INTERNATIONAL STANDARD

ISO 22380

First edition
2018-08

Security and resilience — Authenticity, integrity and trust for products and documents — General principles for product fraud risk and countermeasures

Reference number
ISO 22380:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

There is evidence that virtually every type of product fraud has been committed, including counterfeiting of infant formula, prescription drugs, consumer goods and after-market parts for automobiles, aircraft and nuclear power plants. A large number of individuals or organized criminal groups are committing product fraud, with various motivations, such as financial gain, which is threatening global public health and safety. The public health and safety risks associated with product fraud are diverse and significant when the products are distributed through legitimate global supply chains. Examples include lethal amounts of melamine in infant formula, medicines with little or no active ingredients, aircraft replacement parts that fail and substandard electrical cords that catch fire.

Classical crime prevention strategies begin with an analysis of the situational contexts of a criminal offence in order to find the structural opportunity of a particular crime. Next, specific types of crime are classified according to modus operandi (MO) together with types of criminal intention and motive. Then, the types of criminal offenders and their behaviours are examined to determine how to prevent or deter the crime.

This document starts with understanding the external and internal situational context of product fraud. It considers causes of the fraud, such as product marketplaces and product fraud-related opportunities. It then examines the intentions and motives for product fraud, the types of product fraud, the types of product fraudsters and strategic countermeasures that can be taken against product fraud.

A better understanding and classification of intentions and motives, product fraud activities and fraudsters leads to a better selection of countermeasures. Product fraud countermeasures include profiling product fraud, risk assessment and the selection/implementation of bespoke countermeasures.

Figure 1 illustrates how a strategy for product fraud countermeasures and control as a continual process starts from an analysis of the situational context of product fraud, moves through several classifications of product fraud and fraudsters, and results in the selection/implementation of bespoke countermeasures and their effective assessment.

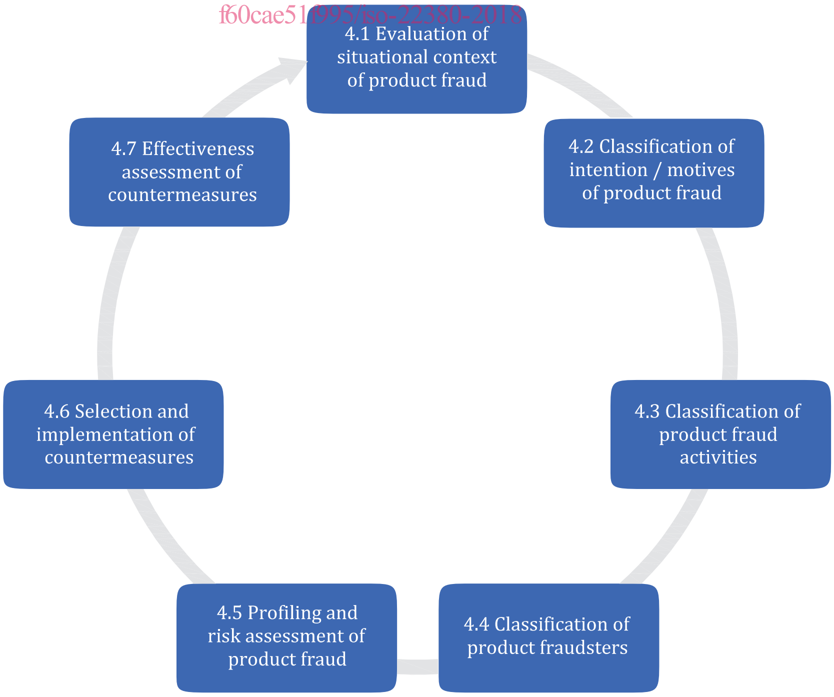
4.1 Evaluation of situational context of product fraud
4.2 Classification of intention / motives of product fraud
4.3 Classification of product fraud activities
4.4 Classification of product fraudsters
4.5 Profiling and risk assessment of product fraud
4.6 Selection and implementation of countermeasures
4.7 Effectiveness assessment of countermeasures

Figure 1 — The continual process for a product fraud countermeasures and control strategy

Security and resilience — Authenticity, integrity and trust for products and documents — General principles for product fraud risk and countermeasures

1 Scope

This document establishes general principles for an organization to identify the risks related to various types of product fraud and product fraudsters. It provides guidance on how organizations can establish strategic, business countermeasures to prevent or reduce any harm, tangible or intangible loss and cost from such fraudulent attacks in a cost-effective manner.

This document is applicable to all organizations regardless of type, size or nature, whether private or public sector. The guidance can be adapted to the needs, objectives, resources and constraints of the organization.

