Food Fraud Prevention THINK TANK

Glossary of Food Fraud-Related Terms

Version: May 17, 2020 -- By John Spink, PhD

This Food Fraud Prevention Think Tank Report is a Glossary of Food Fraud-Related Terms. The version is identified by the update date. Anyone has the opportunity to comment or recommend edits by accessing the link to the "Google Document" listed below. A few key terms are presented here (full citations in the attachment):

Food Fraud (Summary): intentional deception for economic gain using food including ingredients through finished goods.	**Food Authenticity (Elliott Review):** "is about ensuring that food offered for sale or sold is of the nature, substance and quality expected by the purchaser."	**Food Crime (General)** of (1) incidents involving food that is a violation of a criminal statute or (2) Food Fraud incidents that are conducted on a larger scale."
Food Fraud (GFSI): "A collective term encompassing the deliberate and intentional substitution, addition, tampering or misrepresentation of food, food ingredients or food packaging, labeling, product information or false or misleading statements made about a product for economic gain that could impact consumer health."	**Economically Motivated Adulteration –EMA (US FDA):** "Fraudulent, intentional substitution or addition of a substance in a product for the purpose of increasing the apparent value of the product or reducing the cost of its production, i.e., for economic gain."	**Food Integrity (Elliott Review):** "can be seen as ensuring that food which is offered for sale or sold is not only safe and of the nature, substance and quality expected by the purchaser but also captures other aspects of food production, such as the way it has been sourced, procured and distributed and being honest about those elements to consumers."
Vulnerability: "a weakness or flaw that creates opportunities for undesirable events related to the system ("system design")."	**Prevention:** "intended to reduce or eliminate the likelihood of the event occurring."	**Hazard:** "is an event that has not occurred and could cause harm if not addressed"
Risk: "is an uncertainty of an outcome that is assessed in terms of likelihood and consequence"	**Mitigation:** "intended to reduce the consequence of the event"	**Threat:** "the cause of an unwanted event that includes generally known variables or attributes of the source of the negative consequence"

The glossary expanded from 300 terms to now over 850 and from 20 pages to over 70. This is an active process and everyone is invited to provide comments, edits, or recommendations by accessing the "Google Document." The glossary version is identified by the date. Thank you for participating in the process of clarifying the foundation of food fraud prevention. JWS

Add your comments to the working document here in this shared drive document:
https://drive.google.com/open?id=1zL1RuuqAWBq5Kzu4ujW_Ykd9qdLO0O6v

Appendix: Glossary of Food Fraud Related Terms

(Version: May 2020)

These are direct quotes unless clearly noted by "Comment."

Key food fraud terms are in yellow highlight and new additions are noted in red font.

---

1. **Acceptable level** (ISO 22000): level of a **food safety hazard** (3.22) not to be exceeded in the **end product** (3.15) provided by the **organization** (3.31)
2. **Accreditation (GFSI):** A process by which the authoritative body gives formal recognition of the competence of a certification body to provide certification services against an international standard.
3. **Accreditation Body (FDA, FSMA, US CODE):** The term 'accreditation body' means an authority that performs accreditation of third-party auditors.
4. **Accreditation Body (GFSI):** An agency having jurisdiction to formally recognise the competence of a certification body to provide certification services.
5. **Accuracy (Capra): "**how close the measured result is to the actual result" (ref Capra). In addition: "The accuracy of an analytical procedure expresses the closeness of agreement between the value which, is accepted either as a conventional true value or an accepted reference value and the value found. This is sometimes termed trueness." (REF)
6. **Action criterion** (ISO 22000): **-** measurable or observable specification for the **monitoring** (3.27) of an **OPRP** (3.30); Note 1 to entry: An action criterion is established to determine whether an OPRP remains in control, and distinguishes between what is acceptable (criterion met or achieved means the OPRP is operating as intended) and unacceptable (criterion not met nor achieved means the OPRP is not operating as intended).
7. **Activity** (ISO 22380): **process** (3.180) or set of processes undertaken by an **organization** (3.158) (or on its behalf) that produces or supports one or more **products or services** (3.181) **affected area**(ISO 22380): location that has been impacted by a **disaster** (3.69); Note 1 to entry: The term is more relevant to immediate **evacuations** (3.80).
8. **Adequate (FSMA-PC Guide):** That which is needed to accomplish the intended purpose in keeping with good public health practice.
9. **Adequate Security (DNI):** Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, acquisition, development, installation, operational, and technical controls.
10. **Adulterant (ISO TC292):** Summary: materials or substances intentionally added to the product for economic gain (or avoiding loss) or for intentional harm; "materials added to improve the low quality of the product or to mask its defects." (ISO 2451:2017, ISO 7540:2006)
11. **Adulterant (Keyword search, US CODE):** Lethal adulterant.-The offense involved the importation, manufacture, or distribution of a controlled substance (as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802)), mixed with a potentially lethal adulterant, and the defendant was aware of the presence of the adulterant. (18 USC 3592). (Comment- a keyword search of the US

Code was conducted to identify US government definitions of the term "adulterant." One definition was found and the term "adulterant" was used twice in that definition of "lethal adulterant.")

12. **Adulterant (Summary):** intentional act where a substance is added to a food
13. **Adulterant (USP):** Any undeclared biological or chemical agent, foreign matter, or other substance in food that may (though not necessarily) compromise food safety or suitability.
14. **Adulterant (Webster's):** An adulterating substance or agent. (See "adulterate")
15. **Adulterate (Black's law):** To debase or make impure by adding a foreign or inferior substance.
16. **Adulterate (-ion, -ed) (ISO TC292):** Summary: based on the word "adulterant," "adulterated" is the past tense and "adulteration" is the action of including an adulterant – this is in conflict with the FDA Food Drug & Cosmetics Act definition of "Adulterated Foods" that does not require a adulterant.; "Adulterated soluble coffee: products prepared by the co-extraction or the separate extraction of roasted coffee beans and of raw or roasted materials other than coffee beans, where the product is sold as pure soluble coffee and the addition of the non-coffee bean material is not declared on the label," "alteration of the composition of a lot (3.18) of cocoa by any means whatsoever" (ISO 24114:2011)
17. **Adulterate (Webster's):** "to corrupt, debase, or make impure by addition of a foreign or inferior substance or element, to prepare for sale by replacing more valuable with less valuable or inert ingredients."
18. **Adulterated Foods - re., aspects with no health hazard (FD&C Act, quotes) –** "(a) (4) if it has been prepared, packed, or held under insanitary conditions whereby it may have become contaminated with filth, or whereby it may have been rendered injurious to health;" and "(h) Reoffer of food previously denied admission: If it is an article of food imported or offered for import into the United States and the article of food has previously been refused admission."
19. **Adulterated Foods (FD&C Act, GMP, Interstate Commerce):** "Thus, instead of having to prove that the food is adulterated, insanitary conditions are considered sufficient to show that the food might have become adulterated. " Further: "Two sections of the FDCA are directly related to conditions in a facility where food has been manufactured. Section 402 (a)(3) specifies that food has been manufactured under such conditions that it is unfit for consumption. and Section 402 (a)(4) considers that food may be adulterated if it is prepared, packed, or held under insanitary conditions whereby it may have become contaminated with filth or rendered injurious to health. …These provisions are unlike other parts of Section 402, in that they relate to the conditions of a facility where food is produced or stored. Thus, instead of having to prove that the food is adulterated, insanitary conditions are considered sufficient to show that the food might have become adulterated."
20. **Adulterated Foods (FD&C Act, Ostroff Summary, 2017):** "If it bears or contains any poisonous or deleterious substance which may render it injurious to health.", "if any valuable constituent has been in whole or in part omitted or abstracted therefrom; or if any substances has been substituted wholly or in part…; or if damage or inferiority has been concealed… or if any substance has been added thereto or mixed or packed therewith, so as to increase its bulk or weight, or reduce its quality or strength, or make it appear better or of greater value than it is."
21. **Adulterated, Foods (FDA):** Comment- a violation of the Food, Drug & Cosmetics Act section on "Adulterated Foods"
22. **Adulteration (ASTA1):** "Adulteration is the deliberate and intentional inclusion in spices of substances whose presence is not legally declared, is not permitted or is present in a form which might mislead or confuse the consumer, leading to an imitated food and/or a product of reduced value, as well as the deliberate and intentional removal of any valuable constituent from a spice or herb."

23. **Adulteration (Black's law):** The act of corrupting or debasing. The term is generally applied to the act of mixing up with food or drink intended to be sold other matters of an inferior quality, and usually of a more or less deleterious quality.
24. **Adulteration (in the context of food fraud) (CEN):** A type of food fraud which includes the intentional addition of a foreign or inferior substance or element; especially to prepare for sale by replacing more valuable with less valuable or inert ingredients; Note 1 to entry: Economic gain is the most common reason for adulteration, and this practice is referred to as Economically Motivated Adulteration (EMA) of food products
25. **Adulteration (Webster's):** "-tion" is "the action of" or "the result of" adulterate (see "adulterate")
26. **Adulterator (Black's law):** A forger; a counterfeiter, counterfeiters of money; (Comment- there is sometimes translation or language confusion with the term "Adulterer" which is "One who corrupts; one who seduces another man's wife.")
27. **Adversary (DNI):** Any individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities, detrimental to critical assets.
28. **After-action report, AAR** (ISO 22380): **document** (3.71) which records, describes and analyses the **exercise** (3.83), drawing on debriefs and reports from **observers** (3.154), and derives lessons from it; Note 1 to entry: The after-action report documents the results from the after-action **review** (3.197).; Note 2 to entry: An after-action report is also called a final exercise report.
29. **Agent (Black's law):** "something that produces an effect <an intervening agent>"; (Comment- the term "agent" is used in FSMA referring to the source of a "hazard that requires a preventive control.")
30. **Agent (FSMA):** not defined but used in relation to a "physical agent" not a person such as a "broker agent", for example from the Preventive Controls for Human Foods Qualified Individual training (PCHF-QI) from Header: Economically Motivated Hazards, Content: "Include only those agents that can cause illness or injury."
31. **Agent (US CODE):** The term "agent" means a nuclear, biological, chemical, or radiological substance that causes agricultural disease or the adulteration of products regulated by the Secretary of Agriculture under any provision of law. (7 USC 8901)
32. **Agents (ASTA1):** "Businesses that provide similar services as Brokers, typically through an exclusivity agreement representing a foreign seller."
33. **Agroterrorism (Davidson):** Deliberate act which intends to introduce an animal or plant disease, with the purpose to cause fear, economic losses or social disturbance like the infection of animals/plant crops with pathogenic microorganisms or contamination of animal feed/plant fertilisers with chemical, biological or radiological hazards (Gyles, 2010; Monke, 2004)
34. **Alert** (ISO 22380): part of **public warning** (3.183) that captures attention of first responders and **people at risk** (3.166) in a developing **emergency** (3.77) situation
35. **All-hazards** (ISO 22380): naturally occurring **event** (3.82), human induced event (both intentional and unintentional) and technology caused event with potential **impact** (3.107) on an **organization** (3.158), **community** (3.42) or society and the environment on which it depends
36. **Analytical methods for authentication, food product (CEN):** Methods and instruments for determining a range of biochemical food product characteristics; Note 1 to entry: Examples of analytical methods include: DNA based analyses, Stable isotope and trace element analyses, Analysis of lipid profiles, High performance liquid chromatography (HPLC), Gas chromatography–mass spectrometry (GCMS), Nuclear magnetic resonance (NMR) spectroscopy, Near infrared (NIR) spectroscopy, Metabolite profiling, Chemical profiling, Proteomics.
37. **Asset** (ISO 22380): anything that has value to an **organization** (3.158); Note 1 to entry: Assets include but are not limited to human, physical, **information** (3.116), intangible and environmental **resources** (3.193).

38. **Attack (DNI):** Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
39. **Attack** (ISO 22380): successful or unsuccessful attempt(s) to circumvent an **authentication solution** (3.19), including attempts to imitate, produce or reproduce the authentication **elements** (3.17)
40. **Attribute data management system, ADMS** (ISO 22380): system that stores, manages and controls access of data pertaining to **objects** (3.151)
41. **Audit (GFSI):** A systematic and functionally independent examination to determine whether activities and related results comply with a conforming scheme, whereby all the elements of this scheme should be covered by reviewing the supplier's manual and related procedures, together with an evaluation of the production facilities.
42. **Audit** (ISO 22380): systematic, independent and documented **process** (3.180) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled; Note 1 to entry: The fundamental elements of an audit include the determination of the **conformity**(3.45) of an **object** (3.151) according to a **procedure** (3.179) carried out by **personnel** (3.169) not being responsible for the object audited.; Note 2 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit or a joint audit. ; Note 3 to entry: Internal audits, sometimes called first-party audits, are conducted by, or on behalf of, the **organization** (3.158) itself for **management** (3.135) **review** (3.197) and other internal purposes, and can form the basis for an organization's declaration of conformity. Independence can be demonstrated by the freedom from responsibility for the **activity** (3.1) being audited.; Note 4 to entry: External audits include those generally called second- and third-party audits. Second-party audits are conducted by parties having an interest in the organization, such as customers, or by other persons on their behalf. Third-party audits are conducted by external, independent auditing organizations such as those providing certification/registration of conformity or government agencies.; Note 5 to entry: When two or more **management systems** (3.137) are audited together, this is termed a combined audit.; Note 6 to entry: When two or more auditing organizations cooperate to audit a single auditee, this is termed a joint audit.; Note 7 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.; Note 8 to entry: ISO 28000 specifies the **requirements** (3.190) for a **security management** (3.227) system. [SOURCE: ISO 9000:2015, 3.13.1, modified — Note 5 to entry has been replaced and Notes 6 to 8 to entry have been added.]
43. **Audit Agent (FDA, FSMA, US CODE):** The term 'audit agent' means an individual who is an employee or agent of an accredited third-party auditor and, although not individually accredited, is qualified to conduct food safety audits on behalf of an accredited third-party auditor.
44. **Audit, Consultative (FDA, FSMA, US CODE):** The term 'consultative audit' means an audit of an eligible entity— ''(A) to determine whether such entity is in compliance with the provisions of this Act and with applicable industry standards and practices; and (B) the results of which are for internal purposes only."
45. **Auditor (GFSI):** A person qualified to carry out audits for or on behalf of a certification body.
46. **Auditor** (ISO 22380): person who conducts an **audit** (3.13)
47. **Auditor, Accredited Third-Party (FDA, FSMA, US CODE):** The term 'accredited third-party auditor' means a third-party auditor accredited by an accreditation body to conduct audits of eligible entities to certify that such eligible entities meet the applicable requirements of this section. An accredited third-party auditor may be an individual who conducts food safety audits to certify that eligible entities meet the applicable requirements of this section.
48. **Auditor, Third-Party (FDA, FSMA, CFR):** The term 'third-party auditor' means a foreign government, agency of a foreign government, foreign cooperative, or any other third party, as the Secretary

determines appropriate in accordance with the model standards described in subsection (b)(2), that is eligible to be considered for accreditation to conduct food safety audits to certify that eligible entities meet the applicable requirements of this section. A third-party auditor may be a single individual. A third-party auditor may employ or use audit agents to help conduct consultative and regulatory audits.

