This manuscript includes two draft sections for edit and comment from a forthcoming book. The chapter sections are on Cybersecurity and ISO 28000 Supply Chain Security and ISO 28001 Supply Chain Security Risk Assessments. The forthcoming book is Supply Chain Management Introduction. Please use the Google Document link to edit or comment.

Google Document Link – for Edit and Comment:
https://docs.google.com/document/d/1buNiImS6kKoUC9mtcvkhuOTYSPmKQbTX/edit?usp=sharing&ouid=106328742619920569986&rtpof=true&sd=true

Reference: Spink, John, (In Press). Chapter 13/ Section 3: Cybersecurity in ISO 28000 Supply Chain Security, In Supply Chain Management Introduction: Sourcing, Operations & Logistics – including supply chain disruptions, and case studies of food fraud prevention, cybersecurity, and enterprise risk management, York Partners LLC (Publishing), ISBN 978-x-xx-xxxxxx-x, see www.ScmIntro.com.

////

Chapter 13: Cybersecurity

The sections from this chapter include:

1 Overview of Cybersecurity (based on the NIST requirements
2 Cybersecurity and ISO 27000 Information Security & 27032 Cybersecurity
3 **Cybersecurity in ISO 28000 supply chain security** (the role of the SCM manager in Cybersecurity) – includes an introduction to ISO 28000.
   - **Sub-Section: ISO 28001 Risk Thresholds and Rankings of High/Medium/Low**
4 Cybersecurity in ISO 22000 Food Safety Management
5 Summary and Call to Action

////

Chapter 13 – Section 3: Cybersecurity in ISO 28000 Supply Chain Security

This section is an overview of ISO 28000 Supply Chain Security, focusing on how it applies to cybersecurity and product fraud prevention.

- Reference: ISO, International Standards Organization (2007). ISO 28000:2007 Specification for security management systems for the supply chain, [Accessed January 15, 2022], URL: https://www.iso.org/standard/44641.html
- Reference: ISO/DIS, International Standards Organization (2021). Draft Status, ISO/DIS 28000:2021, Security and resilience — Security management systems — Requirements, [Accessed January 15, 2022], URL: https://www.iso.org/standard/79612.html

Overview of ISO 28000 Supply Chain Security

The International Standards Organization/ International Organization for Standardization (ISO) is a non-governmental organization (NGO) that is the internationally recognized leader in coordinating standards for the membership of 165 national standards bodies. The national standards bodies are the officially recognized representatives of governments. Standards development is initiated by request from the members who represent industry and governments, the request is assigned to a Technical Committee (TC) to begin the review, the TC work is based on global expert opinion, the TC uses a multi-stakeholder process to create a comprehensive scope and harmonized approach, and the development includes many reviews before a consensus of the TC and ISO results in a published standard. Several publication options include the draft status (DIS), urgent issue topic (PAS), and then the official publication.

There is an emphasis in the standards that compliance is to the implementation of the standard and is not a guarantee of product or process safety. The standard represents the best practices commonly recognized to reduce problems and help products and processes conform to expectations.

ISO 28000 Specification for Security Management Systems for the Supply Chain (Supply Chain Security) is an overarching management system published in 2007. This standard applies to all companies or organizations that create or update a security management system (including large or small companies, governments, other public entities, or non-profit organizations). As of July 2021, the public discussion period closed, and the voting terminated in May 2021, but the final results were not public. The updated standard is expected to be published in 2022. This update is focused primarily on adapting the format to a more general ISO template (so the major themes should not change). [1] The primary objective of the update is not a substantive update but more of a format change to align with the "High-Level Structure" for Management Systems Standards (MSS).

The ISO 28000 series of standards integrate with other related ISO standards such as ISO 9000 Quality Management, ISO 31000 Risk Management, ISO 27000 Information Technology Security, and ISO 22380 Product Fraud Risk. [2-5] ISO 28002 explicitly outlines the combination of security, crisis, and business continuity programs. [6] From ISO TC292: "the core text for the scope is basically as it was in the prior version, and the intension has been to keep the requirements from the old version as intact as possible." Two significant changes include: (1) clarifying the alignment with terminology in ISO 31000 Risk Management and (2) adjustments for alignment with ISO 22301 Business Continuity Management processes and security plans. [7] The goal is that compliance from the 2007 version will be seamless to the new version.

