FFI Report

Review of Terms and Definitions Related to Supply Chain Management for disruption, disaster, and interruption with a focus on ISO definitions compared to common usage (Working Paper)

February 15, 2025

By John W Spink

ABSTRACT

This report reviews the definitions of "disruption," "disturbance," "disaster," and "interruption" within the context of supply chain management, focusing on ISO standards. The research highlights terminology from International Standards Organization (ISO) Technical Committee 292[1] on Security and Resilience, emphasizing definitions that influence supply chain operations. By comparing ISO definitions with common usage, the study clarifies the varying applications of these terms.

Key findings reveal that "supply chain disruption" is the primary term representing incidents causing unplanned deviations from expected operations, regardless of predictability. Disasters often involve severe, long-term impacts, whereas disturbances usually describe minor, short-term interruptions. Insights from industry literature, including Gartner, illustrate how natural disasters, political instability, labor strikes, or cyberattacks frequently cause supply chain disruptions.

After thorough analysis, "supply chain disruption" is identified as the most precise and widely applicable descriptor for interruptions affecting the flow of goods and services.

[1] The author is a voting member of ISO TC 292 Work Group 1 on vocabulary (ISO 22300), Work Group 2 on product authentication (ISO 22380 series), and Work Group 3 on physical security (ISO 28000 and others). He is also a voting member of ISO/TC 34 Food Products / Sub-Committee 17 Management systems for food safety (ISO 22000).

INTRODUCTION

This project examines the definitions of key supply chain management terms, including "disruption," "disturbance," "disaster," and "interruption." The goal is to provide a clearer understanding of these terms based on ISO definitions, academic research, and industry practices, particularly in the context of supply chain risk management and disruption analysis.

Keywords: Supply Chain Management, Supply Chain Disruption, ISO Definitions, Supply Chain Risk Management, Business Continuity, Security and Resilience, Food Safety, Food Defense, Food Fraud, Food Authenticity

BACKGROUND

The International Standards Organization (ISO) publications were the primary resource since they are consensus-based, international, and official government-endorsed decisions. The ISO standards are developed by experts to address the world's most pressing matters. This ISO focus was supported by a review of the common definitions of the terms.

There are two research tracks, one on 'supply chain management' and another on 'disruptions.' Broadly, ISO Technical Committee 292 on Security and Resilience covers both supply chain security and resistance to disruptions.

ISO/TC 292, Security and Resilience, develops international standards to enhance organizational security, preparedness, and resilience against disruptions such as natural disasters, cyberattacks, and supply chain interruptions. Its standards address risk management, business continuity, emergency management, and protective security, providing a structured framework for organizations to identify threats, mitigate risks, and ensure operational continuity.

In supply chain management, ISO/TC 292 standards play a critical role in safeguarding global logistics networks. Standards like ISO 28000 help organizations assess security risks within their supply chains, implement protective measures, and build resilience against potential disruptions. By fostering a proactive, risk-based approach, these standards enhance supply chain visibility, improve incident response, and promote collaboration across stakeholders.

METHOD

This project was conducted to review definitions of Supply Chain Management related terms of disruption, disturbance, disaster, and interruption. During the review, there was a focus on any general supply chain-related terms. This will also be compared to an everyday use of Webster's Dictionary. This identifies the core references for ISO Technical Committees and Standards. Also, there was a review of additional terms for further research. Previous projects reviewed terms including event, incident, hazard, threat, risk, and vulnerability.

The results are specifically and only from the formal "Terms & Definitions" section of the standards. These are formal and rigorously refined definitions from experts from across all ISO, not just from the Technical Committee or Work Group.

ChatGPT assisted in the data collection, preliminary analysis, and categorization phases.

RESULTS and DISCUSSION (Part 1: ISO Definitions)

The results will be presented in order of the research on each term.

It was found that ISO Technical Committee 292 on Security and Resilience was found to be the most direct ISO resource. TC 292 includes ISO 22300:2021 - Security and Resilience — Vocabulary is the primary reference, as well as the ISO 22301 Business Continuity series and ISO 28000 Supply Chain Security series.

