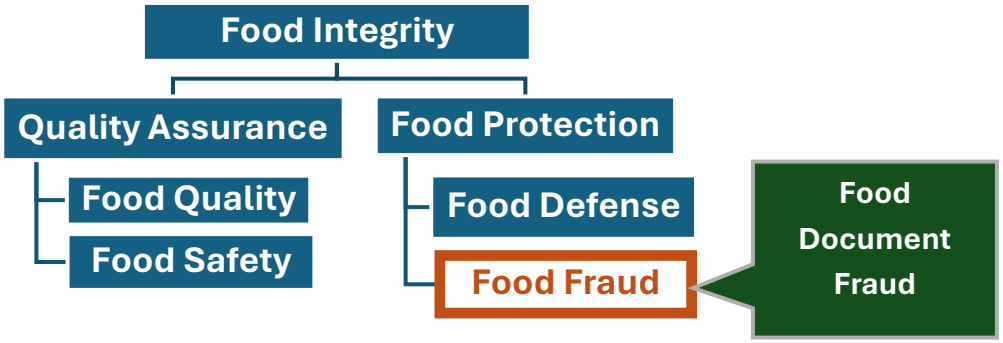
Primer on Food Document Fraud **December 2025**



Food Fraud Prevention –

Defining Food Document Fraud: Data, Information, Form, Format, Medium, Format, Type, and Record, plus Authentication, Traceability, and Certification

This primer presents an overview of comprehensive research projects that systematically define documents, records, and their corresponding components within food supply chain contexts. This review establishes a hierarchical framework clarifying relationships between key terms, including **data**, **information**, **format**, **medium**, **form**, and **authentication**. The findings are based on International Standards Organization (ISO) published standards, utilizing formal terms and definitions to ensure consistency and authoritative rigor across diverse industry applications.

The *research objective* was to support Food Fraud Prevention initiatives by creating standardized definitions that enable stakeholders to understand document-related vulnerabilities in food systems. The research concludes with a comprehensive definition of food document fraud based on document format type, emphasizing how each of five distinct types—**physical**, **digital**, **hybrid**, **multi-factor**, and **phantom**—can be exploited or protected against in food industry contexts. A phantom document represents information mentioned or alluded to that does not actually exist. This framework supports enhanced authentication, certification, and traceability systems essential for protecting food integrity.

This primer provides standardized terminology for food fraud vulnerability assessments, incident investigations, and training program development. Use these ISO-based definitions when documenting fraud risks, designing authentication systems, or communicating with supply chain partners about document security requirements.

www.FoodFraudPrevention.com

Introducing Food Document Fraud

Several ISO standards include procedures and definitions that directly relate to specific food document fraud scenarios, such as counterfeit labels or forged certificates, helping professionals understand practical applications of these standards.[1] Within ISO Technical Committee 292 on "Security and Resilience," Working Group 4 is on "Authenticity, integrity and trust for products and documents.[2]" Key applicable definitions included "product fraud" and "document fraud."

- **Product fraud (ISO 22380: Reconfirmed in 2024 January):** 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.
- **Document fraud (ISO 22388:2023 November):** wrongful or criminal deception that utilizes security documents 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: Fraud includes false use that does not necessarily involve the recreation of documents (e.g., an impostor, using someone else's ID for impersonation).

For efficiency, the ISO definitions have been merged into a summary definition. [3]

- ***Document Fraud (Summary definition): intentional deception for economic gain by misrepresenting information in a document or of the document itself (and in the format of physical, digital, hybrid, or phantom).***

The range of ISO definitions of food, document, and document fraud – considering industry standards – serves as a foundation for integrating these concepts into existing food safety and regulatory frameworks, facilitating practical implementation.[3]