The 2007 publications mention information technology and communication equipment, but they do not specially mention cybersecurity (sometimes presented as cyber-security). The cybersecurity concept was first defined five years after ISO 28000 was published in ISO/IEC

27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. New updates often now mention cybersecurity and cyberthreats, such as the 2018 update of ISO 22000 Food Safety Management.

ISO 28000 is managed under ISO Technical Committee 292 (TC 292) in Working Group 8 Supply chain security (WG8). [8] In addition to the ISO 28000 series under WG8, the ISO/TC 292 currently has the following activities:

- Working Group 1: Terminology
  - ISO 22300 Security and resilience – Vocabulary
  - ISO/TS 22375 Security and resilience – Guidelines for complexity assessment process
- Working Group 2: Continuity and organizational resilience
  - ISO 22301 Security and resilience – Business continuity management systems – Requirements
  - ISO/TS 22318 Societal security – Business continuity management systems – Guidelines for supply chain continuity [under revision]
- Working Group 3: Emergency management
  - ISO 22320 Security and resilience – Emergency management – Guidelines for incident management
  - ISO 22322 Societal security – Emergency management – Guidelines for public warning
- Working Group 4: Authenticity, integrity, and trust for products and documents
  - ISO 22380 Security and resilience – Authenticity, integrity, and trust for products and documents – General principles for product fraud risk
  - ISO 22381 Security and resilience – Authenticity, integrity, and trust for products and documents – Guidelines for interoperability of product identification and authentication systems
  - ISO 22383 Security and resilience – Authenticity, integrity, and trust for products and documents – Guidelines and performance criteria for authentication solutions for material goods
    - ISO 12931:2012 Performance criteria for authentication solutions used to combat counterfeiting of material goods [replaced by ISO 22383:2020]
  - ISO 22384 Security and resilience – Authenticity, integrity, and trust for products and documents - Guidelines to establish and monitor a protection plan and its implementation
  - ISO 16678 Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade* [under revision as ISO 223nn]

- Working Group 5: Community resilience
- Working Group 6: Protective security
    - ISO 22341 Security and resilience – Protective Security – Guidelines for crime prevention through environmental design
- Working Group 7: Guidelines for events
- Working Group 8: Supply chain security [resources listed above]
- Working Group 9: Crisis management
    - ISO 22316 Security and resilience – Organizational resilience – Principles and attributes
- Joint Working Group 1: Managing emerging risk (Joint work with ISO/TC 262)
    - ISO 31050 Risk management - Guidance for managing emerging risks to enhance resilience

Other sub-standards in the ISO 28000 family provide more detailed guidance, including. ISO 28000 is the overall concept, and then more details are provided in numbered codes within this number, such as 28001, 28002, 28003, and 28004.

- ISO 28000 Specification for security management systems for the supply chain [under revision, July 2021]
- ISO 28001 Security management systems for the supply chain – Best practices for implementing supply chain security, assessments, and plans – Requirements and guidance
- ISO 28002 Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use
- ISO 28003 Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems
- ISO 28004 Security management systems for the supply chain – Guidelines for the implementation of ISO 28000

Within the ISO 28000 family, the sub-standards each have a vital role in explaining the intent and guidance on implementation and compliance. The series is often referred to as ISO 28000, but a specific published document is often referred to with the publication year, such as ISO 28000:2007.

ISO 28000:2007 (Reconfirmed in 2021) – The Overview

ISO 28000 begins with the scope of the supply chain and related security.

- "ISO 28000:2007 specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain.

Organizations that choose third-party certification can further demonstrate that they contribute significantly to supply chain security.

- ISO 28000 is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:
  - a) establish, implement, maintain and improve a security management system;
  - b) assure conformance with stated security management policy;
  - c) demonstrate such conformance to others;
  - d) seek certification/registration of its security management system by an Accredited third-party Certification Body; or
  - e) make a self-determination and self-declaration of conformance with this standard." [1]

The standard includes several key definitions that help define the scope (see the Appendix at the end of this section). There were several key updates or clarifications in ISO/DIS 28000:2021 update regarding the term. The most significant was that the term "facility" – referring to a physical facility – was changed to "organization." This clarifies that the control measures are expected to cover and calibrate the entire organization and not just one physical facility.