Disruption Term and Definition

All definitions are direct quotes. Numbers in the definitions refer to definitions of those terms.

The common usage dictionary definition from Webster's is provided as is the most directly applicable ISO definition:

- **Disruption** (Webster's Definition): "The act or process of interrupting the normal course of something; a break or interruption in a normal activity."
- **Disruption** (ISO Definition): " incident (3.1.122), whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services (3.1.192) according to an organization's (3.1.165) objectives (3.1.162)."(ISO 22300:2021(en), 3.1.75 Security and resilience — Vocabulary)

Key insight: This is a broad definition that holistically covers supply chain concerns.

Other definitions or applied terms that provide insight are:

- Disruption: incident, whether anticipated (e.g., hurricane) or unanticipated (e.g., power failure/outage, earthquake, or attack on ICT systems/infrastructure) which disrupts the normal course of operations at an organization location; ISO/IEC 27031:2011(en), 3.6 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity
- maximum tolerable period of disruption/ MTPD/ maximum acceptable outage/ MAO: the time it would take for adverse impacts (3.1.118), which can arise as a result of not providing a product/service or performing an activity (3.1.2), to become unacceptable; ISO 22300:2021(en), 3.1.151

Disturbance Term and Definition

The common usage dictionary definition from Webster's is provided as is the most directly applicable ISO definition:

- **Disturbance** (Webster's Definition): "The act of interfering with or creating disorder; a state of being disturbed."
- **Disturbance** (ISO Definition): "a malfunction of a piece of equipment that loses its capability to work properly for the duration of the interference (3.15); Note 1 to entry: When the interference disappears, the interfered system (3.7) starts working properly again without any external intervention." (ISO 18086:2019(en), 3.16 Corrosion of metals and alloys — Determination of AC corrosion — Protection criteria.)

Key insight: this ISO definition is from a manufacturing process standard not from supply chain or business management. This appears to be a type of disruption where the systems automatically return to normal conditions.

Other definitions or applied terms that provide insight are:

- Disturbance: operational fault (e.g., an abrupt shutdown of an operating system process that brings down a system) or event (e.g., a significant increase of users to the system), or anything that could change the state of the system; Note 1 to entry: For the context of this evaluation module, the disturbances are limited to external faults or events, rather than internal faults that required modifying the application or OS code; ISO/IEC

25045:2010(en), 4.2 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation module for recoverability

- Disturbance: involuntary action which results in a modification in the flight state (3.1.2); Note 1 to entry: The nature of this action can be, for example: human; atmospheric; mechanical; ISO 1151-8:2022(en), 3.1.8 Flight dynamics — Vocabulary — Part 8: Dynamic behavior of aircraft.

Disaster Term and Definition

The common usage dictionary definition from Webster's is provided as is the most directly applicable ISO definition:

- **Disaster** (Webster's Definition): "a sudden event marked by great loss and lasting distress and suffering bringing great damage, loss, or destruction."
- **Disaster** (ISO Definition): "a situation where widespread human, material, economic, or environmental losses have occurred which exceeded the ability of the affected organization, community, or society to respond and recover using its own resources." (SOURCE: ISO 22300:2012, 2.1.11)

Key insight: This ISO definition is from the security and resilience vocabulary and seems to be a type of very severe disruption.

Other definitions or applied terms that provide insight are:

- Disaster control plan, disaster recovery plan: document (3.1.1.38) giving an organized scheme of procedures for preventing, limiting the effects of, and facilitating recovery from natural or man-made disasters; ISO 5127:2017(en), 3.11.3.30 Information and documentation — Foundation and vocabulary
- disaster recovery: the ability of the Information and Communications Technology elements of an organization to support its critical business functions to an acceptable level within a predetermined period following a disaster; ISO/IEC/IEEE 26511:2018(en), 3.1.11 Systems and software engineering — Requirements for managers of information for users of systems, software, and services
- man-made disaster: disastrous event caused directly and principally by one or more identifiable deliberate or negligent human actions; ISO/TR 19083-1:2016(en), 3.17