49. **Authentic (ISO 12931):** "Authentic material good: material good produced under the control of the legitimate manufacturer, originator of the good or holder of intellectual property rights" (ISO 12931:2012),
50. **Authentic material good** (ISO 22380): **material good** (3.139) produced under the control of the legitimate manufacturer, originator of the **goods** (3.98) or **rights holder** (3.198)
51. **Authentic record (ISO 18829):** record that can be proven: a) to be what it purports to be, b) to have been created or sent by the person purported to have created or sent it, and c) to have been created or sent at the time purported
52. **Authentic, Food (Elliott Review) –** "…reflects a reasonable assumption made on the basis of the labeling provided on the finished product bought by the consumer (or the description in a menu entry). 'Reasonableness' should be a Wednesbury test in that it should assume no specialist knowledge of the food industry.
53. **Authentication (DNI):** The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.
54. **Authentication** (ISO 22380): **process** (3.180) of corroborating an **entity** (3.79) or attributes with a specified or understood level of assurance
55. **Authentication (ISO misc.):** Summary: The act or process of proving something is genuine, assurance of the claimed identity such as origin or performance; "Process of determining whether an entity or data is/are who or what, respectively, it claims to be" (ISO/IEC 18000-63:2015), "action of proving that someone or something is genuine" (ISO 8583-1:2003), "assurance of the claimed identity," "provision of assurance that a claimed characteristic of an entity is correct" (ISO/IEC 27000:2016), "process of determining whether an entity or data is/are who or what, respectively, it claims to be," and "the act of proving or showing to be of undisputed origin or veracity."
56. **Authentication (NIST3):** the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
57. **Authentication element** (ISO 22380): tangible **object** (3.151), visual feature or **information** (3.116) associated with a **material good** (3.139)or its packaging that is used as part of an **authentication solution** (3.19)
58. **Authentication function** (ISO 22380): function performing **authentication** (3.16)
59. **Authentication method (ISO TC292):** process of identity authentication using one or more authentication factors (ISO/IEC TR 29156:2015)
60. **Authentication solution** (ISO 22380): complete set of means and **procedures** (3.179) that allows the **authentication** (3.16) of a **material good** (3.139) to be performed
61. **Authentication solution (ISO ISO 12931):** complete set of means and procedures that allows the authentication of a material good to be performed
62. **Authentication tool (ISO 12931):** set of hardware and/or software system(s) that is part of an anticounterfeiting solution and is used to control of the authentication element
63. **Authentication tool** (ISO 22380): set of hardware and/or software system(s) that is part of an anti-counterfeiting solution and is used to control the **authentication element** (3.17)
64. **Authentication, food product (CEN):** The process of verifying the accuracy and correctness of the match between the food product characteristic and the corresponding claim
65. **Authentication, Multifactor (DNI):** Authentication using two or more factors to achieve authentication. Factors include (DNI): (i) something you know (e.g. password/PIN); (ii) something

you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See Authenticator.

66. **Authenticator (DNI):** The means used to confirm the identity of a user, processor, or device (e.g., user password or token).
67. **Authenticity (DNI):** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication.
68. **Authenticity (ISO 17427):** Summary: "Property of being of undisputed origin and not a copy, authenticated, and having the origin supported by unquestionable evidence" (ISO/TR 17427-4:2015 Intelligent transport systems), "property that an entity is what it claims to be," "The property that the claimed data source can be verified to the satisfaction of the recipient."
69. **Authenticity, food product (CEN):** A match between the actual food product characteristic and the corresponding food product claim; when the food product actually is what the claim says that it is
70. **Authoritative source** (ISO 22380): official origination of an attribute which is also responsible for maintaining that attribute
71. **Authorized economic operator** (ISO 22380): party involved in the international movement of **goods** (3.98) in whatever function that has been approved by or on behalf of a national customs administration as conforming to relevant **supply chain**(3.251) security standards; Note 1 to entry: "Authorized economic operator" is a term defined in the World Customs Organization(WCO) (3.277) Framework of Standards; Note 2 to entry: Authorized economic operators include, among others, manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses and distributors.
72. **Automated interpretation** (ISO 22380): **process** (3.180) that automatically evaluates authenticity by one or more components of the **authentication solution** (3.19)
73. **Availability (NIST2)**: ensuring timely and reliable access to and use of data.
74. **Between-unit homogeneity** (ISO Guide 30): <reference material, RM> uniformity of a specified property value among units of a reference material; Note 1 to entry: It is understood that the term "between-unit homogeneity" applies to any type of package (e.g. vial) and other physical shapes and test pieces.
75. **Bias (also called Inaccuracy) (Capra):** "is defined as systematic deviation from the truth" (Ref capra). In this context it is very different from a more general dictionary definition such as "an attitude that always favors one way of feeling or acting especially without considering any other possibilities" (Ref Webster's).
76. **Big Data Application Provider (NIST2):** Organization or entity that executes a generic vertical system data life cycle, including: (a) data collection from various sources, (b) multiple data transformations being implemented using both traditional and new technologies, (c) diverse data usage, and (d) data archiving.
77. **Big Data Engineering (NIST2):** Advanced techniques that harness independent resources for building scalable data systems when the characteristics of the datasets require new architectures for efficient storage, manipulation, and analysis.
78. **Big Data Framework Provider (NIST2):** Organization or entity that provides a computing fabric (such as system hardware, network, storage, virtualization, and computing platform) to execute certain Big Data applications, while maintaining security and privacy requirements.
79. **Biodefense / bio-defense (US GOVT.):** "…includes "medical measures to protect people against bioterrorism" which includes "medicines and vaccinations" (NLM 2016). The World Health Organization generally defines **biosecurity** as "protecting biological resources from foreign or invasive species" (UNOG). (Note: USG is US Government)
80. **Biosafety/ bio-safety (WHO/UN):** "… as "prevent unintentional exposure to pathogens and toxins, or their accidental release"(UNOG). " (Spink, Moyer, Huff, Et Al, Working)

81. **Biosecurity, Agricultural (US CODE): "** means protection from an agent that poses a threat to- (A) plant or animal health; (B) public health as it relates to the adulteration of products regulated by the Secretary of Agriculture under any provision of law that is caused by exposure to an agent; or (C) the environment as it relates to agriculture facilities, farmland, and air and water within the immediate vicinity of an area associated with an agricultural disease or outbreak. (7 US CODE 8901)
82. **Bioterrorism/ bio-terrorism (US GOVT.):** "…which is defined by the US FDA as "threatened or actual terrorist attack on the U.S. food supply and other food-related emergencies" (FDA 2002) and by the USA Center for Disease Control (CDC) "the deliberate release of viruses, bacteria, or other germs (agents) used to cause illness or death in people, animals, or plants. … Biological agents can be spread through the air, through water, or in food" (CDC 2013). Examples are from the USA Center for Disease Control (CDC) includes Anthrax, Botulism, Brucellosis, Plague, Smallpox and Tularemia (CDC 2013). " (Spink, Moyer, Huff, Et Al, Working)
83. **Black Economy (Black's law):** See "Shadow Economy" or "Black Market."
84. **Black Market (Black's law):** An illegal market for goods that are controlled or prohibited by the government, such as the underground market for prescription drugs.
85. **Blending / Mixing (ASTA1):** "Spices provide a distinct, characteristic color and/or flavor to food but, being a natural product, these can vary depending on where they are grown, weather conditions, crop season and other natural reasons. The blending together of different qualities of the same ingredient in order to reduce the natural variation in the aromatic profile (so called "standardization") cannot be considered adulteration. In other cases, blending together different qualities of the same ingredient can be done in order to achieve specific results (e.g. more or less pungency, improved machinability, improve color). This cannot be considered adulteration either (see also Annex I)."
86. **Brokers (ASTA1):** "Companies that facilitate a transaction between a domestic or foreign supplier and a buyer. Responsibilities include negotiating contract terms and handling paperwork and other logistics if requested by either party."
87. **Business Case (DNI):** Structured proposal that justifies a project for decision-makers. Includes an analysis of business process performance and requirements, assumptions, and issues. Also presents the risk analysis by explaining strengths, weaknesses, opportunities, and threats.
88. **Business Case Analysis, BCA (DNI):** An expanded cost/benefit analysis created with the intent of determining a best-value solution for product support. Alternatives weigh total cost against total benefits to arrive at the optimum solution.
89. **Business continuity** (ISO 22380): capability of an **organization** (3.158) to continue the delivery of **products or services** (3.181) at acceptable predefined levels following a **disruption** (3.70)
90. **Business impact analysis** (ISO 22380): **process** (3.180) of analyzing **activities** (3.1) and the effect that a business **disruption** (3.70) can have upon them
91. **Business partner** (ISO 22380): contractor, supplier or service provider with whom an **organization** (3.158) contracts to assist the organization in its function as an **organization in the supply chain** (3.159)
92. **Calibrant** (ISO Guide 30): <of a reference material (RM)> reference material used for calibration of equipment or a measurement procedure
93. **Candidate reference material** (ISO Guide 30): <of a reference material (RM)> material, intended to be produced as a reference material (RM); Note 1 to entry: A candidate material has yet to be characterized and tested to ensure that it is fit for use in a measurement process. To become an RM, a candidate material needs to be investigated to determine if it is sufficiently homogeneous and stable with respect to one or more specified properties, and is fit for its intended use in the development of measurement and test methods that target those properties; Note 2 to entry: A

candidate reference material may be an RM for other properties, and a candidate reference material for the target property.

94. **Capability (DNI):** The ability to perform one or more functions. In this sense, a capability may be represented as a generic statement (e.g., "the ability to collect and analyze human intelligence") or may be more specific to address an explicit function (e.g., "the ability to plot coordinates on a map).
95. **Capability Gap (DNI):** The inability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks. The gap may be the result of no existing capability, lack of proficiency or sufficiency in existing capability, or the need to recapitalize an existing capability.
96. **Capacity** (ISO 22380): combination of all the strengths and **resources** (3.193) available within an **organization** (3.158), **community** (3.42) or society that can reduce the level of **risk** (3.199) or the effects of a **crisis** (3.59); Note 1 to entry: Capacity can include physical, institutional, social, or economic means as well as skilled **personnel** (3.169) or attributes such as leadership and **management** (3.135).
97. **Cargo transport unit** (ISO 22380): road freight vehicle, railway freight wagon, freight container, road tank vehicle, railway tank wagon or portable tank
98. **Certainty (Capra) :** Is generally a statement of the confidence in a measurement. A general definition is "1. fixed, settled, 2. of a specific but unspecified character, quantity, or degree, 3. dependable, reliable, indisputable, etc." (Merriam-Webster 2004). The ISO/IEC Guide 98-3:2008 (JCGM/WG1/100), Uncertainty of measurement -- Part 3: Guide to the expression of uncertainty in measurement (GUM:1995) covers this topic. The ISO definition of Uncertainty (of measurement) is "[A] parameter, associated with the result of a measurement that characterizes the dispersion of the values that could reasonably be attributed to the [thing being measured]" (REF ISO 2008). Further from that definition "The parameter may be, for example, a standard deviation (or a given multiple of it), or the half-width of an interval having a stated level of confidence".
99. **Certification (GFSI):** A process by which accredited certification bodies, based on an audit, provide written assurance those food safety requirements and management systems and their implementation conform to requirements.
100. **Certification Body - CB (GFSI):** A provider of certification services, accredited to do so by an Accreditation Body.
101. **Certification Program Organization - CPO (GFSI):** The organization that oversees the A food safety scheme that has successfully completed the GFSI Benchmark Process.
102. **Certified client** (ISO 22380): **organization** (3.158) whose **supply chain** (3.251)**security management** (3.227) system has been certified/registered by a qualified third party
103. **Certified reference material, CRM** (ISO Guide 30): reference material (RM) characterized by a metrologically valid procedure for one or more specified properties, accompanied by an RM certificate that provides the value of the specified property, its associated uncertainty, and a statement of metrological traceability; Note 1 to entry: The concept of value includes a nominal property or a qualitative attribute such as identity or sequence. Uncertainties for such attributes may be expressed as probabilities or levels of confidence; Note 2 to entry: Metrologically valid procedures for the production and certification of RMs are given in, among others, ISO Guides 34[2]and 35[3]; Note 3 to entry: ISO Guide 31[4] gives guidance on the contents of RM certificates; Note 4 to entry: ISO/IEC Guide 99:2007[1] has an analogous definition (5.14).
104. **Certified value (ISO Guide 30):** <of a reference material (RM)> value, assigned to a property of a reference material (RM) that is accompanied by an uncertainty statement and a statement of metrological traceability, identified as such in the RM certificate
105. **Characteristic, food product (CEN):** A distinguishing feature of the (food) product, Note 1 to entry: A product characteristic can be qualitative or quantitative; Note 2 to entry: A product

characteristic can be inherent in the product itself, or it can relate to the conditions under which the product was produced, or the environment it was produced in; Note 3 to entry: A product characteristic is sometimes referred to as a product attribute or a product property, Note 4 to entry: There are various classes of product characteristics, such as the following: physical (e.g. mechanical, electrical, chemical or biological characteristics), sensory (e.g. related to smell, touch or taste), functional (e.g. medicinal quality of a food product), related to origin (e.g. raw material used, identity of primary processor), related to processing or production method (e.g. mildly processed, cooked at low temperature, halal production, kosher production), related to standards, defined practices, certification schemes or regulations (e.g. produced according to some specification). This characteristic is normally connected to other specified product characteristics that must be present or absent or have some particular value.