ISO 28001:2007 (reconfirmed in 2021) – Conducting Assessments

ISO 28001 provides more detail on "Best practices for implementing supply chain security, assessments and plans - Requirements and guidance." This was reviewed and confirmed in 2021, so the 2007 version remains current. This specifically includes:

- "Define the portion of an international supply chain within which they have
  - established security;
  - conduct security assessments on that portion of the supply chain and develop adequate countermeasures;
  - develop and implement a supply chain security plan, and
  - train security personnel in their security-related duties."

This content includes recommendations for conducting the assessments. The processes preceded but are consistent with ISO 31000 Risk Management. There are suggestions for high/medium/low likelihood and consequence rankings. This includes recommendations for the selection, implementation, and monitoring of countermeasures. (See the next section for more details regarding the assessment method and risk rankings for likelihood and consequence.)

ISO 28002: 2011 (reconfirmed in 2021) – Managing the System

ISO 28002 provides more detail on "Development of resilience in the supply chain - Requirements with guidance for use."

Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use

- "The survivability of organizations within a supply chain depends largely on the resilience of their suppliers and customers. As a result, incorporating resilience, and improving the resilience of an organization within the supply chain, must be focused both within the organization and externally on its suppliers and customers.
- "During a supply chain disruption, it must be emphasized that the exact nature of the disruption will probably not be fully understood at first and may only become fully understood over time. As a result resilience plans and policies developed should stress adaptation and continual evaluation of new information to ensure actions being taken are appropriate. Supply chain disruptions of sufficient magnitude will most likely attract the news media. Failure to properly manage news media relations can negatively impact resiliency response operations, resulting in a loss of stakeholder confidence."

The recommendations are an adaption from other standards and the Demming Wheel of Plan-Do-Check-Act (Table 1):

- "Establish a Supply Chain Resilience Program and Apply Resources
- Define the Supply Chain and Resilience Objectives
- Identify Supply Chain Risks
- Quantify and Prioritize Risks
- Execute Risk Treatment Programs
- Monitor Supply Chain Environment for Risks"

Table 1: Explanation of the Plan-Do-Check-Act (PDCA) Model from ISO 28000:2022 (including the identification from the specification as "Table 1" (REF 28000:2022)

Table 1 — Explanation of the PDCA model

Plan (Establish)	Establish security policy, objectives, targets, controls, processes and procedures relevant to improving security in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the security policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against security policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the security management system by taking corrective action, based on the results of management review and reappraising the scope of the security management system and security policy and objectives.

Also, the integrated activities our explained (Figure 1): (ref iso28000:2022)

Figure 1 — PDCA model applied to the security management system

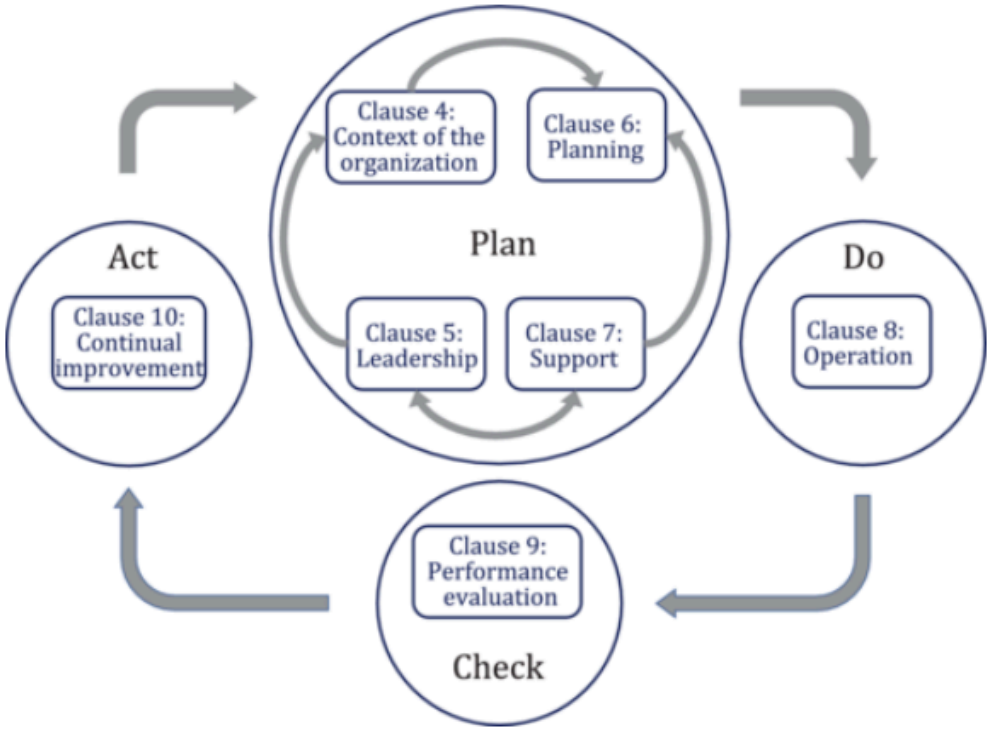

Figure 1: Presentation of the Plan-Do-Check-Act (PDCA) Model Applied to the Security Management System (including the identification from the specification as "Figure 1") (REF: iso 28000:2022)