Intelligent transport systems — Emergency evacuation and disaster response and recovery — Part 1: Framework and concept of operation

- natural disaster: natural event such as a flood, earthquake, or hurricane that causes great damage or loss of life; ISO 37100:2016(en), 3.1.14 Sustainable cities and communities — Vocabulary

Interruption Terms and Definitions

The common usage dictionary definition from Webster's is provided as is the most directly applicable ISO definition:

- **Interruption** (Webster's Dictionary): "an act of breaking the uniformity or continuity of, or hindering by breaking in, of something or someone."
- **Interruption / interrupt** (ISO Definition): "suspension of a process, such as the execution of a computer program, caused by an event external to that process, and performed in such a way that the process can be resumed; Note 1 to entry: interrupt; interruption." (ISO/IEC 2382:2015(en), 2122873 Information technology — Vocabulary)

Key insight: This appears to be a type of disruption where an event occurs that can be quickly resolved.

Other definitions or applied terms that provide insight are:

- Interruption: a situation where the service (3.37) is not available; Note 1 to entry: Interruptions can be planned or unplanned; ISO/TS 24520:2017(en), 3.21 Service activities relating to drinking water supply systems and wastewater systems — Crisis management — Good practice for technical aspects
- Interruption: single temporary failure (3.3) or damage (3.2), or a single failure or damage that can be removed by a minor action by the operator; ISO 11994:1997(en), 3.4 Cranes — Availability — Vocabulary

Other Related Terms

Other definitions or applied terms that provide insight are:

First, the terms from TC 292 on Security and Resilience, are presented before a separate section from other TCs.

- Emergency: sudden, urgent, usually unexpected occurrence or event (3.1.96) requiring immediate action; Note 1 to entry: An emergency is usually a disruption (3.1.75) or condition that can often be anticipated or prepared for, but seldom exactly foreseen; ISO 22300:2021(en), 3.1.87
- recovery point objective/ RPO: point to which information (3.1.127) used by an activity (3.1.2) is restored to enable the activity to operate on resumption; Note 1 to entry: Can also be referred to as “maximum data loss”; ISO 22300:2021(en), 3.1.202
- recovery time objective/ RTO: period of time following an incident (3.1.122) within which a product and service (3.1.191) or an activity (3.1.2) is resumed, or resources (3.1.207) are recovered; Note 1 to entry: For products, services and activities, the RTO is less than the time it would take for the adverse impacts (3.1.118) that would arise as a result of not providing a product/service or performing an activity to become unacceptable; ISO 22300:2021(en), 3.1.203
- Recovery: restoration and improvement, where appropriate, of operations, facilities (3.1.104), livelihoods, or living conditions of affected organizations (3.1.165), including efforts to reduce risk (3.1.216) factors; ISO 22300:2021(en), 3.1.201
- Robustness: the ability of a system to resist virtual or physical, internal or external attacks (3.2.4); Note 1 to entry: Particularly, the ability to resist attempted imitation, copy, intrusion or bypassing; ISO 22300:2021(en), 3.1.233

The other terms are:

- Recovery: operational, transactional, and short-term activity to enhance preparedness following an emergency, disaster, or crisis; Note 1 to entry: Recovery is focused on communities, i.e. the people, places and processes, and is underpinned by power and partnerships; Note 2 to entry: Recovery should be informed by the business continuity processes and the strategic objectives of the organization for recovery following a crisis; ISO 22393:2023(en), 3.1 Security and resilience — Community resilience — Guidelines for planning recovery and renewal
- Reliability: <cybersecurity> property of consistent intended behaviour and results; [SOURCE:ISO/IEC 27000:2018, 3.55] Information security management
- Reliability: <system> ability of an item to perform as required, without failure, for a given time interval, under given conditions; Note 1 to entry: The time interval duration can be

expressed in units appropriate to the item concerned (e.g., calendar time, operating cycles, distance run, etc.) and the units should always be clearly stated; Note 2 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance; [SOURCE: IEC 60050-192:2015, 192-01-24, modified — The domain has been changed, the phrase "of an item" has been added at the beginning of the definition and Note 3 to entry has been removed.]