This document is intended to promote common understanding in the field of product-related fraud risk and its countermeasures.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Security and resilience — Vocabulary*

ISO 31000:2018, *Risk management — Guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
product fraud
wrongful or criminal deception that utilizes material goods for financial or personal gain

Note 1 to entry: Fraud means wrongful or criminal deception intended to result in financial or personal gain that creates social or economic harm.

Note 2 to entry: Products include electronic media carried on material goods.

Note 3 to entry: Fraud related to digitally transmitted electronic media shall be considered separately.

4 General principles for product fraud risk and countermeasures

4.1 Evaluation of situational context of product fraud

4.1.1 Considering the product fraud opportunities

The organization should base its fraud control strategies on a proper understanding of the intentions, motives, nature and types of the fraud and the fraudster.

The organization should consider all of the three elements (fraudster, victim/target and poor guardianship) essential in crime occurrence for its basis of applied crime prevention.

Crime occurs when a motivated fraudster and suitable target come together in a time and a place, without a capable guardian present.

Product fraudsters commit fraud crime when they perceive that a specific fraud target is vulnerable, there are sufficient rewards from fraud attacks, and there is no or weak guardianship and countermeasures for deterring, delaying, hindering or stopping their attacks. The vulnerability is referred to as "fraud opportunity". This is based on the "rational choice" theory in criminology, which states that people commit crime when they perceive the risk of offending to be low and the rewards to be high, as illustrated in Figure 2.

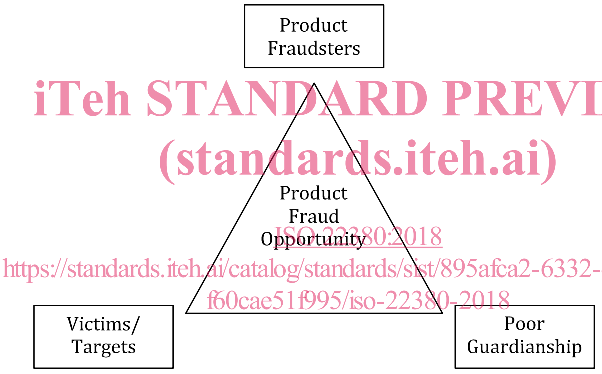

Figure 2 — The crime triangle for product fraud opportunity

The organization should distinguish between product fraud and financial fraud insofar that product fraud is always related to products whereas financial fraud is broader and is not necessarily related to products.

The main elements of financial fraud are pressure, opportunity and rationalization. The fraudsters in financial fraud are usually employees, whereas the fraudsters in product fraud are varied, as suggested in Table 4.

4.1.2 Evaluating the product fraud risk

The organization should evaluate the situational context of product fraud. It should understand the factors that significantly influence the product fraud risk and the effectiveness of countermeasures.

Evaluating the external situational context of product fraud risk includes the following:

- the social and cultural, political, legal, regulatory, financial, technological and economic context;
- the natural and competitive environment, whether international, national, regional or local marketplaces and the supply chain;
- key drivers and trends that have an impact on the particular products and brand-owners;
- relationships with, and perceptions and values of, external stakeholders.

Evaluating the internal situational context of product fraud risk includes the following:

— governance, organizational structure, roles and accountabilities;

— policies, objectives and the strategies that are in place to achieve them;

— capabilities, which are understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

— information systems, information flows and decision-making processes (both formal and informal);

— relationships with, and perceptions and values of, internal stakeholders;

— the organization's culture;

— standards, guidelines and models adopted by the stakeholders.

4.2 Classification of intention and motive of product fraud

The organization should classify the intentions for product fraud, see Table 1:

— deceptive products are products that are placed into supply chains with the intent to deceive the consumer into believing that the product is genuine in every way;

— non-deceptive products are products that do not try to deceive the consumer into believing the products are genuine by their positioning in the market, whether through the type of retail outlet in which they are sold (flea markets, etc.), their price (exponentially low) or quality (poor).

Even if the distributors and sellers of non-deceptive products do not try to deceive the consumer into believing the products are genuine, they are still product fraudsters because they have deceived intellectual property rights (IPR) holders.

Table 1 — Taxonomy of product by intention

Intention of deception	Description
Deceptive product	Products that are placed into supply chains with the intent to deceive the consumer into believing that the product is genuine.
Non-deceptive product	Products that do not try to deceive the consumer into believing the products are genuine.

The organization should also classify the motives for product fraud, see Table 2:

— recreational product fraud means fraudulent acts committed for entertainment, amusement, fun or just thrill;

— occasional product fraud means rather passive fraudulent acts that occur infrequently or opportunistically;

— occupational product fraud means insiders' fraudulent acts at their place of employment, either as an individual or with the organization's knowledge;

— professional product fraud means fraudulent acts that fully finance the fraudster's lifestyle as their full-time, or almost full-time, job;

— activism product fraud means fraudulent acts committed by domestic or international terrorists who are making an ideological or political statement or intend to economically harm an entity.