ISO 28003:2007 (confirmed in 2016) – Audit and Certification

ISNO 28003:2007 provides more detail on "Requirements for bodies providing audit and certification of supply chain security management systems." Essentially this offers more

guidance on certifying compliance with the ISO 28000 series. The intent is to provide common or harmonized audit and certification methods and levels of implementation. This is valuable to the auditor and sets the expectations for those customers who are being audited and certified. The audit and compliance process includes: (1) a document review before the on-site activities, (2) Certification Audit Stage 1 and stage 2, (3) Surveillance audits every 12 months, and (4) Recertification Audit after three years (see auditor details. [9, 10]

ISO 28004:2004 (four parts) – Guidance for Implementation

ISO 28004 provides more detail on "Guidelines for the implementation of ISO 28000." This includes helpful suggestions for ways to implement the standard. Four parts apply to different situations or businesses. Part 1 is an overview of implementation guidance. For example, part 3 of 4 provides "Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)."

Summary

ISO 28000 provides broad insight and guidance for managing the security of the supply chain. For cybersecurity, there is no specific mention. Still, there is an insinuation that it is covered as part of the overall "information tampering" concept as it applies to disrupting the physical facility operations. For product fraud prevention, there is no specific mention and could apply – though product fraud is not intended as an attack – under "cargo integrity."

Section II

Sidebar: ISO 28001 Risk Thresholds and Rankings of High/Medium/Low

Considering the application to cybersecurity and specific risk assessment rankings, this is a deeper of ISO 28001 Security management systems for the supply chain — Best practices for implementing supply chain security, assessments, and plans. [11] The ISO 28001 standard was published in 2007 and reconfirmed in 2021 (e.g., in 2021, the 2007 version was determined not to need to be updated).

ISO 28001 is a sub-standard within the overall management system family of ISO 28000. Applicable to this chapter on cybersecurity, ISO 28001 provides insight on assessments and risk rankings.

- Reference: ISO, International Standards Organization (2007). Security management systems for the supply chain — Best practices for implementing supply chain security, assessments, and plans — Requirements and guidance, [Accessed January 15, 2022], URL: https://www.iso.org/standard/45654.html

Review of Key Terms and Definitions

Each standard includes a list of terms and definitions. The base for most of the definitions are from ISO/PAS 20858 Maritime port facility security assessments and security plan and ISO 31000 Risk Management.

The complete definitions are provided at the end of this section. They include conveyance (how a product is moved, such as a box or truck), countermeasures, downstream, goods (material goods), likelihood, management system, security plan, security, supply chain, target, security threat scenario, and upstream (see Appendix at the end of this section).

Implementation, Documentation, and Assessment of the supply chain security plan

ISO 28001 defines the documentation and monitoring required for a supply chain security plan. The guidance is general and high level. This standard includes overall requirements, no prescribed actions, or definitive risk ranking thresholds.

- Security Plan Implementation and Documentation:
  - "The organization shall establish and maintain procedures to document, monitor, and measure the performance of its management system referred to above. The organization shall carry out audits of the management system at planned intervals to ensure it has been properly implemented and maintained. The results of audits shall be documented and retained."
- Continual Improvement:
  - "The organization shall assess opportunities for improving its security arrangements to enhance the security of its portion of the supply chain."
- Actions required after a security incident:
  - "The organization shall carry out a review of its security plan after the occurrence of any security incident that relates to any portion of the international supply chain the organization controls.
- After Security Incident Review components:
  - "This review shall a) determine the cause of the incident and the corrective action; b) determine the effectiveness of measures and procedures for security recovery; and c) consider such determinations, re-assess those portions of the supply chain."

Together these provide a foundation for the management system.