- Resilience: <governance> ability to anticipate and adapt to, resist, or quickly recover from a potentially disruptive event, whether natural or man-made; [SOURCE: ISO 15392:2019, 3.21, modified] Sustainability in buildings and civil engineering works — General principles
- Resilience: <system> capability (3.3.2) of a system (3.3.10) to maintain its functions and structure in the face of internal and external change and to degrade gracefully when this is necessary [SOURCE: ISO 15392:2019, 3.21, modified]
- Resilience: adaptive capacity of an organization in a complex and changing environment; Note 2 to entry: Resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event; Note 3 to entry: Resilience is the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when this is necessary; [SOURCE: ISO Guide 73:2009, 3.8.1.7] Risk management — Vocabulary
- Robustness: the ability of a structure (3.59) to withstand accidental and abnormal events without being damaged to an extent disproportionate to the cause [SOURCE: ISO 19900:2013, 3.42] ISO 19904-1:2019(en), 3.45 Petroleum and natural gas industries — Floating offshore structures
- Robustness: the ability of a system (3.3.10) to maintain its level of performance under a variety of circumstances; ISO/IEC TS 5723:2022(en), 3.2.16 Trustworthiness — Vocabulary
- Supply Chain Risk Management: The identification, assessment, prioritization, and mitigation of business, technical, and physical risks as they pertain to the manufacturing process including the use of third-party components and services in addition to the delivery of the product to the end user; ISO/IEC 20243-1:2023(en), 3.48 Information technology — Open Trusted Technology Provider TM Standard (O-TTPS) — Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products
- Supply Chain Security: The manufacturing and/or development process performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation. Extends the NIST definition [NIST SP 800-12]; ISO/IEC 20243-1:2023(en), 3.49 Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products

RESULTS and DISCUSSION (Part 2: Common Usage)

This research was conducted to consider the most appropriate term for the study of the underlying incidents or events that cause problems in supply chain management. This section was created to review the everyday use of the terms. In part, this section was created to review attributes or classifications of the supply chain problems.

This section does NOT consider the definitions of ISO or its general usage in supply chain management applications.

While all three terms involve interruptions, “disaster” denotes a severe, often catastrophic event; “disturbance” implies a minor interruption of disorder; and “disruption” refers to a break of interruption in normal processes, with severity depending on the context. The disasters are typically severe and often referred to as natural or man-made, such as earthquakes, floods, or industrial accidents. Attributes are severe and long-lasting impacts that require emergency response and long-term recovery strategies. The disturbances are generally less severe than disasters. They can pertain to minor interruptions or disorders, such as loud noises disrupting sleep or minor public commotions. Attributes are minor or short-term interruptions that are quickly identifiable with minimal loss of service. Finally, disasters can vary in severity and often refer to interruptions in systems or processes, such as service outages or schedule changes. Attributes are moderate in severity and may require process adjustments and new stakeholder relationships.

- Disaster:
  - A massive earthquake destroys a significant manufacturing hub, halting production and causing months-long delays.
  - A hurricane damages critical ports and warehouses, disrupting the flow of goods across continents.
- Disturbance:
  - A brief labor protest delays deliveries for a day but doesn’t cause lasting issues.
  - A software glitch causes a short-term delay in inventory management but is quickly fixed.
- Disruption:
  - A key supplier suddenly goes out of business, requiring the sourcing of alternate suppliers.

- A transportation strike causes prolonged delays, forcing companies to reroute shipments.

The terms were analyzed for their typical applications in supply chain contexts:

Table 1: Review of Characteristics of Disaster, Disruption, and Disturbance (Some Events could fall into several categories based on their intensity)

Aspect	Disaster	Disruption	Disturbance
Severity	High (catastrophic)	Moderate (medium	Low (minor)
Duration	Long-term impact	Medium-term impact	Short-term impact
Examples	Natural disasters, pandemics, wars, widespread counterfeit raw materials	Supplier bankruptcy, transportation strikes	Minor protests, brief tech issues, single counterfeit raw material shipment, and finished goods stolen in transit.
Response	Crisis management, recovery plans	Contingency plans, process adjustments	Quick fixes, adjusting activities

Key Insight: Applying the common usage of the terms, “supply chain disruptions” are typically moderate-severity events that interrupt operations but are manageable with contingency plans. "Disaster" describes catastrophic events, while "disturbance" indicates minor, often quickly resolved issues.