106. **Characterization** (ISO Guide 30): <of a reference material> determination of the property values or attributes of a reference material, as part of the production process; Note 1 to entry: See also the IUPAC Compendium of Analytical Nomenclature.[5]
107. **Civil protection** (ISO 22380): measures taken and systems implemented to preserve the lives and health of citizens, their properties and their environment from undesired **events** (3.82); Note 1 to entry: Undesired events can include accidents, emergencies and **disasters** (3.69).
108. **Claim, food product (CEN):** A statement where a (food) product is said to have a certain characteristic; Note 1 to entry: The claim can be explicit, e.g. on the label or in the accompanying documentation, or it can be implicit, in that if the food product had the characteristic in question, it should have been stated explicitly; Note 2 to entry: A product claim is sometimes referred to as a product description.
109. **Client** (ISO 22380): **entity** (3.79) that hires, has formerly hired, or intends to hire an **organization** (3.158) to perform **security operations** (3.232) on its behalf, including, as appropriate, where such an organization subcontracts with another company or local forces; EXAMPLE: Consumer, contractor, end-user, retailer, beneficiary, purchaser.; Note 1 to entry: A client can be internal (e.g. another division) or external to the organization.
110. **Code, Penal (Black's Law):** A compilation of criminal laws, usually defining and categorizing the offenses and setting forth their respective punishments.
111. CODEX: abbreviation for Codex Alimentarius (Codex Alimentarius 2014)
112. **Command and control** (ISO 22380): **activities** (3.1) of target-orientated decision making, including assessing the situation, **planning**(3.170), implementing decisions and controlling the effects of implementation on the **incident** (3.111); Note 1 to entry: This **process** (3.180) is continuously repeated.
113. **Command and control system** (ISO 22380): system that supports effective **emergency management** (3.78) of all available **assets** (3.10) in a preparation, **incident response** (3.115), **continuity** (3.49) and/or **recovery** (3.187) **process** (3.180)
114. **Community** (ISO 22380): group of associated **organizations** (3.158), individuals and groups sharing common interests; Note 1 to entry: Impacted communities are the groups of people and associated organizations affected by the provision of **security** (3.223) services, projects or operations.
115. **Community of Interest, COI (DNI):** A collaborative group of users who exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have a shared vocabulary for the information they exchange. The group exchanges information within and between systems to include security domains.
116. **Community-based warning system** (ISO 22380): method to communicate **information** (3.116) to the public through established networks

117. **Commutability** (ISO Guide 30): property of a reference material (RM), demonstrated by the equivalence of the mathematical relationships among the results of different measurement procedures for an RM and for representative samples of the type intended to be measured; Note 1 to entry: See also ISO/IEC Guide 99:2007,[1]ISO 17511:2003.[7]
118. **Comparable Standards (DNI):** Standards on the same products, processes or services, approved by different standardizing bodies, in which different requirements are based on the same characteristics and assessed by the same methods, thus permitting unambiguous comparison of differences in the requirements. NOTE: Comparable standards are not harmonized (or equivalent) standards.
119. **Compatibility (DNI):** Suitability of products, processes or services for use together under specific conditions to fulfill relevant requirements without causing unacceptable interactions.
120. **Competence** (ISO 22380): ability to apply knowledge and skills to achieve intended results
121. **Compliance (DNI):** Obliged adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements. See Conformance.
122. **Confidentiality (NIST2):** preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary data; and
123. **Conforming scheme (GFSI):** A food safety scheme that has successfully completed the GFSI Benchmark Process.
124. **Conformity:** fulfilment of a **requirement** (3.190)
125. **Consensus (DNI):** General agreement, characterized by the absence of sustained opposition to substantial issues by any important part of the concerned interests and by a process that involves seeking to take into account the views of all parties concerned and to reconcile any conflicting arguments. Note consensus need not imply unanimity.
126. **Consensus Body (DNI):** The group that approves the content of a standard and whose vote demonstrates evidence of consensus.
127. **Consequence (DHS Lexicon 2017):** effect of an event, incident, or occurrence
128. **Consequence (ISO 31000): "**outcome of an event (2.17) affecting objectives"; NOTE 1 an event can lead to a range of consequences. NOTE 2 a consequence can be certain or uncertain and can have positive or negative effects on objectives. NOTE 3 consequences can be expressed qualitatively or quantitatively. NOTE 4 initial consequences can escalate through knock-on effects. [ISO Guide 73:2009, definition 3.6.1.3]
129. **Contaminant (CODEX, Procedural Manual):** "Codex Alimentarius defines a contaminant as follows: "Any substance not intentionally added to food, which is present in such food as a result of the production (including operations carried out in crop husbandry, animal husbandry and veterinary medicine), manufacture, processing, preparation, treatment, packing, packaging, transport or holding of such food or as a result of environmental contamination. The term does not include insect fragments, rodent hairs and other extraneous matter." (CODEX STAN 193-1995)
130. **Contaminant (FDA, FSMA IA Guide):** Contaminant means, for purposes of this part, any biological, chemical, physical, or radiological agent that may be added to food to intentionally cause illness, injury, or death.
131. **Contaminant (FSMA-IA):** substances intentionally added to cause harm (FSMA IA Final Rule, Part B. Other definitions, 2. Contaminant)
132. **Contamination (DNI):** Type of incident involving the introduction of data of one security classification or security category into data of a lower security classification or different security category.
133. **Contamination (IFS):** Introduction or occurrence of a contaminant in food or food environment. Contamination does include: physical, chemical, biological contamination. Contamination can also mean correlation of packages among themselves.

134. **Contamination** (ISO 22000): introduction or occurrence of a contaminant including a **food safety hazard** (3.22) in a **product** (3.37) or processing environment
135. **Contingency** (ISO 22380): possible future **event** (3.82), condition or eventuality
136. **Continual improvement** (ISO 22000): recurring activity to enhance **performance** (3.33)
137. **Continuity** (ISO 22380): strategic and tactical capability, pre-approved by **management** (3.135), of an **organization** (3.158) to plan for and respond to conditions, situations and **events** (3.82) in order to continue operations at an acceptable predefined level; Note 1 to entry: Continuity is the more general term for operational and **business continuity** (3.24) to ensure an organization's ability to continue operating outside of normal operating conditions. It applies not only to for-profit companies, but to organizations of all types, such as non-governmental, public interest and governmental.
138. **Control activities (GAO Green):** The policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks (paragraph 10.02)
139. **Control measure** (ISO 22000): action or activity that is essential to prevent a significant **food safety hazard** (3.22) or reduce it to an **acceptable level** (3.1); Note 1 to entry: See also **significant food safety hazard** (3.40); Note 2 to entry: Control measure(s) is (are) identified by hazard analysis.
140. **Control System (NIST3):** A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable.
141. **Control System (Rohan):** A control system is an interconnection of components forming a system configuration that will provide a desired system response.
142. **Conveyance** (ISO 22380): physical instrument of international trade that transports **goods** (3.98) from one location to another; EXAMPLE: Box, pallet, **cargo transport unit** (3.32), cargo handling equipment, truck, ship, aircraft, railcar.
143. **Cooperation** (ISO 22380): process of working or acting together for common interests and values based on agreement; Note 1 to entry: The **organizations** (3.158) agree by contract or by other arrangements to contribute with their **resources** (3.193) to the **incident response** (3.115) but keep independence concerning their internal hierarchical structure.
144. **Coordination** (ISO 22380): way in which different **organizations** (3.158) (public or private) or parts of the same organization work or act together in order to achieve a common **objective** (3.153); Note 1 to entry: Coordination integrates the individual response **activities** (3.1) of involved parties (including, for example, public or private organizations and government) to achieve synergy to the extent that the **incident response** (3.115) has a unified objective and coordinates activities through transparent **information** (3.116) sharing regarding their respective incident response activities; Note 2 to entry: All organizations are involved in the **process** (3.180) to agree on a common incident response objective and accept to implement the strategies by this consensus decision-making process.
145. **Copyright (Black's law):** 1. the right to copy; specifically, a property right in an original work of authorship (including literary, musical, dramatic, choreographic, pictorial, graphic, sculptural, and architectural works; motion pictures and other audiovisual works; and sound recordings) fixed in any tangible medium of expression, giving the holder the exclusive right to reproduce, adapt, distribute, perform, and display the work.
146. **Copyright** (TRIPs)**:** "Copyright protection shall extend to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such" (REF TRIPS). Furthermore "Computer programs, whether in source or object code, shall be protected as literary works," "Compilations of data or other material, whether in machine readable or other form," (REF TRIPS). "A form of protection provided to the authors of "original works of authorship." This generally

protects “Literary, dramatic, musical, artistic, and certain” and the duration is “In general, author’s life + 70 years” (REF USPTO)

147. **Copyright Infringement (Black’s law):** The act of violating any of a copyrights owner’s exclusive rights granted by the federal Copyright Act.

148. **Correction (FSMA-PC Guide):** An action to identify and correct a problem that occurred during the production of food, without other actions associated with a corrective action procedure (such as actions to reduce the likelihood that the problem will recur, evaluate all affected food for safety, and prevent affected food from entering commerce).

149. **Correction** (ISO 22380): action to eliminate a detected **nonconformity** (3.149)

150. **Corrective action (FSMA-PC Guide):** An action to identify and correct a problem that occurred during the production of food, including actions associated with a corrective action procedure (such as actions to reduce the likelihood that the problem will recur, evaluate all affected food for safety, and prevent affected food from entering commerce).

151. **Corrective action** (ISO 22380): action to eliminate the cause of a **nonconformity** (3.149) and to prevent recurrence; Note 1 to entry: In the case of other undesirable outcomes, action is necessary to minimize or eliminate causes and to reduce **impact** (3.107) or prevent recurrence. Such actions fall outside the concept of “corrective action” in the sense of this definition.

152. **Counterfeit (Black’s law):** To unlawfully forge, copy, or imitate an item, especially money or a negotiable instrument (such as a security or promissory note) or other officially issued item of value (such as a postage stamp or a food stamp), or to possess such an item without authorization and with the intent to deceive or defraud by presenting the item as genuine. Counterfeiting includes producing or selling an item that displays a reproduction of a genuine trademark, usually to deceive buyers into thinking they are purchasing genuine merchandise. (Includes: counterfeiter)

153. **Counterfeit (IEC in ISO 12931):** goods made to imitate something of value, which may not be made with the same level of safety, quality or reliability

154. **Counterfeit (ISO 12931):** material good imitating or copying an authentic material good

155. **Counterfeit (ISO 22380):** simulate, reproduce or modify a **material good** (3.139) or its packaging without authorization

156. **Counterfeit good (ISO 22380): material good** (3.139) imitating or copying an **authentic material good** (3.15)

157. **Counterfeit Material good (ISO 22300):** imitating or copying an authentic material good (3.15) counterfeit simulate, reproduce or modify a material good (3.139) or its packaging without authorization

158. **Counterfeit Trademark (Black’s law):** A spurious mark that is identical to, or substantially indistinguishable from, a registered trademark. – Also termed “counterfeit mark.”

159. **Counterfeit trademark goods** (TRIPs)**:** “shall mean any goods, including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such goods, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the owner of the trademark in question under the law of the country of importation;”

160. **Counterfeiters (GMA BP):** are organizations that create and distribute inauthentic or adulterated product for profit

161. **Counterfeiting (Black’s law):** (The unlawful acts of counterfeit) The unlawful forgery, copying, or imitating of an item, especially money or a negotiable instrument (such as a security or promissory note) or other officially issued item of value (such as a postage stamp or a food stamp), or to poses such an item without authorization and with the intent to deceive or defraud by presenting the item as genuine. Counterfeiting includes producing or selling an item that displays a reproduction of a

genuine trademark, usually to deceive buyers into thinking they are purchasing genuine merchandise.

162. **Counterfeiting, Product (WHO Glossary):** unauthorized representation of a registered trademark carried on goods identical or similar to goods for which the trademark is registered, with a view to deceiving the purchaser into believing that he/she is buying the original goods

163. **Counterintelligence (DNI):** Information gathered and activities conducted to identify, deceive, exploit, interdict, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, foreign organizations or persons, or international terrorist organizations or activities.

164. **Countermeasure (DNI):** The deployment of a set of security services to protect against a security threat.

165. **Countermeasure** (ISO 22380): action taken to lower the **likelihood** (3.133) of a **security threat scenario** (3.241) succeeding in its **objectives** (3.153), or to reduce the likely **consequences** (3.46) of a security threat scenario

166. **Covert authentication element** (ISO 22380): **authentication element** (3.17) that is generally hidden from the human senses and can be revealed by an informed person using a tool or by **automated interpretation** (3.23)

167. **Crime (Black's Law):** An act that the law makes punishable; the breach of a legal duty treated as the subject-matter of a criminal proceeding. – Also termed "criminal wrong."

168. **Crime, Consensual (Black's Law):** See "Victimless Crime."

169. **Crime, Corporate (Black's Law):** A crime committed by a corporation's representatives acting on its behalf. / Although a corporation as an entity cannot commit a crime other than through its representatives, it can be named a criminal defendant. –Also termed "organizational crime."

170. **Crime, Economic (Black's Law):** A nonphysical crime committed to obtain a financial gain or professional advantage. (Two types: in regular business activities [e.g. embezzlement] and white collar crime [e.g. larger organized activity])

171. **Crime, Occupational (Black's Law):** A crime that a person commits for personal gain while on the job.

172. **Crime, Organized (Black's Law):** 1. Wide-spread criminal activities that are coordinated and controlled through a central syndicate. See "Racketeering." 2. Persons involved in these criminal activities; a syndicate of criminals who rely on their unlawful activities for income.

173. **Crime, Statutory (Black's Law):** A crime punishable by statute.

174. **Crime, Victimless (Black's Law):** A crime that is considered to have no direct victim, usually because only consent adultery [see Adultery] is involved. Examples are possession of illicit drugs and deviant sexual intercourse between consenting adults.