Scope of ISO 28001 Focuses on Physical Facilities and Material Goods

The ISO 28000 series primarily focuses on the legitimate supply chain's physical facilities and material goods. The examples in the standard provide insight into the intended scope of activities. The key overall questions include:

"Goods and Conveyance Security questions:

- Are procedures in place to restrict, detect, and report unauthorized access to all shipping, loading dock areas, and closed cargo transport unit storage?
- Are qualified persons designated to supervise cargo operations?
- Are procedures in place for notifying appropriate law enforcement in cases where anomalies or illegal activities are detected or suspected by the organization?
- Are procedures in place to ensure the integrity of the goods/cargo when the goods/cargo are delivered to another organization (transportation provider, consolidation center, intermodal facility, etc.) in the supply chain?
- Are processes in place to track changes in threat levels along transport routes?"

The standard provides questions but no further clarity, such as what is a "qualified person."

Scope of ISO 28001 Presents Threat Scenario Likelihood and Consequence Examples

The scenarios and examples of likelihood and consequences provide insight into the scope (e.g., the specific threat scenarios). As shown in Table 2, the scenarios focus on access to physical facilities and legitimate products.

The main focus of the examples is on terrorist acts –intentional acts with the intent to cause public health or economic harm or terror. Note: there is no definition or explanation of "terror" or "terrorism" (for more, see the Food Defense section).

Cybersecurity could be considered included under "Information Tampering" with the example of "…gaining access to the supply chain's information/documentation systems to disrupt operations or facilitate illegal activities. Almost all types of product fraud – intentional deception for economic gain using a product – are outside the scope of this standard. Broadly, "cause civil or economic disturbance" could include product fraud, but considering the other examples, that scope is not for economic gain by the criminal.

Table 2: List of Security Threat Scenarios to the Supply Chain ((including the identification from the specification as "Table B.1") (REF: iso 28000:2022)

Table B.1 — Security threat scenarios to the supply chain

Example security threat scenarios	Application example
1 Intrude and/or take control of an asset (including conveyances) within the supply chain.	Damage/destroy the asset. Damage/destroy outside target using the asset or goods. Cause civil or economic disturbance. Take hostages/kill people.
2 Use the supply chain as a means of smuggling	Illegal weapons into or out of the country/economy Terrorist into or out of the country/economy
3 Information tampering	Locally or remotely gaining access to the supply chain's information/documentation systems for the purpose of disrupting operations or facilitating illegal activities.
4 Cargo Integrity	Tampering, sabotage and/or theft for the purpose of terrorism
5 Unauthorized use	Conducting operations in the international supply chain to facilitate a terrorist incident (e.g. using the means of transport as a weapon)
6 Others	

Classification of Consequence: High/ Medium/ Low

The standard measures the consequence in terms of loss of life and economic loss. There is a clear and emphatic recommendation to use qualitative terms of high/ medium/ low. Also, this scale is further emphasized by the statement that "A numerical system may be used in the assessment process, as long as the numerical results are converted to a qualitative system." This is consistent with ISO 31000 Risk Management, which states that numbers should only be used when a statistical probability is derived. A numerical system is appropriate if there are underlying quantitative and statistically significant data. Often, risk ranks are based on qualitative assessments or expert insight. For example, if to risk ranks are "5" and "7," then there is an insinuation of at least one significant figure. If further detail such as "5.5" and "5.6" are used, there is a further insinuation of at least two significant figures. ISO 28001, following guidance from ISO 31000, recommends that qualitative assessment such as high/ medium/ low is usually most appropriate when explaining the results of the data.

ISO 28001 provides very general differences in the risk ranks:

- "A "high" consequence classification may be considered as a consequence that would be unacceptable in all but low likelihood situations.
- A "medium" classification of consequence may be considered as a consequence that would be unacceptable in a high likelihood situation.
- A "low" classification of consequence may be considered as a consequence that is normally acceptable."

ISO 31000, COSO/ ERM, and others often recommend a five-rank system with "very high" and "very low" to represent a wider dispersion of close to 100% and 0%. The use of "very high" and "very low" provides more variation in the middle of the rank.

It is crucial to emphasize that all adverse events are bad and undesirable and a recognition that the goal is not "zero-risk." "Acceptability should not be confused with desirability or approval. Rather, acceptability could be considered a judgment of the amount of possible damage that the organization or government under which it is operating is willing to accept under certain conditions related to probability."