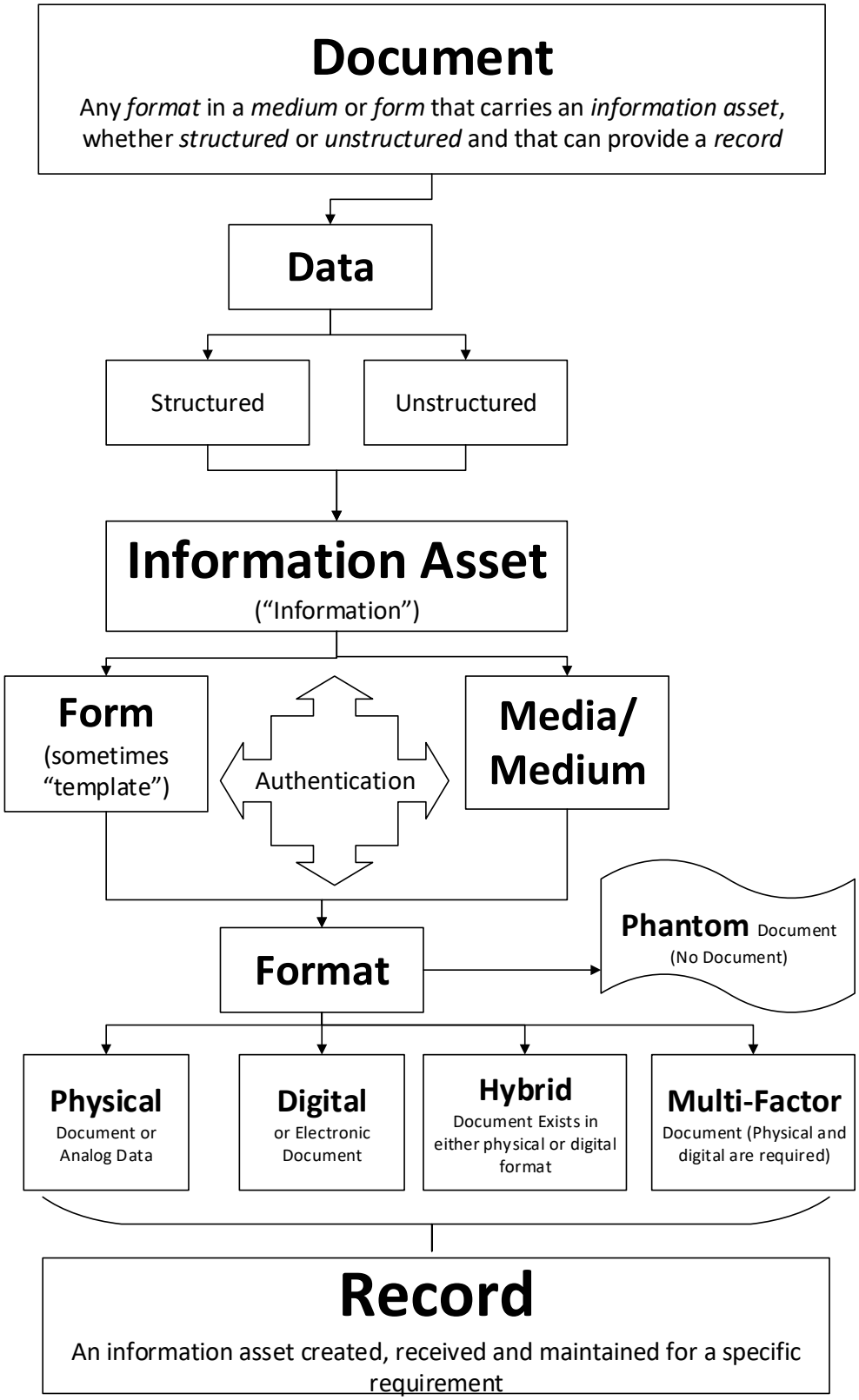
- ***Food document fraud (ISO-Based Summary definition) is crucial to understand, as it helps industry stakeholders recognize and prevent deceptive practices, fostering trust and clarity in food transactions.***

The Relationship of Documents, Records, Data, and Related Terms

During the research to develop a definition of "food document fraud," there was a need to build upon an official resource. It was determined that the International Standards Organization (ISO) formal "Terms & Definitions" was the most formal and comprehensive. These terms & definitions were thoroughly and rigorously developed and edited, including comparison to the use in application and other standards.

The relationship of the terms is present in a hierarchy (Figure):

Figure 1 Relationship Hierarchy for Document, Record, Data, and Related Terms



Definitions

All the definitions quoted have an ISO reference, which should reassure the audience of the standards' credibility and the thoroughness of the research behind these classifications. [3][4].

The hierarchy begins with a “document.”

- **Document** (Summary Definition): An **information asset** in any **format** and the **medium** on which it is contained, whether structured or unstructured, that is often created to provide a **record** of an activity.

Next is the “data” and “information.”

- **Data** (Summary Definition): a fact or measurement of an object that has not yet undergone processing into meaningful **information**.
    - **Unstructured Data** (ISO 20546 and ISO 17251): data that are characterized by not having any structure apart from that of the record or file level; information assembled from narrative words and word fragments, following either casual conventions or language-specific grammatical rules.
    - **Semi-Structured Data** (ISO 20944): aggregate datatype whose components' datatypes and their labels are not predetermined
    - **Structured Data** (ISO 20546 and ISO 22957): data that is organized based on a pre-defined set of rules; a document that follows a strict structure or format
- **Information Asset** (Summary Definition): information that can be shared.
- **Information** (Summary Definition): data that has undergone processing, filtering, and organization to explain a concept or idea.

The document carries data and information presented in a “from,” “medium,” and “format,” which enables a clear understanding of a comprehensive grasp of how information is structured and communicated.

- **Format** (Summary Definition): The arrangement of the information on a medium that allows it to be communicated or used.
- **Medium/ Media** (Summary Definition): a digital or physical material good, film, magnetic tape, optical or computer storage disk that records and can communicate information.
    - The complete lists of media or formats covered in ISO 4669-1 include: paper-based information, electronic documents and digital files, film and tape, voice, images, mobile working, assistive technology, collaborative platforms, database tools, websites, social media, internet or world-wide web, and intranets.
- **Form** or **Template** (Summary Definition): a document with pre-designed locations and structural rules to later enter information.
- **Document Format Type**: the structure of information and the medium on which it is contained that can be used for reference or analysis.