175. **Crime, White-collar (Black's Law):** A nonviolent crime usually involving cheating or dishonesty in commercial matters. Examples include fraud, embezzlement, bribery, and insider trading.

176. **Crisis** (ISO 22380): unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, **assets** (3.10), property or the environment

177. **Crisis management** (ISO 22380): holistic **management** (3.135)**process** (3.180) that identifies potential **impacts** (3.107) that threaten an **organization** (3.158) and provides a framework for building **resilience** (3.192), with the capability for an effective response that safeguards the interests of the organization's key **interested parties**(3.124), reputation, brand and value-creating **activities** (3.1), as well as effectively restoring operational capabilities; Note 1 to entry: Crisis management also involves the management of **preparedness** (3.172), **mitigation** (3.146) response, and **continuity** (3.49) or **recovery** (3.187) in the event of an **incident** (3.111), as well as management of the overall programme

through **training** (3.265), rehearsals and **reviews** (3.197) to ensure the preparedness, response and continuity plans stay current and up-to-date.

178. **Crisis management team** (ISO 22380): group of individuals functionally responsible for directing the development and execution of the response and operational **continuity** (3.49) plan, declaring an operational **disruption** (3.70) or **emergency** (3.77)/**crisis** (3.59) situation, and providing direction during the **recovery** (3.187)**process**(3.180), both pre-and post-disruptive **incident** (3.111); Note 1 to entry: The **crisis management team** (3.61) can include individuals from the **organization**(3.158) as well as immediate and first responders, and **interested parties** (3.124).
179. **Crisis: (US GOVT.):** "…is an event that has occurred – or is occurring – that has a confirmed harm (ANSI 2009) – this includes imminent hazard (21 CFR), attack, emergency (ISO 2007b, 21 CFR, FDA 2016), disaster, etc. " (Spink, Ortega, Chen & Wu, 2017)
180. **Critical Control Point (CCP) (FDA, FSMA, US CODE):** The term 'critical control point' means a point, step, or procedure in a food process at which control can be applied and is essential to prevent or eliminate a food.
181. **Critical control point (CCP) (FSMA-PC Guide):** A point, step, or procedure in a food process at which control can be applied and is essential to prevent or eliminate a food safety hazard or reduce such hazard to an acceptable level.
182. **Critical control point (CCP)** (ISO 22000): step in the **process** (3.36) at which **control measure(s)** (3.8) is (are) applied to prevent or reduce a **significant food safety hazard**(3.40) to an acceptable level, and defined **critical limit(s)** (3.12) and **measurement** (3.26) enable the application of **corrections** (3.9). [Note: ISO 22000 Food Safety Management narrows the scope to food safety.]
183. **Critical control point, CCP** (ISO 22380): point, step or **process** (3.180) at which controls can be applied and a **threat** (3.259) or **hazard** (3.99)can be prevented, eliminated or reduced to acceptable levels. [Note: ISO 22380 covers all products and thus the scope is NOT narrowed to only food safety hazards.] [Note: ISO 22380 is under product fraud NOT part of the ISO 22000 food safety series.]
184. **Critical Customer** (ISO 22380): **entity** (3.79), the loss of whose business would threaten the survival of an **organization** (3.158)
185. **Critical Infrastructure (DHS):** the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The nation's critical infrastructure provides the essential services that underpin American society.
186. **Critical Infrastructure Protection (DNI):** Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include; changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc.
187. **Critical limit (CL) (FSMA-PC Guide):** A maximum and/or minimum value to which a biological, chemical, or physical parameter must be controlled to prevent, eliminate or reduce to an acceptable level the occurrence of a food-safety hazard.
188. **Critical limit** (ISO 22000): measurable value which separates acceptability from unacceptability; Note 1 to entry: Critical limits are established to determine whether a **CCP** (3.11) remains in control. If a critical limit is exceeded or not met, the products affected are to be handled as potentially unsafe products.[SOURCE: CAC/RCP 1-1969, modified — The definition has been modified and Note 1 to entry has been added.]
189. **Critical product or service** (ISO 22380): **resource** (3.193) obtained from a supplier which, if unavailable, would disrupt an **organization's**(3.158) critical **activities** (3.1) and threaten its survival
190. **Critical supplier** (ISO 22380): provider of **critical products or services** (3.64); Note 1 to entry: This includes an "internal supplier", who is part of the same **organization** (3.158) as its customer.

191. **Criticality analysis** (ISO 22380): **process** (3.180) designed to systematically identify and evaluate an **organization's** (3.158)**assets**(3.10) based on the importance of its mission or function, the group of **people at risk** (3.166), or the significance of an **undesirable event** (3.268) or **disruption** (3.70) on its ability to meet expectations
192. **Custodian copy** (ISO 22380): duplicate that is subordinate to the **authoritative source** (3.21)
193. **Custody** (ISO 22380): period of time where an **organization in the supply chain** (3.159) is directly controlling the manufacturing, handling, processing and transportation of **goods** (3.98) and their related shipping **information** (3.116) within the **supply chain** (3.251)
194. **Data (DNI):** A value or set of values representing a specific concept or concepts. Data become ""information"" when analyzed and possibly combined with other data in order to extract meaning, and to provide context. The meaning of Data can vary depending on its context.
195. **Data Consumer (NIST2):** End users or other systems that use the results of data applications.
196. **Data Contamination (DNI):** A deliberate or accidental process or act that compromises the integrity of the original data.
197. **Data Definition (DNI):** A description, which determines the rules to which one or more collections of data instances must conform.
198. **Data integrity (Manning): "**of information accompanying the food item throughout the supply chain i.e. the consistency and accuracy of data through the food product life-cycle"
199. **Data Provider (NIST2):** Organization or entity that introduces information feeds into the Big Data system for discovery, access, and transformation by the Big Data system.
200. **Data Quality (DNI):** Indications of the degree to which data satisfies stated or implied needs. This includes information about lineage, completeness, currency, logical consistency and accuracy of the data.
201. **Dependability (DNI):** That property of a computer system such that reliance can be justifiably placed on the service it delivers. The service delivered by a system is its behavior as it is perceived by its user(s); a user is another system or human that interacts with the former.
202. **Dependency (DNI):** A logical linkage between tasks. Most often a 'Finish - Start' (activity A must finish before activity B can start).
203. **Deprecate (DNI):** To mark (a component of a software standard) as obsolete to warn against its use in the future so that it may be phased out.
204. **Deviation (FSMA-PC Guide)::** Failure to meet a critical limit.
205. **Dilution (in the context of food fraud) (CEN)**: The process of increasing the quantities of an inactive or already present substance with the purpose of increasing weight or volume and thereby price; Note 1 to entry: Dilution is a type of food product adulteration.
206. **Disaster** (ISO 22380): situation where widespread human, material, economic or environmental losses have occurred which exceeded the ability of the affected **organization** (3.158), **community** (3.42) or society to respond and recover using its own **resources** (3.193)
207. **Disruption** (ISO 22380): **event** (3.82), whether anticipated (e.g. a labour strike or hurricane) or unanticipated (e.g. a blackout or earthquake), that causes an unplanned, negative deviation from the expected delivery of **products or services** (3.181) according to an **organization's** (3.158)**objectives** (3.153)
208. **Distributors (GMA BP):** are firms that sell or deliver merchandise to retail stores.
209. **Diversion (Black's Law):** 1. A deviation of alteration from the natural course of things; especially, the unauthorized alteration of a watercourse to the detriment of the lower riparian owner, or the unauthorized use of funds. 2. A distraction or pastime.
210. **Diverters (GMA BP):** can be authorized or unauthorized buyers or sellers of manufacturers' (brand owner) products. In the consumer goods market these diverters are typically the middle

person who may buy quantities of products from manufacturers, retailers and wholesalers and sells the inventory as a secondary source for distribution to retailers. The "diversion" of authorized branded products to unauthorized geographic regions or retail outlets is typically described as the sale of "grey goods," which are distinct from counterfeits that were never authorized by the brand owner. The issues associated with grey goods and diversion are beyond the scope of this guide. However, diverters, by way of their function as a source of legitimate goods (like overruns, closeouts, etc.) to the secondary retail market, are also an important potential entry point for counterfeit goods.

211. **Document** (ISO 22380): **information** (3.116) and the medium on which it is contained; Note 1 to entry: The medium can be paper, magnetic, electronic or optical computer disc, photograph or master sample, or a combination thereof; Note 2 to entry: A set of documents, for example specifications and **records** (3.186), is frequently called "documentation".
212. **Documented information** (ISO 22380): **information** (3.116) required to be controlled and maintained by an **organization** (3.158) and the medium on which it is contained; Note 1 to entry: Documented information can be in any format and media and from any source; Note 2 to entry: Documented information can refer to: — the **management system** (3.137), including related **processes** (3.180); — information created in order for the organization to operate (documentation); — evidence of results achieved (**records** (3.186)).
213. **Downstream** (ISO 22380): handling, processing and movement of **goods** (3.98) when they are no longer in the **custody** (3.68) of the organization in the **supply chain** (3.159)
214. **Drill** (ISO 22380): **activity** (3.1) which practises a particular skill and often involves repeating the same thing several times; EXAMPLE: A fire drill to practise safely evacuating a building on fire.
215. **Economic Adulteration (TBD):** Undefined, there no formal definition or glossary term was found. (NOTE: review, consider 1996 FDA Juice Adulteration report)
216. **Economic Adulteration (Webster's Dictionary):** combination of the definition of economic ("of or relating to the production, distribution, and consumption of goods and services" and adulteration ("the action of" or "the result of" "to corrupt, debase, or make impure by addition of a foreign or inferior substance or element, to prepare for sale by replacing more valuable with less valuable or inert ingredients."
217. **Economically motivated adulteration - EMA (PAS96:2014):** A typical feature of EMA (see 3.2) is the substitution of a low cost item in place of a relatively high cost component/ingredient. The TACCP team needs to be alert to the availability of such alternatives. An example where this may happen is when added value is claimed, (e.g. organic, non-gm, locally grown, free range or with protected designations of origin). The attacker is likely to have ready access to lower value equivalents, which are almost indistinguishable.
218. **Economically Motivated Adulteration (CODEX EWG, DRAFT 11/2017):** Comment – under review, currently defined as an adulterant-substance; "Economically motivated adulteration is the deliberate addition (including substitution) of an adulterant to a food item for financial gain through increasing the apparent quality or value of the product or reducing the cost of its production
219. **Economically motivated adulteration (EMA) – "FDA Working Definition" (FDA 2009):** "Fraudulent, intentional substitution or addition of a substance in a product for the purpose of increasing the apparent value of the product or reducing the cost of its production, i.e., for economic gain." (See Economically Motivated Hazard, Economically Motivated Food Safety Hazard, etc.) (Comment- that the "adulterated" scope does not align with the FDCA scope of "Adulterated Foods.")
220. **Economically Motivated Adulteration (FSMA-IA):** Comment - this was not defined in the final rule and refers to the FSMA-PC rule.

221. **Economically Motivated Adulteration (FSMA-PC)**: Comment - this is not defined in the FSMA-PC final rule but it was made clear by FDA that all "economically motivated" acts that lead to an agent that creates a health hazard are within the scope.
222. **Economically Motivated Adulteration (PCHF-QI):** See Economically Motivated Food Safety Hazard
223. **Economically Motivated Food Safety Hazard (EMFSH):** Comment a new term introduced in the FSMA Preventive Controls for Human Foods Qualified Individual Training (PCHF-QI) that is not explicitly defined.
224. **Economically motivated food safety hazard (PCHF-QI):** Undefined
225. **Economically Motivated Hazard (PCHF-QI): Un**defined. See Economically Motivated Food Safety Hazard
226. **Economically-Motivated Adulteration (EMA-FPDI/NCFPD): "**EMA is intentional adulteration of food by intelligent perpetrators actively trying to deceive consumers, defraud customers and avoid detection by quality assurance and regulatory systems. FPDI categorizes EMA into eight adulteration methods: dilution, substitution, artificial enhancement, mislabeling, trans-shipment and origin masking, counterfeiting, theft and resale, and intentional distribution of contaminated product." (Food Safety Magazine, December 2017); "EMA is often referred to as "food fraud," and FPDI uses the two terms interchangeably" (website FAQ).
227. **Economically-Motivated Adulteration (EMA-USP): "**More generally referred to as "food fraud," EMA is the fraudulent addition of non-authentic substances or removal or replacement of authentic substances without the purchaser's knowledge for the economic gain of the seller. An EMA-related adulterant (which is the focus of this guide [USP Food Fraud Mitigation Guide]) is an adulterant added to food by a supplier for economic gain."
228. **Effectiveness** (ISO 22000): extent to which planned activities are realized and planned results achieved
229. **Effectiveness** (ISO 22380): extent to which planned **activities** (3.1) are realized and planned results achieved
230. **Elasticity (NIST2):** The ability to dynamically scale up and down as a real-time response to the workload demand. Elasticity will depend on the Big Data system, but adding or removing "software threads" and "virtual or physical servers" are two widely used scaling techniques. Many types of workload demands drive elastic responses, including web-based users, software agents, and periodic batch jobs.
231. **Electronic commerce, e-commerce) (WTO):** The production, advertising, sale and distribution of products via telecommunications networks.
232. **Electronic database (DSCSA):** A manufacturer may satisfy the requirements of this paragraph by developing a secure electronic database or utilizing a secure electronic database developed or operated by another entity. The owner of such database shall establish the requirements and processes to respond to requests and may provide for data access to other members of the pharmaceutical distribution supply chain, as appropriate. The development and operation of such a database shall not relieve a manufacturer of the requirement under this paragraph to respond to a request for verification submitted by means other than a secure electronic database.
233. **Electronic format (DSCSA):** (i) In general.--Beginning not later than 4 years after the date of enactment of the Drug Supply Chain Security Act, except as provided under clause (ii), a manufacturer shall provide the transaction information, transaction history, and transaction statement required under subparagraph (A)(i) in electronic format.
234. **Emergency** (ISO 22380): sudden, urgent, usually unexpected occurrence or **event** (3.82) requiring immediate action; Note 1 to entry: An emergency is usually

a **disruption** (3.70) or condition that can often be anticipated or prepared for, but seldom exactly foreseen.