The details of the consequences are very general, such as High: "Death & Injury – loss of life on a certain scale" or Low: "Death & Injuries – injuries but no loss of life." No category includes no loss of life or no injuries (Table 3). To note, in all cases, product fraud would be a "low" consequence.

Table 3: Classification of Consequence for List of Security Threat Scenarios to the Supply Chain (including the identification from the specification as "Table B.2") (REF: iso 28000:2022)

Table B.2 — Classification of consequence

Assign a rating	Consequence
High	**Death & Injury** - loss of life on a certain scale **and /or** **Economic Impact** - major damage to a asset and/or infrastructure preventing further operations **and /or** **Environmental Impact** - complete destruction of multiple aspects of the eco-system over a large area
Medium	**Death & Injury** - for example loss of life **and /or** **Economic Impact** – for example damage to asset and/or infrastructure requiring repairs **and /or** **Environmental Impact** – for example long term damage to a portion of the eco-system
Low	**Death & Injury** – injuries but no loss of life, **and /or** **Economic Impact** - minimal damage to a asset and/or infrastructure and systems, **and /or** **Environmental Impact** – some environmental damage

Classification of Likelihood of Supply Chain Security Incidents

There is even less direction on the likelihood risk ranks.

- High likelihood: "should be used when the security measures in place offer little resistance to the security incident occurring. If a numerical system is used in the assessment process, the numerical results should be converted into this qualitative system."
- Medium likelihood: "should be used when the security measures in place offer moderate resistance to the security incident occurring."
- Low likelihood: "should be used in cases where the security measures in place offer substantial resistance to the security incident occurring."

The standard provides general statements but no further clarity, such as what is a "substantial resistance."

Security Incident Scoring and Risk Treatment

The incident scoring is used to assess specific threats. The threat assumes a "motivated offender," This physical facility and product are the intended target. The threat has a potential consequence and then likelihood. A generic scoring chart is provided that includes countermeasures (implement an action that reduces the risk to an acceptable level), consider, countermeasure or consider as appropriate, and document (do nothing except assess the problem).

The countermeasures include the following actions that are consistent with ISO 31000 Risk Management:

- "**Treat:** This may be organizational and/or physical measures.
- **Transfer:** The transfer of the risk may be subcontracting, physical transfer to other locations, time, etc.
- **Terminate:** It is possible that due to the level of risk, the organization decides not to continue the activities.
- **Tolerate:** The situation is such that no action can be taken by the organization. In certain circumstances an organization may have to tolerate (see note) a risk due to impracticality of the countermeasures needed, lack of authority to impose the countermeasures needed or other insurmountable factors."

Summary

ISO 28001 provides an internationally recognized set of terms, recommendations, and risk assessment insight important for the supply chain management introduction. Further, this is important to review in terms of supply chain disruptions and cybersecurity. A key finding is that ISO 28000 and ISO 28001 are fundamentally aligned with the other general risk management systems such as ISO 9000, ISO 31000, and COSO/ERM. This section provided more insight and guidance on conducting risk assessments, ranking, and deciding on the risk treatment.

Section III

Appendix: for Sidebar Section on ISO 28000 – Terms and Definitions

The terms and definitions are from: ISO 28000:2007, ISO/DIS 28000:2021 (a draft of the next update scheduled for 2022), ISO 28001:2007, ISO 22380, and Guide 73. [Note: the ISO document reference is included with the term.]

- **Asset** (ISO 22380): anything that has value to the organization; Note 1 to entry: Assets include but are not limited to human, physical, information, intangible, and environmental resources.
- Assets (ISO 28001): are plant, machinery, property, buildings, vehicles, ships, aircraft, conveyances, and other items of infrastructure or plant and related systems that have a distinct and quantifiable business function or service.
- **Competence** (ISO/DIS 28000:2021): ability to apply knowledge and skills to achieve intended results effectiveness extent to which planned activities are realized and planned results achieved
- **Continual improvement** (ISO/ DIS 28000:2021): r recurring process of enhancing the security management system in order to achieve improvements in overall security performance consistent with the organization's security policy
- **Conveyance (ISO 28001):** a physical instrument of international trade that transports goods from one location to another; EXAMPLE: Box, pallet, cargo transport unit, cargo handling equipment, truck, ship, aircraft, and railcar.
- **Countermeasures (ISO 28001):** actions taken to lower the likelihood of a security threat scenario succeeding in its objectives, or to reduce the likely consequences of a security threat scenario
- **Disaster** (ISO 22380): event that causes great damage or loss
- **Disruption** (ISO 22380): anticipated or unanticipated event that interrupts normal functions, operations, or processes (e.g., severe weather, political or labour unrest, utility outage, criminal/terrorist attack, technology failure, or earthquake); Note 1 to entry: A disruption

can be caused by either positive or negative factors that will disrupt normal functions, operations, or processes.