SIDEBAR: Industry Application

For context and to understand the real-world applications, it is helpful to review the industry literature. A key resource for the supply chain management leaders is reports by Gartner.

- **Supply chain disruption:** “refers to unexpected events that interrupt the normal flow of goods and materials within a supply chain. These disruptions can be caused by natural disasters, pandemics, political instability, economic upheaval, cyberattacks, or rapid changes in consumer demand. Such disruptions can lead to delays, increased costs, and inefficiencies, impacting businesses and consumers alike.” (REF Gartner)

CONCLUSION

ISO standards, particularly ISO 22300 and ISO 28000, provide critical definitions that help distinguish between "disruption," "disturbance," "disaster," and "interruption" in supply chain contexts. After reviewing ISO standards, industry literature, and common usage, the term "supply chain disruption" is the most accurate and applicable descriptor for events interrupting the flow of goods and services.

The International Standards Organization (ISO) plays a crucial role in providing standardized terminology for supply chain risk management. A general vocabulary standard such as ISO 22300:2021 offers definitions applicable across the entire ISO Technical Committee 292 on Security and Resilience. This committee focuses on enhancing organizational resilience against disruptions, including natural disasters, cyberattacks, and supply chain interruptions.

ISO standards are structured hierarchically. General standards like ISO 22300 establish foundational vocabulary, while more specialized standards, like ISO 28000, address specific applications such as supply chain security. The ISO 28000 series is essential for organizations seeking to secure their supply chains by identifying risks, implementing protective measures, and improving resilience.

The ISO 22300 series cover critical aspects of system management, including resilience and recovery. Within this context, key terms like disruption and supply chain disruption are defined with precision. According to ISO 22300, a disruption is an incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from expected operations. Disruptions can stem from various causes, ranging from routine issues to novel and unforeseen events.

Supply chain disruptions specifically refer to events that interrupt the normal flow of goods and materials. These interruptions can result from natural events, labor strikes, supplier failures, or cyberattacks. The impact of such disruptions varies in severity and duration, requiring distinct responses like contingency planning, process adjustments, or crisis management.

Upon a review of published ISO terms and definitions, as well as a review of the common usage and industry practices, the most appropriate term for issues that cause these problems is “Supply Chain Disruption.”

Appendix: ISO Use of Supply Chain Disaster Terms

This section was created as a process check to review what phrase was most used across all ISO standards as well as anywhere in the text, not just the "Terms & Definitions. For this section, the keywords and results are: Chain Disrup* (8), Supply Chain Distur* (0), Supply Chain Disaster* (0), and Supply Chain Interup* (0).

The following content is all direct quotes from ISO.

ISO/TS 22318:2021(en) Security and resilience — Business continuity management systems — Guidelines for supply chain continuity management

Introduction

Organizations rely on resources to be delivered on time and at an agreed quality and cost. These include, for example, materials, labor, information and data, workplace, facilities, associated utilities, equipment, consumables, information communication technology (ICT) systems, transportation, logistics, finance, and other services required to support the business activities of the organization. This is referred to as "upstream".

Organizations also rely on being able to deliver their products and services to their customers, whether they are the following link in the supply chain or the end customer. Product and service delivery (e.g., transportation, logistics, implementation services, machinery installation services) is performed by the organization or by a third party under the organization's responsibility. This is referred to as "downstream".

An organization needs to recognize the potential impact of not resuming activities within an acceptable time frame due to **supply chain disruption**. Failure by a supplier to deliver resources on time at an agreed quality and cost can trigger a business disruption. The organization needs to take into account and manage conflicting objectives, such as reducing supply chain costs by reducing cycle times or buffer stock and managing the supply chain continuity risk arising from a single source and just-in-time supply approaches. The organization needs to achieve an acceptable balance between risks and continuity measures.