235. **Emergency management** (ISO 22380): overall approach for preventing **emergencies** (3.77) and managing those that occur; Note 1 to entry: In general, emergency management utilizes a **risk management** (3.208) approach to **prevention** (3.173), **preparedness** (3.172), response and **recovery** (3.187) before, during and after potentially destabilizing **events** (3.82) and/or **disruptions** (3.70).
236. **Enterprise (DNI):** An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management.
237. **Entity** (ISO 22380): something that has a separate and distinct existence and that can be identified within context; Note 1 to entry: An entity can be a human, **organization** (3.158), physical **object** (3.151), class of objects or intangible object.
238. **Entity-level control (GAO Green):** Controls that have a pervasive effect on an entity's internal control system; entity-level controls may include controls related to the entity's risk assessment process, control environment, service organizations, management override, and monitoring (paragraph 10.09)
239. **Environmental pathogen(FSMA-PC Guide):** A pathogen capable of surviving and persisting with the
240. **Evaluation** (ISO 22380): systematic **process** (3.180) that compares the result of **measurement** (3.143) to recognised criteria to determine the discrepancies between intended and actual **performance** (3.167)
241. **Event (DNI):** Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.
242. **Event** (ISO 22380): occurrence or change of a particular set of circumstances; Note 1 to entry: An event can be one or more occurrences, and can have several causes.; Note 2 to entry: An event can consist of something not happening.; Note 3 to entry: An event can sometimes be referred to as an **incident** (3.111) or "accident"; Note 4 to entry: An event without **consequences** (3.46) can also be referred to as a "near miss", "incident", "near hit" or "close call"; Note 5 to entry: The nature, **likelihood** (3.133), and consequence of an event cannot be fully knowable; Note 6 to entry: Likelihood associated with the event can be determined; Note 7 to entry: An event can consist of a non-occurrence of one or more circumstances; Note 8 to entry: An event with a consequence is sometimes referred to as an incident
243. **Event (US GOVT.):** "…is essentially something that occurs (ISO 2002, CNSSI 2010, Merriam-Webster 2004). There is no evaluation yet of the change in the consequence." (Spink, Ortega, Chen & Wu, 2017)
244. **Exercise** (ISO 22380): **process** (3.180) to train for, assess, practise and improve **performance** (3.167) in an **organization**(3.158); Note 1 to entry: Exercises can be used for validating policies, plans, **procedures** (3.179), **training**(3.265), equipment, and inter-organizational agreements; clarifying and training **personnel** (3.169) in roles and responsibilities; improving inter-organizational **coordination** (3.52) and communications; identifying gaps in **resources** (3.193); improving individual performance and identifying opportunities for improvement; and a controlled opportunity to practise improvisation; Note 2 to entry: See also **test** (3.257).
245. **Exhaustion (sales exhaustion rule) (WTO):** In intellectual property protection, the principle that once a product has been sold on a market, the intellectual property owner no longer has any rights over it. (A debate among WTO member governments is whether this applies to products put on the

market under compulsory licences.) Countries' laws vary as to whether the right continues to be exhausted if the product is imported from one market into another, which affects the owner's rights over trade in the protected product. See also parallel imports.

246. **Exposure (DNI):** Extent to which an organization and/or stakeholder is subject to an event.

247. **External control system (GAO Green):** opposite of internal control systems

248. **Extraneous matter (ASTA1):** "Extraneous matter is defined as everything foreign to the product itself and includes, but is not restricted to: stones, dirt, wire, string, stems, sticks, nontoxic foreign seeds, excreta, manure and animal contamination. ASTA1 has established Cleanliness Specifications that set limits on these items. The ASTA Cleanliness Specifications were designed to meet or exceed the FDA's Defect Action Levels (DALs). These levels can normally be achieved through a combination of Good Agricultural Practice followed by thorough physical cleaning (Good Manufacturing Practice)."

249. **Facility (FSMA-PC Guide):** A domestic facility or foreign facility that is required to register under section 415 of the Federal Food, Drug, and Cosmetic Act, in accordance with the requirements of 21 CFR part 1, subpart H.

250. **Facility** (ISO 22380): plant, machinery, property, buildings, transportation units, sea/land/air ports and other items of **infrastructure** (3.117) or plant and related systems that have a distinct and quantifiable business function or service

251. **False acceptance rate** (ISO 22380): proportion of **authentications** (3.16) wrongly declared true

252. **False rejection rate** (ISO 22380): proportion of **authentications** (3.16) wrongly declared false

253. **Falsified (WHO IMPACT)**: medical products that deliberately/fraudulently misrepresent their identity, composition or source.

254. **Fishing - Illegal fishing (EU):** means fishing activities: (a) conducted by national or foreign fishing vessels in maritime waters under the jurisdiction of a State, without the permission of that State, or in contravention of its laws and regulations; (b) conducted by fishing vessels flying the flag of States that are contracting parties to a relevant regional fisheries management organisation, but which operate in contravention of the conservation and management measures adopted by that organisation and by which those States are bound, or of relevant provisions of the applicable international law; or (c) conducted by fishing vessels in violation of national laws or international obligations, including those undertaken by cooperating States to a relevant regional fisheries management organisation;"

255. **Fishing - Illegal, unreported and unregulated (IUU) fishing** (EU Regulation 1005/2008): see entries for each word

256. **Fishing - Unregulated fishing (EU):** means fishing activities: (a) conducted in the area of application of a relevant regional fisheries management organisation by fishing vessels without nationality, by fishing vessels flying the flag of a State not party to that organisation or by any other fishing entity, in a manner that is not consistent with or contravenes the conservation and management measures of that organisation; or (b) conducted in areas or for fish stocks in relation to which there are no applicable conservation or management measures by fishing vessels in a manner that is not consistent with State responsibilities for the conservation of living marine resources under international law

257. **Fishing - Unreported fishing (EU):** means fishing activities: (a) which have not been reported, or have been misreported, to the relevant national authority, in contravention of national laws and regulations; or(b) which have been undertaken in the area of competence of a relevant regional fisheries management organisation and have not been reported, or have been misreported, in contravention of the reporting procedures of that organisation;

258. **Food (FSMA-PC Guide):** Includes (1) articles used for food or drink for man or other animals, (2) chewing gum, and (3) articles used for components of any such article and includes raw materials and ingredients.

259. **Food Assurance (Elliott Review):** "… is normally provided by schemes which provide consumers and businesses with guarantees that food has been produced to particular standards. These schemes are mainly voluntary arrangements although many food businesses make certification in an assurance scheme a specification requirement for their suppliers. Examples of assurance schemes are the Red Tractor, which covers production standards, and the British Egg Industry Council lion logo for eggs. These schemes must ensure that communications and claims about them are accurate."

260. **Food Authenticity (CODEX, DRAFT 11/2017):** Food with undisputed origin and genuine in its nature, substance and quality including nutritional values and food preferences expected by the consumer [purchaser] or a food standard or claimed by the food business operator (Under review)

261. **Food Authenticity (Elliott Review):** "… is about ensuring that food offered for sale or sold is of the nature, substance and quality expected by the purchaser (Section 14 Food Safety Act 1990). Authenticity can be a particular issue for faith groups or consumers with particular food preferences who do not want to purchase products containing certain ingredients." (Comment – "authenticity" is not specifically used in the Food Safety Act 1990 Section 14 on consumer protection; "authenticated" is referred to later in the act regarding document confirmation).

262. **Food Authenticity (Webster's Dictionary) –** Food and "genuine, real", "the general quality of being authentic or of established authority for truth and correctness, 2. Genuineness; the quality of being genuine or not corrupted from the original."

263. **Food contamination (Davidson):** Some authors differentiate between contamination (unintentional) and adulteration (intentional) (Lipp, 2014; Manning and Soon, 2016). In this paper we use the terms deliberate or malicious to indicate intentional contamination and natural or accidental to indicate unintentional contamination and have chosen not to use adulteration to avoid confusion

264. **Food Crime (0 - General):** of (1) incidents involving food that is a violation of a criminal statute or (2) Food Fraud incidents that are conducted on a larger scale."

265. **Food Crime (Comment from Reviewer):** "It is unclear what [the details of the definition] means. Does a "large scale" act that doesn't violate a criminal law count? -- More generally, what about civil violations? [A soda drink], made with corn syrup, claims it is "natural" - a word not defined by the FDA. Many people sue (rightly). It should be fraud but is excluded by our definition which narrowly focuses on crimes (punishable by imprisonment) when there are many other types of deception and misrepresentation."

266. **Food Crime (Comment from Reviewer):** "The definition of food crime makes reference to criminal statute, and 'larger scale'. Food fraud could be committed and never proven to a criminal standard, but could meet the UK civil test for fraud. In the UK criminal evidence must be beyond reasonable doubt, while civil is to a lower standard generally considered to be on the balance of probabilities. As such, food fraud may occur which would not pass the test of food crime. The consequence is the sanction, not the methods necessary to prevent the fraud from occurring in the first place. The inclusion of 'larger scale' is problematic as I am not aware the scale is defined anywhere."

267. **Food crime (Davidson):** Elliot (2014) defined food crime as being an organised activity by larger groups aimed at deceiving or injuring consumer via food products. In this paper we use a broader definition to include any nefarious activity, within the food supply chain, perpetrated by groups or single individuals, whose motivations can vary from personal revenge to financial gain, by indirectly inflicting losses to a food company or product, through deceiving, and or injuring those purchasing a

food product or by extortion, such as hoax threats (Knechtges, 2012). Economically motivated contamination would fall in this category, for example. Food terrorism is a type of food crime however the motivation is ideological rather the financial or personal Food fraud EU legislation does not define food fraud but fraudulent practices have an "intent to deceive" as well as resulting in financial benefits (EU, 2013, 2016).

268. **Food Crime (Elliott Review):** "Food fraud becomes **food crime** when it no longer involves a few random acts by 'rogues' within the food industry but becomes an organised activity perpetrated by groups who knowingly set out to deceive and or injure those purchasing a food product." (Comment- original definition created for this report.)

269. **Food Crime (Huisman): "…**this has two commons definitions of (1) incidents involving food that is a violation of a criminal statute (Manning and Soon 2016) and (2) Food Fraud incidents that are conducted on a larger scale (FBI 2012, UK NFCU 2016)." (Huisman, VanRuth, et. al. 2017) –

270. **Food defence (Davidson):** Some authors use this to indicate ideologically motivated incidents of malicious food adulteration (Manning and Soon, 2016; GFSI, 2014) whereas other use a broader definition to include other protection activities (BRC, 2015). In this paper food defence is defined as the methodology and countermeasures taken to prevent and mitigate the effects of intentional incidents and threats to the food chain. The type of threat that can be addressed by food defence practices can range from food crime, food fraud, tampering and food terrorism

271. **Food Defence (food defense) (GFSI Position Paper, 2014, in text):** which protects against tampering with intent to harm –

272. **Food defence (GFSI v7.2, Glossary):** The process to ensure the security of food and drink from all forms of intentional malicious attack including ideologically motivated attack leading to contamination.

273. **Food Defence / Food Defense (GFSI):** The process to ensure the security of food and drink and their supply chains from all forms of intentional malicious attack including ideologically motivated attack leading to contamination or supply failure.

274. **Food defence plan (GFSI v7.2, in text):** The standard shall require that the organisation has a documented plan in place that specifies the measures the organisation has implemented to mitigate the public health risks from any identified food defence threats.

275. **Food defence threat assessment (GFSI v7.2, in text):** The standard shall require that the organisation have a documented food defence threat assessment procedure in place to identify potential threats and prioritise food defence measures

276. **Food Defense (0 Summary):** Comment - is defined as intentional attacks on the food supply chain

277. **Food Defense (Comment from Reviewer):** Note: "Food defense is not the attacks themselves, but the protection against potential attacks." And "No. FD are the collective activities that are intended to reduce the likelihood that an IA event will occur."

278. **Food Defense (FDA, Pre-FSMA, 2009): "**the efforts to prevent intentional contamination of food products (Human intervention as the source of contamination)"

279. **Food Defense (food defense) (IFS):** The protection of food products from intentional contamination or adulteration by biological, chemical, physical, or radiological agents for the purpose of causing harm.

280. **Food defense (food defense) (IFS):** The protection of food products from intentional contamination or adulteration by biological, chemical, physical, or radiological agents for the purpose of causing harm.

281. **Food Defense (FPDI/NCFPD, 2018)**: "the sum of actions related to prevention, protection, mitigation, response, and recovery of the food system from intentional acts of adulteration"

282. **Food Defense (FSMA-IA, 2011):** Food Defense as defined by the IA rule only includes "wide scale [human] health harm" – or essentially the health hazards from food terrorism.
283. **Food Defense (FSSC):** The process to prevent food and feed supply chains from all forms of ideologically or behaviorally motivated, intentional adulteration that might impact consumer health.
284. **Food Defense (FSSC):** The process to prevent food and feed supply chains from all forms of ideologically or behaviourally motivated, intentional adulteration that might impact consumer health.
285. **Food Defense (SQF):** As defined by the US Food and Drug administration, the efforts to prevent intentional food contamination by biological, physical, chemical or radiological hazards that are not reasonably likely to occur in the food supply.
286. **Food Defense (SQF):** As defined by the US Food and Drug administration, the efforts to prevent intentional food contamination by biological, physical, chemical or radiological hazards that are not reasonably likely to occur in the food supply.
287. **Food Defense (USP referring to GCC/SCC referring to FDA FD): "** Food defense is the protection of food products from intentional contamination or adulteration where there is an intent to cause public health harm and/or economic disruption.4" (citing: Food Defense Fact Sheet, June2016, Food & Agriculture Sector Councils, which cites the main FDA Food Defense website that narrows to "wide-scale public health harm") (USP non-Targeted Methods report)
288. **Food Fraud (0 Summary):** Comment - intentional deception of food or food ingredients for economic food, includes all types of fraud (e.g., not only adulterant-substances and counterfeits to include stolen and some diverted goods) and all products (e.g., raw materials and finished goods). (Journal of Food Science, Elliott Review, FSA UK, Book on Food Safety in China, ISO, CODEX CCFICS EWG, GFSI, etc.)
289. **Food fraud (Avery):** There is currently no EU definition of the term, but it is generally accepted that food fraud is an intentional action carried out for financial gain. Different types of food fraud include adulteration, counterfeiting, substitution and deliberate mislabelling of goods.
290. **Food fraud (CEN):** Intentionally causing a mismatch between food product claims and actual food product characteristics, either by deliberately making claims known to be false or by deliberately omitting to make claims that should have been made; Note 1 to entry: Financial gain is the most common motivation for food fraud, but there might also be other reasons; bioterrorism is one example; Note 2 to entry: An implicit claim for all commercial products is 'this product produced and sold according to the relevant requirements and regulations', and this means that food fraud occurs when some aspect of the production violates the requirements or regulations; not only when an explicit claim is falsified. Examples of this type of food fraud include: When there are production agreements or quotas for the product, and the product in question is deliberately produced in excess of these; When there is a geographical restriction on the sale and distribution of the product, and the product in question is deliberately sold or distributed in other areas; When a legitimate product is stolen and passed off as a legitimately procured product; When an Intellectual Property Rights (IPR) infringement is in effect; this could include any or all aspects of the another product or packaging being fully replicated
291. **Food Fraud (CODEX EWG, DRAFT 11/2017): Comment -** under review, currently defined as all types of fraud and all products; "Any deliberate action taken by businesses or individuals that deceive other businesses and/or individuals in terms of misrepresenting food, food ingredients or food packaging that brings about a financial gain. The main types of fraud include: adulteration (including substitution, dilution, concealment, unapproved enhancement), , tampering, simulation, counterfeiting, and misrepresentation of food, food ingredients or food packaging, product overrun, theft, diversion, and false or misleading statements made about a product."