- **Downstream (ISO 28001):** handling, processes and movements of goods when they no longer are in the custody of the organization in the supply chain

- **Facility** (ISO 22380): plant, machinery, property, buildings, transportation units, sea/land/airports, and other items of infrastructure or plant and related systems that have a distinct and quantifiable business function or service
- **Facility** (ISO 28000:2007 in ISO/ DIS 28000:2021 the focus shifted to the "organization"): plant, machinery, property, buildings, vehicles, ships, port facilities and other items of infrastructure or plant and related systems that have a distinct and quantifiable business function or service.
- **Goods (material goods) (ISO 28001):** those items or materials that, upon the placement of a purchase order, are being manufactured, processed, handled or transported within the supply chain for usage or consumption by the purchaser

- **Hazard** (ISO 22380): source of potential harm [SOURCE: ISO Guide 73:2009, definition 3.5.1.4]; Note 1 to entry: A hazard can be a risk source.
- **Incident** (ISO 22380): event that has the capacity to lead to human, intangible or physical loss, or a disruption of an organization's operations, services, or functions, which, if not managed, can escalate into an emergency, crisis, or disaster
- **Integrity** (ISO 22380): property of safeguarding the accuracy and completeness of assets

- **Likelihood (ISO 28001):** ease or difficulty with which a security threat scenario could progress to become a security incident; Note 1 to entry: Likelihood is evaluated based on the resistance the security processes in place pose to a security incident involving the security threat scenario being examined and is expressed either qualitatively or quantitatively.
- **Management system (ISO 28001):** organization's structure for managing its processes or activities that transform inputs of resources into a product or service, which meet the organization's objectives; Note 1 to entry: It is not the intent of this International Standard to specify a specific management system or require the creation of a separate security management system. ISO 9001 (Quality Management Systems), ISO 14001 (Environmental Management Systems), ISO 28000 (Security management systems for the supply chain), and the International Maritime Organization’s International Safety Management (ISM) Code are examples of management systems.

- **Mitigation** (ISO 22380): limitation of any negative consequence of a particular incident

- **Organization** (ISO/DIS 28000:2021, 3.1 – note: changed from facility in ISO 28000:2007): person or group of people that has its own functions with responsibilities, authorities, and relationships to achieve its objectives. Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority,

partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

- **Prevention** (ISO 22380): measures that enable an organization to avoid, preclude, or limit the likelihood or consequences of a disruption
- **Prevention of Hazards and Threats** (ISO 22380): process, practices, techniques, materials, products, services, or resources used to avoid, reduce, or control hazards and threats and their associated risks of any type in order to reduce their potential likelihood or consequences
- **Preventive Action** (ISO 22380): action to eliminate the cause of a potential nonconformity or other undesirable potential situation; Note 1 to entry: There can be more than one cause for a potential nonconformity; Note 2 to entry: Preventive action is taken to prevent occurrence whereas corrective action is taken to prevent recurrence.
- **Security** (ISO 22380): condition of being protected against hazards, threats, risks, or loss; Note 1 to entry: In the general sense, security is a concept similar to safety. The distinction between the two is an added emphasis on being protected from dangers that originate from outside.
  - **Security** (ISO 28000): resistance to intentional, unauthorized acts designed to cause harm or damage to, or by, the supply chain.
  - **Security (ISO 28001):** resistance to intentional acts designed to cause harm or damage to or by the supply chain
  - Security (ISO 28001): means the resistance to intentional acts designed to cause harm or damage to or by the supply chain
  - **Security Management** (ISO 28000): systematic and coordinated activities and practices through which an organization optimally manages its risks, and the associated potential threats and impacts there from.
  - **Security Management Objective** (ISO 28000): specific outcome or achievement required of security in order to meet the security management policy.
  - **Security Management Target** (threshold, goal) (ISO 28000): specific level of performance required to achieve a security management objective.
  - **Security plan (ISO 28001):** planned arrangements for ensuring that security is adequately managed; Note 1 to entry: It is designed to ensure the application of measures that protect the organization from a security incident; Note 2 to entry: The plan can be incorporated into other operational plans.
  - **Security Threat Scenario (ISO 28001):** means by which a potential security incident might occur
  - **Supply Chain** (ISO 28000): the linked set of resource and processes that begins with the sourcing of raw material and extends through the delivery of products or services to the end user across the modes of transport. The supply chain may include vendors, manufacturing

facilities, logistics providers, internal distribution centers, distributors, wholesalers and other entities that lead to the end user.