Scope

1 Scope

This document gives guidance on methods for understanding and extending the principles of business continuity embodied in ISO 22301 and ISO 22313 to the management of supplier relationships. It enables an organization to develop and document the strategy to be better prepared to manage supply chain continuity.

This document is generic and applicable to all organizations. It is applicable to suppliers of products, services, and resources, both upstream and downstream.

Supply chain continuity management (SCCM) considers explicitly the issues faced by an organization that relies on the continuity of supply of resources as well as the ability to continue the delivery of its products and services. The objective of SCCM is to protect the organization's business activities from **supply chain disruption**.

ISO 28004-3:2014(en) Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)

3 Additional guidance

...risk is considered to be managed if the likelihood of a medium or high consequence **supply chain disruption** is limited to a low likelihood situation. Care should be taken in managing large...

ISO/TS 22331:2018(en) Security and resilience — Business continuity management systems — Guidelines for business continuity strategy

Business continuity strategy determination and selection outcomes include:

— measures to attempt to decrease the frequency of disruptive incidents and the impact associated with these disruptive incidents;
— identification of the financial resources needed to respond to a disruptive incident;
— effective internal and external communications capabilities;
— alternate workspace capabilities to address the loss or inaccessibility of premises;
— arrangements to address the unavailability of personnel;
— alternative methods of maintaining, fixing, and replacing resources for performing activities in the event of loss;
— capabilities to recover lost information and communications technology (ICT) assets, including data;
— alternate means to deliver products and services when faced with a **supply chain disruption**.

Appendix: ISO Standards with “Supply Chain” in the Title

In this research project, each was reviewed for any focus on disruptions. Note that TC 292 is Security and Resilience and was covered thoroughly in the ISO 22300 and ISO 28000 series.

- ISO 29404:2015 Ships and marine technology — Offshore wind energy — Supply chain information flow
  - TC: ISO/TC 8
- ISO 28004-2:2014 Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations
  - TC: ISO/TC 8
- ISO 28004-3:2014 Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)
  - TC: ISO/TC 292
- ISO 19443:2018 Quality management systems — Specific requirements for the application of ISO 9001:2015 by organizations in the supply chain of the nuclear energy sector supplying products and services important to nuclear safety (ITNS)
  - TC: ISO/TC 85
- ISO 19443:2018/Amd 1:2024 Quality management systems — Specific requirements for the application of ISO 9001:2015 by organizations in the supply chain of the nuclear energy sector supplying products and services important to nuclear safety (ITNS) — Amendment 1: Climate action changes
  - TC: ISO/TC 85
- ISO 20333:2017 Traditional Chinese medicine — Coding rules for Chinese medicines in supply chain management
  - TC: ISO/TC 249
- ISO 18495-1:2016 Intelligent transport systems — Commercial freight — Automotive visibility in the distribution supply chain — Part 1: Architecture and data definitions
  - TC: ISO/TC 204
- ISO 28004-4:2014 Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective
  - TC: ISO/TC 292
- ISO 17363:2013 Supply chain applications of RFID — Freight containers
  - TC: ISO/TC 104/SC 4
- ISO/IEC 27036-3:2023 Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security
  - TC: ISO/IEC JTC 1/SC 27
- ISO 28001:2007 Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance
  - TC: ISO/TC 292

- ISO 28004-1:2007/Cor 1:2012 Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles — Technical Corrigendum 1
    - TC: ISO/TC 292
- ISO 28003:2007 Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems
    - TC: ISO/TC 292
- ISO 14052:2017 Environmental management — Material flow cost accounting — Guidance for practical implementation in a supply chain
    - TC: ISO/TC 207/SC 1
- ISO 32120:2024 Transaction assurance in E-commerce — Guidelines on sharing goods quality assurance traceability information in E-commerce supply chains
    - TC: ISO/TC 321
- ISO 23664:2021 Traceability of rare earths in the supply chain from mine to separated products
    - TC: ISO/TC 298

/END/