292. **Food Fraud (Comment from Reviewer):** "An important point, in my opinion, is the inclusion of 'deliberate and intentional'. The test for fraud (in the UK) includes the mens rea (the intention or knowledge of wrongdoing that constitutes part of a crime, as opposed to the action or conduct of the accused.) Without proving deliberate and intentional action (or omission) it is likely fraud (and thus food fraud) would be more likely to prove. It could be reasonably argued that what was first considered a fraud was infact a mistake as it was unintentional (and not reckless)."

293. **Food fraud (Davidson):** can be further divided by the different types of fraudulent acts aimed at deceiving consumers (Avery, 2014; Elliot, 2014; GFSI, 2014; Zhang and Xue, 2016): substitution; artificial enhancement; addition; tampering; and dilution; which together are often grouped under economically motivated deliberate contamination (Everstine et al., 2013); as well as product overrun; misrepresentation which can range from incorrect labelling of ingredients to product simulation and counterfeiting; as well as diversion and theft (Spink and Moyer, 2011)

294. **Food Fraud (Elliott Review, in glossary):** "… is defined by the Food Standards Agency as: deliberately placing food on the market, for financial gain, with the intention of deceiving the consumer. Although there are many kinds of food fraud, the two main types are: Sale of food which is unfit and potentially harmful, such as: -recycling of animal by-products back into the food chain, -packing and selling of beef and poultry with an unknown origin, -knowingly selling goods which are past their 'use by' date. Deliberate mis-description of food such as: -products substituted with a cheaper alternative, for example farmed salmon sold as wild, and Basmati rice adulterated with cheaper varieties. -making false statements about the source of ingredients, i.e. their geographic, plant or animal origin. Food fraud may also involve the sale of meat from animals that have been stolen and/or illegally slaughtered, as well as wild game animals like deer that may have been poached."

295. **Food Fraud (Elliott Review, in text):** "…encompasses deliberate and intentional substitution, addition, tampering, or misrepresentation of food, food ingredients, or food packaging; or false or misleading statements made about a product for economic gain. The types of fraud include adulteration, tampering, product overrun, theft, diversion, simulation, and counterfeiting3." (Note: "3" on Page 12, cites Spink & Moyer, 2011)

296. **Food Fraud (GFSI Position Paper 2014, glossary) (GFSI):** "…is deception of consumers using food products, ingredients and packaging for economic gain and includes substitution, unapproved enhancements, misbranding, counterfeiting, stolen goods or others." (Note: The GFSI Position Paper on Food Fraud is a detailed and expanded explanation of the intent of the GFSI Board of Directors for the GFSI Food Safety Management System.)

297. **Food Fraud (GFSI Position Paper, 2014, in text):** Food fraud, including the subcategory of economically motivated adulteration, is of growing concern. It is deception of consumers using food products, ingredients and packaging for economic gain and includes substitution, unapproved enhancements, misbranding, counterfeiting, stolen goods or others.

298. **Food Fraud (GFSI, Version 7, Glossary, 2017) (GFSI):** "A collective term encompassing the deliberate and intentional substitution, addition, tampering or misrepresentation of food, food ingredients or food packaging, labeling, product information or false or misleading statements made about a product for economic gain that could impact consumer health."

299. **Food Fraud (IFS):** The deliberate and intentional substitution, mislabeling, adulteration or counterfeiting of food, raw materials, ingredients or packaging placed upon the market for economic gain. This definition also applies to outsourced processes.

300. **Food Fraud (SQF):** As defined by Michigan State University, a collective term used to encompass the deliberate and intentional substitution, addition, tampering, or misrepresentation of food, food ingredients, or food packaging; or false or misleading statements made about a product, for economic gain.

301. **Food Fraud Hazard (NA):** no specific definition

302. **Food Fraud Mitigation Plan (GFSI v7.2, in text):** The standard shall require that the organization has a documented plan in place that specifies the measures the organization has implemented to mitigate the public health risks from the identified food fraud vulnerabilities.

303. **Food Fraud Mitigation Plan (IFS):** A process that defines the requirements on when, where and how to mitigate fraudulent activities, identified by a food fraud vulnerability assessment. The resulting plan will define the measures and controls that are required to be in place to effectively mitigate the identified risks. The control measures required to be put into place may vary according to the nature of – the food fraud (substitution, mislabelling, adulteration or counterfeiting) – detection methodology – type of surveillance (inspection, audit, analytical, product certification) – source of the raw material, ingredient and packaging.

304. **Food fraud mitigation plan (prevention strategy) (detail) (GFSI):** The standard shall require that the organization's Food fraud mitigation plan shall be supported by the organisation's Food Safety Management System.

305. **Food fraud mitigation plan (prevention strategy) (GFSI)**: The standard shall require that the organisation has a documented plan in place that specifies the measures the organisation has implemented to mitigate the public health risks from the identified food fraud vulnerabilities.

306. **Food Fraud Prevention (FSSC):** The process to prevent food and feed supply chains from all forms of economically motivated, intentional adulteration that might impact consumer health.

307. **Food Fraud Risk:** "…is the combined likelihood and consequence – that considers the threat and vulnerability – of food fraud. This is a function of the vulnerability and threat; e.g., an estimate of the likelihood and consequence of milk diluted with water, sold to a deceived customer. Following these definitions, it is important to note that there could be a vulnerability assessment, separate from a risk assessment, for food fraud or for food defense (food safety risk is traditionally addressed in a Hazard Analysis and Critical Control Point HACCP plan). (Spink, Ortega, Chen & Wu, 2017))

308. **Food Fraud Threat:** "…is the cause of a food fraud event; e.g., a criminal could dilute milk with water and then sell to a deceived customer. (Spink, Ortega, Chen & Wu, 2017)

309. **Food fraud vulnerability (GFSI v7.2, Glossary):** Susceptibility or exposure to a food fraud risk, which is regarded as a gap or deficiency that could place consumer health at risk if not addressed.

310. **Food Fraud Vulnerability (GFSI, Version 7, glossary, 2017) (GFSI):** "Susceptibility or exposure to a food fraud risk, which is regarded as a gap or deficiency that could place consumer health at risk if not addressed."

311. **Food Fraud Vulnerability Assessment (GFSI Position Paper, 2014, Glossary):** The standard shall require that the organisation have a documented food fraud vulnerability assessment in place to identify potential vulnerability and prioritise food fraud vulnerability control measures. From the text: "in which information is collected at the appropriate points along the supply chain (including raw materials, ingredients, products, packaging) and evaluated to identify and prioritise significant vulnerabilities for food fraud."

312. **Food fraud vulnerability assessment (GFSI v7.2, in text):** The standard shall require that the organisation has a documented food fraud vulnerability assessment procedure in place to identify potential vulnerability and prioritise food fraud mitigation measures.

313. **Food Fraud Vulnerability Assessment (IFS):** A systematic documented form of risk assessment to identify the risk of possible food fraud activity within the supply chain (including all raw materials, ingredients, food, packaging and outsourced processes). The method of risk assessment may vary from company to company, … ."

314. **Food Fraud Vulnerability Control Plan – Scope (GFSI Position Paper, 2014, Glossary):** This plan shall cover the relevant GFSI scope and shall be supported by the organisation's Food Safety Management System.

315. **Food Fraud Vulnerability Control Plan (GFSI Position Paper, 2014, Glossary):** The standard shall require that the organisation have a documented plan in place that specifies the control measures the organisation has implemented to minimize the public health risks from the identified food fraud vulnerabilities.
316. **Food Fraud Vulnerability:** "…is the susceptibility of a system to food fraud (e.g., milk is not tested for adulterants such as water). (Spink, Ortega, Chen & Wu, 2017)
317. **Food Fraud/ Product Fraud (ISO TC292):** Summary: deception utilizing material goods for economic gain or avoiding a loss; "wrongful or criminal deception utilizing 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 creating 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 needs to be considered separately." (ISO/DIS 22380)
318. **Food Integrity (CODEX EWG, DRAFT 11/2017):** Comment – under review; "Food meets acceptable levels of specifications defined as quality including nutritional values, safety and authenticity including label claims."
319. **Food Integrity (EC, FIP, 1):** "the state of being whole, entire, or undiminished or in perfect condition." And *"…* can be seen as ensuring that food which is offered for sale or sold is not only safe and of the nature, substance and quality expected by the purchaser but also captures other aspects of food production, such as the way it has been sourced, procured and distributed and being honest about those elements to consumers."
320. **Food Integrity (EC, FIP, 2):** "the state of being whole, entire, or undiminished or in perfect condition". "Providing assurance to consumers and other stakeholders about the safety, authenticity and quality of European food (integrity) is of prime importance in adding value to the European Agri-food economy. The integrity of European foods is under constant threat from fraudulently labelled imitations that try to exploit that added value." (Comment- this is a definition expanded from the first "EC, FIP, 1" definition.)
321. **Food integrity (Elliott Review):** "… can be seen as ensuring that food which is offered for sale or sold is not only safe and of the nature, substance and quality expected by the purchaser but also captures other aspects of food production, such as the way it has been sourced, procured and distributed and being honest about those elements to consumers." (See Food Integrity, Eight Pillars).
322. **Food integrity (Manning):** Fraud in the food supply chain can arise as a result of misrepresentation associated with (1) **product integrity** (authenticity) - the inherent quality attribute of totality or completeness [2] i.e. intrinsic characteristics; (2) **process integrity** – the activities undertaken to produce the food item encompassing the design, assurance, monitoring and verification of processes within the product life-cycle to ensure that they remain authentic and intact, i.e. extrinsic characteristics; (3) **people integrity** can be described as the honesty and morals exhibited by an individual and/or (4) **data integrity** of information accompanying the food item throughout the supply chain i.e. the consistency and accuracy of data through the food product life-cycle (Manning, 2016) - Manning L. (2016), Food Fraud, policy and food chain, Current Opinions in Food Science, 10, 16-21
323. **Food Integrity (Webster's Dictionary):** Comment- based on combing the definition of both terms: "Food" and "adherence to a code of values, soundness, completeness."
324. **Food Integrity, The Eight Pillars (Elliott Review):** "The Eight Pillars of Food Integrity" which are: (1) The result is a robust system that puts the needs of consumers before all others; (2) adopts a zero tolerance approach to food crime; (3) invests in intelligence gathering and sharing; (4) supports resilient laboratory services that use standardised, validated methodologies; (5) improves the efficiency and quality of audits and more actively investigates and tackles food crime; (6)

acknowledges the key role Government has to play in supporting industry; and (7) reinforces the need for strong leadership and effective crisis management. (Comment- see other Elliott Review definitions including Food Integrity and Food Authenticity.)

325. **Food Quality (Codex):** "Quality includes all the attributes that influence a product's value to the consumer. This includes negative attributes such as spoilage, contamination with filth, discoloration, off-odours and positive attributes such as the origin, colour, flavour, texture and processing method of the food" (FAO 2017).
326. **Food Quality (Manning and Baines):** By separating product and process (production method), quality can be defined in terms of intrinsic quality (quality of the product) and extrinsic quality (systems of production and processing)."
327. **Food Safety (Codex):** "The assurance that food will not cause harm to the consumer when prepared and/or eaten according to its intended use" (FAO 2017) (See Codex Acceptable Levels of Protection ALOP).
328. **Food safety (Davidson):** Ensuring food: safe to eat and free from dangerous levels of harmful infectious and toxic agents (natural and accidental contamination) (EU, 2002)
329. **Food Safety (GFSI): "**A concept that food will not cause harm to the consumer when it is prepared and / or eaten according to its intended use."
330. **Food Safety (GFSI):** A concept that food will not cause harm to the consumer when it is prepared and/or eaten according to its intended use.
331. **Food safety** (ISO 22000): assurance that food will not cause an adverse health effect for the consumer when it is prepared and/or consumed in accordance with its intended use; Note 1 to entry: Food safety is related to the occurrence of **food safety hazards** (3.22) in **end products** (3.15) and does not include other health aspects related to, for example, malnutrition; Note 2 to entry: It is not to be confused with the availability of, and access to, food ("food security"); Note 3 to entry: This includes feed and animal food. [SOURCE: CAC/RCP 1-1969, modified — The word "harm" has been changed to "adverse health effect" and notes to entry have been added.]
332. **Food safety hazard** (ISO 22000): biological, chemical or physical agent in **food** (3.18) with the potential to cause an adverse health effect; Note 1 to entry: The term "hazard" is not to be confused with the term "risk" (3.39) which, in the context of food safety, means a function of the probability of an adverse health effect (e.g. becoming diseased) and the severity of that effect (e.g. death, hospitalization) when exposed to a specified hazard; Note 2 to entry: Food safety hazards include allergens and radiological substances; Note 3 to entry: In the context of feed and feed ingredients, relevant food safety hazards are those that can be present in and/or on feed and feed ingredients and that can through animal consumption of feed be transferred to food and can thus have the potential to cause an adverse health effect for the animal or the human consumer. In the context of operations other than those directly handling feed and food (e.g. producers of packaging materials, disinfectants), relevant food safety hazards are those hazards that can be directly or indirectly transferred to food when used as intended (see 8.5.1.4); Note 4 to entry: In the context of animal food, relevant food safety hazards are those that are hazardous to the animal species for which the food is intended.
333. **Food Safety Management System (GFSI v7.2, Glossary):** A series of defined rules, policies and procedures which are intended to ensure the safe supply of food and protect public health.
334. **Food Safety Management System, FSMS (GFSI):** A series of defined rules, policies and procedures which are intended to ensure the safe supply of food and protect public health.
335. **Food safety plan (FSMA-PC Guide):** A set of written documents that is based upon food safety principles and incorporates hazard analysis, preventive controls, and delineates monitoring, corrective action, and verification procedures to be followed, including a recall plan.