- **Supply chain (ISO 28001):** linked set of resources and processes that upon placement of a purchase order begins with the sourcing of raw material and extends through the manufacturing, processing, handling and delivery of goods and related services to the purchaser; Note 1 to entry: The supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers and other entities involved in the manufacturing, processing, handling and delivery of the goods and their related services.
- Supply chain (ISO 28001): is the linked set of resources and processes that upon placement of a purchase order begins with the sourcing of raw material and extends through the manufacturing, processing, handling and delivery of goods and related services to the purchaser. NOTE The supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers and other entities involved in the manufacturing, processing, handling and delivery of the goods and their related services.

- **Target** (ISO 22380): detailed performance requirement applicable to the organization (or parts thereof) that arises from the objectives and that needs to be set and met in order to achieve those objectives; Note 1 to entry: Adapted from ISO 14001:2004, definition 3.12.
  - **Target (ISO 28001):** personnel, means of transport, goods, physical assets, manufacturing processes and handling, control or documentation systems within an organization in the supply chain
- **Testing** (ISO 22380): activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria; Note 1 to entry: Testing usually involves exercises designed to keep teams and employees effective in their duties, and to reveal weaknesses in the preparedness and response/continuity/recovery plans.
- **Threat** (ISO 22380): potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization, the environment, or the community
  - **Upstream (ISO 28001):** handling, processes and movements of goods that occur before the organization in the supply chain takes custody of the goods
- **Vulnerability** (ISO 22380): intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence. [SOURCE: ISO Guide 73:2009, definition 3.6.1.6.]
- **Vulnerability Assessment** (ISO 22380): process of identifying and quantifying vulnerabilities

Section IV

References

1. ISO, International Organization for Standardization, *The new draft of ISO 28000 available for public review, ISO/ TC 292 Online Website,*. 2021.
2. ISO, International Organization for Standardization. *ISO/IEC 27000:2012, Information technology -- Security techniques -- Information security management systems*. 2012; Available from: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56891.
3. ISO, International Organization for Standardization, *ISO 9000: 2015 Quality management systems -- Fundamentals and vocabulary, International Standards Organization (ISO), URL: https://www.iso.org/standard/45481.html.* 2015.
4. ISO, International Organization for Standardization, *ISO 31000:2018 Risk management -- Guidelines, URL: https://www.iso.org/standard/65694.html.* 2018.
5. ISO, International Organization for Standardization, *ISO 22380:2018 Security and resilience -- Authenticity, integrity and trust for products and documents -- General principles for product fraud risk and countermeasures, Status: Published, Publication date: 2018-08-22 URL: https://www.iso.org/standard/73857.html.* 2018.
6. ISO, International Organization for Standardization, *ISO 28002:2011 Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use, [Accessed January 15, 2022], URL: https://www.iso.org/standard/56087.html.* 2011.
7. ISO, International Organization for Standardization, *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements, [Accessed January 15, 2022], URL: https://www.iso.org/standard/75106.html.* 2019.
8. ISO, International Organization for Standardization, *ISO/TC 292 Online Webpage, Organization - Activities by Working Group, [Accessed January 15, 2022], URL: https://www.isotc292online.org/organization/working-group-8/.* 2022.
9. TUV SUD, *ISO 28000 Certification Mark, web page,[Accessed January 15, 2022], URL: https://www.tuvsud.com/en-us/services/auditing-and-system-certification/management-system-certification-marks/iso-28000.* 2022.
10. ISO, International Organization for Standardization, *ISO 28003:2007 Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems [Accessed January 15, 2022], URL: https://www.iso.org/standard/45416.html.* 2007.
11. ISO, International Organization for Standardization, *ISO 28001:2007 Security management systems for the supply chain — Best practices for implementing supply*

chain security, assessments, and plans — Requirements and guidance, [Accessed January 15, 2022], URL: https://www.iso.org/standard/45654.html. 2007. /END/