Table 2 — Types of motives for product fraud[13]

Motives	Description
Recreational product fraud	Fraudulent acts for entertainment or amusement.
Occasional product fraud	Fraudulent acts committed infrequently or opportunistically.
Occupational product fraud	Fraudulent acts at a place of employment, either by an individual or with the organization’s knowledge.
Professional product fraud	Fraudulent acts that fully finance a fraudster’s lifestyle as their job.
Activism product fraud	Individuals or groups who commit fraudulent acts to make an ideological or political statement or to harm an entity.

4.3 Classification of product fraud activities

The organization should classify the types of product fraud and their potential consequences, see Table 3.

The types of product fraud listed in Table 3 stretch the traditional definitions of IPR violations or even of property theft.

In each case, some component or statement is fraudulent. For example, a stolen product is fraudulent when re-introduced into the supply chain unless the seller admits it is stolen; if they admit it is stolen, it is still a crime.

Each case represents a public health and safety risk for the consumer and a benefit for the fraudster. For example, stolen goods that generate revenue for the fraudster may have spoiled due to mishandling, which is a health hazard for the consumer.

Counterfeiters also use stolen goods to fool suspicious customers by first providing them with a genuine, but stolen, product before then replenishing orders with fraudulent products.

Table 3 — Types of product fraud[14]

Type	Description	Examples	Potential consequences
Counterfeiting	To simulate, reproduce or modify a product or its packaging without authorization (see ISO 12931).	Counterfeit pressure gauge case in Germany[4]. UK insurer links rising electrical fault fires to counterfeits[5].	Human or environmental harm (safety risks).
IPR infringement	Application and implementation of technical capabilities covered by intellectual property rights.	Workmate™ cases of unauthorized use of patent.	Economic harm to IPR holders.
Adulterant-substance	A component of the finished product is fraudulent.	Adulteration of infant formula by melamine in China. Estimated 300,000 victims including the death of 6 infants[6].	Low quality or unsafe products leading to human or environmental harm.
Tampering	A legitimate product but packaging or security elements are altered.	Acetaminophen re-marking old chips as new chips[7].	Dangerous, misleading consumer information leading to human or environmental harm.
Substitution	Complete or partial undeclared replacement of authentic components or ingredients with a substitute.	Substitution of horsemeat for beef in the UK[8].	Misleading consumers and regulators with possibly unsafe components or ingredients leading to human or environmental harm.

Table 3 *(continued)*

Type	Description	Examples	Potential consequences
Simulation	Illegitimate product designed to look like but not exactly copy the legitimate product.	"Knock-offs" of popular products not produced with the same product safety assurances[9].	Inferior quality leading to human or environmental harm.
Diversion	Sale or distribution of products outside of intended markets.	Shipment of discounted retroviral medicines to central African countries re-sold to northern European countries at normal prices. Relief product redirected to markets where aid is not required[10].	Shortages or delays of relief product to needy populations. Difficulties in recall of products leading to human or environmental harm.
Distribution of stolen goods	A legitimate product stolen and passed off as legitimately procured.	Stolen products[11] mixed with legitimate products in an online shopping cart.	Economic loss; loss of control in distribution channel; tax evasion.
Over-run	A legitimate product made in excess of contractual or regulatory agreements. False reporting of production. Undeclared production shift.	Contracted textile/garment companies producing more than the contracted amount of product and selling the over-production to counterfeiters[12].	Economic loss and inability of recall leading to human or environmental harm.

4.4 Classification of product fraudsters

The organization should classify product fraudsters by geographic scale and the extent of their organizational system.

Geographical scale separates product fraudsters into three groups:

- local fraudsters who commit product fraud mainly within one local area in a country;
- national fraudsters who manufacture, package and lease fraudulent products and then store, exhibit, distribute and sell them through supply chains across a country;
- international fraudsters who act at a transnational level.

Table 4 describes various types of product fraudsters by the extent of their organizational system.

Table 4 — Types of product fraudsters[15]

Type	Description	Characteristics
Individuals	One fraudster	Usually has recreational motives.
Small groups	A group of 2 to 3 fraudsters	Usually recreational. Not very systematic.
Commercial enterprise	An organization making or distributing products that infringe IP	Business driven.
Criminal enterprise	A group of more than 3 fraudsters and organized/operated in a systematic way like a commercial enterprise	Not involved in threats, violence, bribery or blackmailing.