336. **Food Safety Scheme (GFSI):** A systematic plan which has been developed, implemented, and maintained for the scope of food safety. This shall consist of a standard and food safety system in relation to specified processes or a food safety service to which the same particular plan applies. The food safety scheme should contain at least the following items: a standard, clearly defined scope, and a food safety system
337. **Food Safety Standard (GFSI):** A series of defined requirements developed to ensure the safety of food when effectively implemented.
338. **Food Safety System (FSMA-PC Guide):** The result of the implementation of the Food Safety Plan.
339. **Food Safety System (GFSI v7.2, Glossary):** A series of defined rules, policies and procedures which are intended to ensure the safe supply of food and protect public health.
340. **Food Safety System (GFSI):** A series of defined rules, policies and procedures which are intended to ensure the safe supply of food and protect public health.
341. **Food security (Davidson):** Ensuring the availability and accessibility of nutritious food, for all people at all times to live a healthy life (Gross et al., 2000). This means that there is sufficient food at regional and national levels, households have access to this food (i.e. it is affordable) and at an individual level there is nutritional adequacy (EU, 2008)
342. **Food Security (WHO):** the access to safe, continuous, nutritious, and economic supply of food (WHO 2009)
343. **Food Standards (Elliott Review):** "…covers the requirement that food must be correctly and accurately labelled, that it contains legal ingredients and that any claims made are truthful. Food standards legislation sets out specific requirements for the labelling, composition and, where appropriate, safety parameters for specific high value foodstuffs which are potentially at risk of being misleadingly substituted with lower quality alternatives."
344. **Food Supply Chain (GFSI v7.2, Glossary):** A defined sequence of activities in relation to the provision of food and feed from primary production to consumption. In relation to GFSI this involves activities associated with the Food and Feed Industries.
345. **Food supply chain integrity (Davidson):** Multifaceted framework includes food safety, security, defence, traceability, authenticity, ethics and product information, including labelling, throughout the food supply chain (from farm to fork) (Elliot, 2014) Threats to food supply chain Food adulteration Natural, accidental or intentional process whereby any foreign substance, with potential human health implications, originates or is introduced into the food (Saxowsky, 2015)
346. **Food Terrorism (Bio-terrorism)**: See bio-terrorism.
347. **Food terrorism (Davidson):** An act or threat of deliberate contamination of food for human consumption with chemical, biological or radiological or nuclear agents for the purpose of causing injury or death to civilian populations and/or disruption of social, economic or political stability (Karaca, 2012; WHO, 2002). The perpetrator has ideological or political motivations behind the attack/threat of attack rather than personal or financial motivations (Carus, 2001)
348. **Food Terrorism** (WHO): "an act or threat of deliberate contamination of food for human consumption with chemical, biological or radionuclear agents for the purpose of causing injury or death to civilian populations and/or disrupting social, economic or political stability" (WHO 2002)."(Comment- Since the definition was published in 2002 the WHO website has two mentions of the use of the term.)
349. **Forensic** (ISO 22380): related to, or used in, courts of law; Note 1 to entry: This applies to video-surveillance used to produce legal evidence.
350. **Forensic analysis (ISO 22300):** scientific methodology for authenticating material goods (3.139) by confirming an authentication element (3.17) or an intrinsic attribute through the use of specialized equipment by a skilled expert with special knowledge

351. **Forensic analysis (ISO 22380):** scientific methodology for authenticating **material goods** (3.139) by confirming an **authentication element** (3.17) or an intrinsic attribute through the use of specialized equipment by a skilled expert with special knowledge
352. **Fraud (Black's Law):** 1. A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment. Fraud is usually a tort but in some cases (especially when the conduct is willful) it may be a crime. <– also termed "intentional fraud."> 2. A misrepresentation made recklessly without belief in its truth to induce another person to act. 3. A tort arising from a knowing misrepresentation, concealment or material fact, or reckless misrepresentation made to induce another to act to his or her detriment. 4. Unconsciable dealing; especially, in contract law, the unfair use of the power arising out of the parties' relative positions and resulting in an unconscionable bargain.
353. **Fraud (GAO Green):** Involves obtaining something of value through willful misrepresentation (paragraph 8.02)
354. **Fraud, Criminal (Black's Law):** fraud that has been made illegal by statute and that subjects the offender to criminal penalties such as fines and imprisonment. An example is the willful evasion of taxes accomplished by filing a fraudulent tax return.
355. **Fraud, Extrinsic (Black's Law):** 1. Deception that is collateral to the issues being considered in the case; intentional misrepresentation or deceptive behavior outside the transaction itself (whether a contract or a lawsuit), depriving one party of informed consent or full participation. For example, a person might engage in extrinsic fraud by convincing a litigant not to hire counsel or answer by dishonestly saying the matter will not be pursued. – Also termed "collateral fraud." 2. Deception that prevents a person from knowing about or asserting certain rights.
356. **Fraud, Intrinsic (Black's Law):** deception that pertains to an issue involved in an original action. Examples include the use of fabricated evidence, a false return of service, perjured testimony, and false receipts or other commercial documents.
357. **Fraude (Black's Law):** [French] Civil law. Fraud committed in performing of a contract. (Comment- this is an example of the challenge of translating terms since the French word "fraude" has a different definition that the English word with similar spelling "fraud.")
358. **Fraudfeasor (Black's Law):** A person who has committed fraud. – Also termed "defrauder."
359. **Fraudulent Act (Black's Law):** Conduct involving bad faith, dishonesty, a lack of integrity, or moral turpitude. – Also termed "dishonest act;" "fraudulent or dishonest act."
360. **Frequency (DHS Lexicon 2017):** number of occurrences of an event per defined period of time or number of trials
361. **FSMA Preventive Controls for Human Foods Qualified Individual Training (PCHF-QI):** the officially recognized FSMA Qualified Individual training managed by the Food Safety Preventive Controls Alliance (FSPCA). FSMA-PC requires that a PCHF-QI develop and manage the Preventive Controls aspect of FSMA.
362. **General controls (GAO Green):** The policies and procedures that apply to all or a large segment of an entity's information systems; general controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning (paragraph 11.07)
363. **Geographical Indication, Trademark (TRIPs):** This is a type of trademark where "indications which identify a good as originating in the territory of a Member, or a region or locality in that territory, where a given quality, reputation or other characteristic of the good is essentially attributable to its geographical origin" (REF TRIPS). There are specific details addressing "Additional Protection for Geographical Indications for Wines and Spirits."
364. **Geo-location, Geographic Location** (ISO 22380): specific location defined by one of several means to represent latitude, longitude, elevation above sea level and coordinate system; Note 1 to

entry: Geo-location generally means the meaningful specification of the position of a point or **object** (3.151) on the earth. The term itself does not carry a prescription of the coordinate system to be used. Additional attributes associated with a geo-location are not a part of a geo-location specification.

365. **Goods (ISO 22300):** items or materials that, upon the placement of a purchase order, are manufactured, handled, processed or transported within the supply chain (3.251) for usage or consumption by the purchaser

366. **Gray Market (Black's law):** A market in which the seller uses legal but sometimes unethical methods to avoid a manufacturer's distribution chain and thereby sell goods (especially imported goods) at prices lower than those envisions by the manufacturer. See "Parallel Imports."

367. **Gray-Market Goods (Black's law):** See "Parallel Imports."

368. **HACCP - Hazard Analysis and Critical Control Point plan (GFSI):** Hazard Analysis and Critical Control Point, A system which identifies, evaluates controls and monitors hazards relating to food safety and specified by Codex Alimentarius or the National Advisory Committee on Microbiological Criteria for Foods.

369. **HACCP (Hazard Analysis and Critical Control Point) (FSMA-PC Guide):** A system which identifies, evaluates, and controls hazards that are significant for food safety.

370. **HACCP Hazard Analysis and Critical Control Point (GFSI v7.2, Glossary):** A system which identifies, evaluates, controls, and monitors hazards relating to food safety and specified by Codex Alimentarius or the National Advisory Committee on Microbiological Criteria for Foods.

371. **Harmonization (DNI):** With respect to standards (DNI): activities undertaken by communities of experts to align standards. For example, to define common metadata and application schema from legacy sources, harmonization will consider: -- Architecture - multiple viewpoints that capture high-level requirements, use cases, scenarios, information flows and computational flows. -- Data modelling - definition and UML encoding of feature type, attribute type, data type, coding, dependency mapping -- Schema modelling - UML mapping and encoding to GML, mapping of profiles to one another, and delineation to service types -- Iteration and development - build a little, see if it works, build more -- Delivery to standards organizations for approval.

372. **Harmonized Standards (DNI):** Equivalent standards. Standards on the same subject approved by different standardizing bodies, that establish interchangeability of products, processes and services, or mutual understanding of test results or information provided according to these standards. NOTE: Within this definition, harmonized standards might have differences in presentation and even in substance, e.g. in explanatory notes, guidance on how to fulfill the requirements of the standard, preferences for alternatives and varieties.

373. **Hazard (DHS Lexicon 2017):** natural or man-made source or cause of harm or difficulty

374. **Hazard (EFSA):** something that has the potential to harm you; e.g. a shark in the sea while you are on land, e.g. lightning when you are in a house

375. **Hazard (EU178/2002):** means a biological, chemical or physical agent in, or condition of, food or feed with the potential to cause an adverse health effect;

376. **Hazard (FDA, FSMA, CFR):** Hazard means any biological, chemical (including radiological), or physical agent that has the potential to cause illness or injury. (21CFR117.3)

377. **Hazard (FSMA-PC Guide):** Any biological, chemical (including radiological), or physical agent that has the potential to cause illness or injury.

378. **Hazard (FSMA-PC/ FDA):** A hazard is an agent that is reasonably likely to cause illness or injury in the absence of its control (§ 117.3); The facility must consider factors associated with risk (i.e., the severity of the illness or injury if the hazard were to occur and the probability that the hazard will occur in the absence of preventive controls) in evaluating whether any potential hazard is a hazard requiring a preventive control (§ 117.130(c)).

379. **Hazard** (ISO 22380): source of potential harm; Note 1 to entry: Hazard can be a **risk source** (3.213).
380. **Hazard (US GOVT.):** "…is an event that has not occurred and could cause harm if not addressed (ISO 2007b, PAS 96 2014, NRC 1996, 21 CFR, Merriam-Webster 2004) – this includes damaging potential (ISO 2007b). For food this is often applied to unintentional events that have potential to harm." (Spink, Ortega, Chen & Wu, 2017)
381. **Hazard Analysis (FSMA CFR):** "(a) (1) you must conduct a hazard analysis to identify and evaluate… known or reasonably foreseeable hazards…" including"(2) The hazard analysis must be written **regardless of its outcome**; (iii) The hazard may be intentionally introduced for purposes of **economic gain**."
382. **Hazard analysis (FSMA-PC Guide):** The process of collecting and evaluating information on hazards and conditions leading to their presence to decide which should be addressed through a preventive control.
383. **Hazard monitoring function** (ISO 22380): **activities** (3.1) to obtain evidence-based **information** (3.116) on **hazards** (3.99) in a defined area used to make decisions about the need for **public warning** (3.183)
384. **Hazard requiring a preventive control (FSMA-PC Guide):** A known or reasonably foreseeable hazard for which a person knowledgeable about the safe manufacturing, processing, packing, or holding of food would, based on the outcome of a hazard analysis (which includes the severity of the illness or injury if the hazard were to occur and the probability that the hazard will occur in the absence of preventive controls) establish one or more preventive controls to significantly minimize or prevent the hazard in a food and components to manage those controls (such as monitoring, corrections or corrective actions, verification and records) as appropriate to the food, the facility and the nature of the preventive control and its role in the facility's food safety system.
385. **Hazard that requires a preventive control (FDA, FSMA, US CODE): Section 218, (C)** Preventive Controls. —The owner, operator, or agent in charge of a facility shall identify and implement preventive controls, including at critical control points, if any, to provide assurances that— '(1) hazards identified in the hazard analysis conducted under subsection (b)(1) will be significantly minimized or prevented;
386. **Homogeneity** ((ISO Guide 30): uniformity of a specified property value throughout a defined portion of a reference material (RM); Note 1 to entry: Tests for homogeneity are described in ISO Guide 35; Note 2 to entry: The 'defined portion' may be, for example, an RM batch or a single unit within the batch; Note 3 to entry: See also IUPAC Compendium of Analytical Nomenclature.[5]
387. **Human interpretation** (ISO 22380): authenticity as evaluated by an **inspector** (3.120)
388. **Identification (DNI):** 1) The process, generally employing unique machine-readable names, that enables recognition of users or resources as identical to those previously described to the computer system. 2) The assignment of a name by which an entity can be referenced. The entity may be high level (such as a user) or low level (such as a process or communication channel.
389. **Identification** (ISO 22380): **process** (3.180) of recognizing the attributes that identify an **entity** (3.79),
390. **Identifier** (ISO 22380): specified set of attributes assigned to an **entity** (3.79) for the purpose of **identification** (3.104)
391. **Identity (Black's law):** In the law of evidence. Sameness; the fact that a subject, person, or thing before a court is the same as it is represented, claimed, or charged to be.
392. **Identity (DNI):** The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.

