACCESS CONTROL AND PHYSICAL SECURITY

- Access control and permanence in the facility

It is recommended that a security perimeter be defined to protect critical areas through appropriate access controls to ensure that only authorized personnel are allowed to access.

• INFORMATION SECURITY

- Cybersecurity and information technology

The cybersecurity measures for the company should be proportional to the size, nature, criticality of the operations and business model.

Companies that use multi-factor authentication (MFA) access should take into account the distinct factors required for a successful verification of the user's identity.

The superuser or system administrator should be required to periodically deliver to senior management all access credentials to the computer systems and the tools

that are part of the technological infrastructure of the company.

BUSINESS ALLIANCE FOR SECURE COMMERCE

Miami, Florida.
United States of America

Design and Layout:
World BASC Organization

BUSINESS ALLIANCE FOR SECURE COMMERCE

World BASC Organization
www.wbasco.org