For efficiency, the ISO definitions are integrated into ISO-based summary definitions. [3]

1. **Physical Document** or **Analog document** (Summary definition): a material document, such as in a paper medium. For example, a receipt of sale or a driver's license.

2. **Digital Document** or **Electronic Document** (Summary definition): a document that exists on a device or in a computer file. Note: "Digital document" is the preferred term since a "physical document" can also be in electronic format. ISO has a reference to "born digital," meaning that the original document never existed in a physical or material format. For example, a travel authorization format was created on a computer, and the approvals were routed and completed with a "digital signature."

3. **Hybrid Document** (Summary definition): A document where the official and complete information exists in both physical and digital formats. Either document is considered the original or official record. For example, a physical and digital receipt for purchase could be used to authorize a product return.

4. **Multi-Factor Document** (Summary definition): A document where part of the information is carried in the physical medium, and part of the information is in a digital medium. Both sets of documented information are required to complete the transaction. For example, the physical factor may be biometrics such as a fingerprint or iris scan, and the digital format may receive an authentication code.

5. **Phantom Document or No Document** (Summary Definition): A mention or allusion to a document that actually does not exist. For example, during a discussion or in a communique, a document might be referred to but not explicitly presented, and the document may not actually exist.

Finally, everything comes together in a record.

- **Record** (Summary Definition): An information asset created and maintained as evidence and as a separate asset to confirm an obligation or requirement.

Document Purpose: Security, Authentication, Certification, and Traceability

Documents serve multiple security functions including to support authentication, certification, and traceability.

- **Document security** (Summary definition): is a collection of procedures, guidelines, coordinated activities, and security features that protect physical and digital documents from unauthorized access, use, dissemination, and alteration that can cause damage or harm [**adapted from ISO 22376 definition of document, ISO 28001 definition of security, and ISO 22340 definition of protective]**.

More specific purposes include:

- ***Authentication*** (Summary definition): is the act of verifying that the product, user, or document is "what it says it is." For example, a product sample can be tested against a reference sample to confirm the source. Also, a document feature, such as a confirmation number, can be confirmed with the issuing entity.
- ***Certification*** (Summary definition): is the confirmation that a product, user, or document meets prescribed requirements. For example, it is a statement that this product meets food safety management system standards or organic processing requirements.
- ***Traceability*** (Summary definition): is the ability to follow or identify a product or document's history, movement, or location through a process. This includes the aspect of ***tracking,*** monitoring a product as it moves through a process, and ***tracing*** to confirm where a product has been. As a rule, documents should be recorded and stored, including the notice of updates or changes to the details of the agreement.

Statement About Limitations

While ISO standards provide authoritative foundations, some food-specific applications may require additional contextual interpretation. This framework focuses on document format types rather than detection methodologies. Future research should address implementation protocols and integration with existing food safety management systems.

Conclusion

This primer establishes a common terminology framework for food document fraud, providing clear definitions grounded in ISO standards—an authoritative, industry-neutral foundation. By systematically defining document format types (physical, digital, hybrid, multi-factor, and phantom) and their hierarchical relationships, this framework supports critical research on incident investigation and vulnerability assessment across food supply chains. The ISO-based approach ensures universal applicability while maintaining the scientific rigor necessary for both academic research and practical industry implementation. As a living document, this framework will continue evolving to address emerging threats, including AI-enabled fraud, advanced digital printing, and novel electronic document manipulation. These standardized definitions enable food industry stakeholders to develop more effective prevention strategies, conduct meaningful vulnerability assessments, and build resilient authentication and traceability systems essential for protecting food integrity.

Food industry stakeholders should immediately assess document vulnerabilities across their supply chains using this five-format framework, integrate these definitions into supplier audit protocols and training programs, and contribute feedback to support ongoing refinement of this living framework.

References

1. ISO, International Organization for Standardization. *ISO Homepage*. 2008; Available from: http://www.iso.org/iso/home.htm.
2. ISO, International Organization for Standardization, *Technical Committee 292 Security Management and Resilience, Work Group 04 Product Fraud Countermeasures and Controls, Home Page, URL: https://www.iso.org/committee/5259148.html.* 2017.
3. Food Fraud Prevention Academy, FFPA, *Preliminary Literature Review of Document, Fraud Related terms including Types, Formats, Functions, and Information, Food Fraud Insight Report (FFIR), Food Fraud Prevention Academy, Editor: John W Spink, URL: https://foodfraudpreventionthinktank.com/food-fraud-insight-reports/ Accessed: January 11, 2025.* 2024.
4. Roy Fenoff, John W Spink, Byung Lee, *Food Document Fraud: A preliminary survey of the Food Industry Perception and Awareness including Unmet Training Needs, found at www.FoodFraudPrevention.com*. Working Paper, 2025.

/END/