393. **Identity** (ISO 22380): set of attributes that are related to an **entity** (3.79); Note 1 to entry: An identity can have unique attributes that enable an **object** (3.151) to be distinguished from all others; Note 2 to entry: Identity can be viewed in terms of human, **organization** (3.158) and objects (physical and intangible).
394. **Illegal (Black's law):** Not authorized by law; Illicit; unlawful; contrary to law. Sometimes this term means merely that which lacks authority of or support from law; but more frequently it imports a violation. Illicit (Black's law): Not permitted or allowed; prohibited ; unlawful; as an illicit trade
395. **Illegitimate product (DSCSA):** The term `illegitimate product' means a product for which credible evidence shows that the product: (A) is counterfeit, diverted, or stolen; (B) is intentionally adulterated such that the product would result in serious adverse health consequences or death to humans; (C) is the subject of a fraudulent transaction; or (D) appears otherwise unfit for distribution such that the product would be reasonably likely to result in serious adverse health consequences or death to humans.
396. **Illicit trade (Black's law):** This term applies to any trade with a country that has been forbidden by a law.
397. **Imitation (Black's law):** The making of one thing in the similitude or likeness of another; as, counterfeit coin is said to be made "in imitation" of the genuine. An imitation of a trade-mark is that which so far resembles the genuine trade-mark as to be likely to induce the belief that it is genuine, whether by the use of words or letters similar in appearance or in sound, or by any sign, device, or other means. (See simulation)
398. **Impact** (ISO 22380): evaluated **consequence** (3.46) of a particular outcome
399. **Impact analysis**, **consequence analysis** (ISO 22380): **process** (3.180) of analysing all operational functions and the effect that an operational interruption can have upon them; Note 1 to entry: Impact analysis is part of the **risk assessment** (3.203) process and includes **business impact analysis** (3.29). Impact analysis identifies how the loss or damage will manifest itself; the degree for potential escalation of damage or loss with time following an **incident** (3.111); the minimum services and resources (human, physical, and financial) needed to enable business processes to continue to operate at a minimum acceptable level; and the timeframe and extent within which **activities** (3.1), functions and services of the organization should be recovered.
400. **Impartiality** (ISO 22380): actual or perceived presence of objectivity; Note 1 to entry: Objectivity means that conflicts of interest do not exist or are resolved so as not to adversely influence subsequent activities.; Note 2 to entry: Other terms commonly used to convey the element of impartiality are objectivity, independence, freedom from conflict of interests, freedom from bias, lack of prejudice, neutrality, fairness, open-mindedness, even-handedness, detachment and balance.
401. **Import (Black's law):** Importations; goods or other property imported or brought into the country from a foreign country. Also: Importation: The act of bringing goods and merchandise into a country from a foreign country.
402. **Improvisation** (ISO 22380): act of inventing, composing or performing, with little or no preparation, a reaction to the unexpected
403. **Incident (0 Summary):** "A type of event… that has occurred and evaluated and that could have a negative consequence (DHS 2008, ANSI 2009, CNSSI 2010). " (Spink, Ortega, Chen & Wu, 2017)
404. **Incident (Black's law):** This word, used as a noun, denotes anything which inseparably belongs to, or is connected with, or inherent in, another thing, called the "principal." In this sense, a court-baron is incident to a manor. Also, less strictly, it denotes anything which is usually connected with another, or connected for some purposes, though not inseparably.

405. **Incident (DNI):** An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
406. **Incident** (ISO 22380): situation that can be, or could lead to, a **disruption** (3.70), loss, **emergency** (3.77) or **crisis** (3.59)
407. **Indicative value, information value, informative value** (ISO Guide 30): <of a reference material (RM)> value of a quantity or property, of a reference material, which is provided for information only; Note 1 to entry: An indicative value cannot be used as a reference in a metrological traceability chain
408. **Industrial Design, Patent** (TRIPs)**:** "The owner of a protected industrial design shall have the right to prevent third parties not having the owner's consent from making, selling or importing articles bearing or embodying a design which is a copy, or substantially a copy, of the protected design, when such acts are undertaken for commercial purposes" (REF TRIPS).
409. **Information (DNI):** Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
410. **Information** (ISO 22380): data processed, organized and correlated to produce meaning
411. **Information Assurance, IA (DNI):** Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
412. **Information Leakage (DNI):** An application or protocol weakness where controlled data is inappropriately revealed to an unauthorized user or service.
413. **Information Management, IM (DNI):** The discipline that analyzes information as an organizational resource. It covers the definitions, uses, value and distribution of all data and information within an organization whether processed by computer or not. It evaluates the kinds of data/information an organization requires in order to function and progress effectively
414. **Information Needs (DNI):** A condition or situation requiring knowledge or intelligence derived from received, stored, or processed facts and data.
415. **Information Security Risk (DNI):** Potential that a threat will exploit a vulnerability of an information asset or group of assets and thereby cause harm to the organization.
416. **Infrastructure** (ISO 22380): system of **facilities** (3.90), equipment and services needed for the operation of an **organization**(3.158)
417. **Infringement, Criminal (Black's law):** The statutory criminal offense of either (1) willfully infringing a copyright to obtain a commercial advantage or financial gain, or (2) trafficking in goods or services that bears a counterfeit mark.
418. **Infringement, Innocent (Black's Law):** The act of violating an intellectual-property right without knowledge or awareness that the act constitutes infringement.
419. **Infringement, Intellectual property (Black's law):** An act that interferes with one of the exclusive rights of a patent, copyright, or trademark owner.
420. **Infringement, Trademark (Black's Law):** The unauthorized use of a trademark – or of a confusingly similar name, word, symbol, or any combination of these – in connection with the same or related goods or services and in a manner about the source of goods or services.
421. **Infringement, Vicarious (Black's law):** A person's liability for an infringing act of someone else, even though the person has not directly committed an act of infringement.
422. **Ingredient (GFSI v7.2, Glossary):** A component of a food, feed or packaging that has undergone processing.

423. **Ingredient (GFSI):** A component of a food, feed or packaging that has undergone processing
424. **Inherent risk (COSO/ERM):** the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.
425. **Inherently dangerous property** (ISO 22380): property that, if in the hands of an unauthorized individual, would create an imminent **threat** (3.259) of death or serious bodily harm; EXAMPLE: Lethal weapons, ammunition, explosives, chemical agents, biological agents and toxins, nuclear or radiological materials.
426. **Inject** (ISO 22380): scripted piece of **information** (3.116) inserted into an **exercise** (3.83) that is designed to elicit a response or decision and facilitate the flow of the exercise; Note 1 to entry: Injects can be written, oral, televised and/or transmitted via any means (e.g. phone, email, fax, voice, radio or sign).
427. **Inspection (Black's law):** The examination or testing of food, fluids, or other articles made subject by law to such examination, to ascertain their fitness for use or commerce. … Also the examination by a private person of public records and documents; or of the books and papers of his opponent in an action, for the purpose of better preparing his own case for trial.
428. **Inspector** (ISO 22380): person who uses the **object examination function** (3.152) with the aim of evaluating an **object**(3.151); Note 1 to entry: Any **participant** (3.163) within an identification and authentication system can act as an inspector; Note 2 to entry: Inspectors can have different levels of qualification and **training** (3.265); Note 3 to entry: The inspector can be an automated system.
429. **Inspector access history** (ISO 22380): access logs detailing when unique identifiers (UID) (3.269) were checked, optionally by which (privileged) **inspector** (3.120), and optionally from what specific location; Note 1 to entry: Time stamps are often used.
430. **Integrated authentication element** (ISO 22380): **authentication element** (3.17) that is added to the **material good** (3.139)
431. **Integrated frameworks (COSO/ERM):** Are defined as interconnectivity of internal controls to coordinate operations as well as provide an overall monitoring and calibrating system.
432. **Integrity - Data Integrity (DNI):** The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.
433. **Integrity - System Integrity (DNI):** Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
434. **Integrity (Black's law):** As occasionally used in statutes prescribing the qualifications of public officers, trustees, etc., this term means soundness of moral principle and character, as shown by one person dealing with others in the making and performance of contracts, and fidelity and honesty in the discharge of trusts; it is synonymous with "probity," "honesty," and "uprightness."
435. **Integrity (DNI):** The property whereby an entity has not been modified in an unauthorized manner.
436. **Integrity (ISO 22300):** property of safeguarding the accuracy and completeness of assets (3.10)
437. **Integrity (NIST2):** guarding against improper data modification or destruction, and includes ensuring data nonrepudiation and authenticity;
438. **Integrity (NIST3):** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
439. **Integrity Program (IFS):** Program implemented by IFS in order to: – Monitor, as preventive actions performance of auditors and certification bodies as well as audited companies, – Manage, as corrective actions, any complaints addressed to IFS.
440. **Integrity, Product (ISO TC292):** Summary: The statement of the unimpaired, unaltered, and unmodified condition of the item with safekeeping of the accuracy, completeness of the claim; "property that data has not been modified or deleted in an unauthorized and undetected manner"

(ISO/IEC 19790:2012), "probability of a system satisfactorily performing the required function under all the stated conditions within a stated period"(ISO 10418:2003), "state of an artefact that has not been altered, deliberately or accidentally" (ISO 18308:2011), "property of safeguarding the accuracy and completeness of assets" (ISO 28002:2011), "the property of the unimpaired condition of the authentication element, the associated data, the information or the elements and the means for processing them" (ISO 28002:2011), "attribute of a document whose content is completed and unaltered", "physical acceptability of a [product] to meet the specification designated by the [product] supplier"; [Comment- Note: Usually presented with an evaluation of a meeting requirements (e.g., safety integrity level); Note: only one result mentioned ethical or personal value, e.g., "adherence to ethical principles" (ISO 20121:2012)].

441. **Intellectual Property (Black's law):** 1. a category of intangible rights protecting commercially valuable products of the human intellect. The category comprises primarily trademark, copyright, and patent rights, but also includes trade-secret rights, publicity rights, moral rights, and rights against unfair competition. 2. A commercially valuable product of the human intellect, in a concrete or abstract form, such as a copyrightable work, a protected trademark, a patentable invention, or a trade secret.
442. **Intellectual property rights, IPR (WTO):** Ownership of ideas, including literary and artistic works (protected by copyright), inventions (protected by patents), signs for distinguishing goods of an enterprise (protected by trademarks) and other elements of industrial property.
443. **Intellectual Property, IP (DNI):** Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract "properties" has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered.
444. **Intelligence Community, IC (DNI):** A federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.
445. **Intentional (Black's law):** This means a thing is done with reason and purpose.
446. **Intentional Adulteration (0 Summary): "…** any adulterant-substance intentionally added to the food or ingredient for any reason. (Comment- when applied to Food Defense, **intentional contamination** is a misnomer if using the Codex definition of contaminant (unintentional excess substance that is common in the processing or manufacturing) (Codex Alimentarius 2014).")
447. **Intentional Adulteration (Adapted from Black's law):** Comment- this combines the definitions for each term: "with reason and purpose," "mixing up with food or drink intended to be sold other matters of an inferior quality, and usually of a more or less deleterious quality."
448. **Intentional Adulteration (FDA, FSMA, IA Rule):** The purpose of this rule is to protect food from intentional acts of adulteration where there is an intent to cause wide scale public health harm. …and that the food is at high risk of intentional adulteration caused by acts of terrorism under section 420 of the FD&C Act.
449. **Intentional Adulteration (FDA, FSMA, US CODE):** no direct definition or glossary term
450. **Intentional Adulteration (FDCA 1938):** the words and phrase defined by the US Food, Drug& Cosmetics Act of 1938, specifically the Adulterated Foods section
451. **Intentional Adulteration (FSMA):** no direct definition or glossary term; general text includes "…is wide-scale human health harm scope in the FSMA-IA rule; Section 418, (b) Hazard Analysis. (2) identify and evaluate hazards that may be intentionally introduced, including by acts of terrorism;"
452. **Intentional Adulteration, Protection Against (FDA, FSMA, US CODE):** "'(1) IN GENERAL.—The Secretary shall— ''(A) conduct a vulnerability assessment of the food system, including by consideration of the Department of Homeland Security biological, chemical, radiological, or other

terrorism risk assessments; ‘‘(B) consider the best available understanding of uncertainties, risks, costs, and benefits associated with guarding against intentional adulteration of food at vulnerable points; and ‘‘(C) determine the types of science-based mitigation strategies or measures that are necessary to protect against the intentional adulteration of food.

453. **Interdiction (DNI):** Impeding or denying someone the use of system resources.

454. **Interested party, stakeholder** (ISO 22380): person or **organization** (3.158) that can affect, be affected by, or perceive itself to be affected by a decision or **activity** (3.1); EXAMPLE: Customers, **owners** (3.162), people in an organization, providers, bankers, regulators, unions, partners or society that can include competitors or opposing pressure groups; Note 1 to entry: A decision maker can be an interested party; Note 2 to entry: Impacted communities and local populations are considered to be external interested parties; Note 3 to entry: Throughout this document, the use of the term “interested party” is consistent with its usage in **security operations** (3.232).

455. Interlaboratory comparison, interlaboratory study, interlaboratory test, collaborative study (ISO Guide 30): <of a reference material (RM)> organization, performance and evaluation of measurements or tests on the same or similar items by two or more laboratories in accordance with predetermined conditions; Note 1 to entry: See also “interlaboratory test” in the IUPAC Compendium of Analytical Nomenclature[5];Note 2 to entry: See also the Codex Alimentarius Commission Procedural Manual.[9];

456. **Internal attack** (ISO 22380): **attack** (3.11) perpetrated by people or entities directly or indirectly linked with the legitimate manufacturer, originator of the **goods** (3.98) or **rights holder** (3.198) (staff of the rights holder, subcontractor, supplier, etc.)

457. **Internal audit** (ISO 22380): **audit** (3.13) conducted by, or on behalf of, an **organization** (3.158) itself for **management**(3.135)**review** (3.197) and other internal purposes, and which can form the basis for an organization’s self-declaration of **conformity** (3.45); Note 1 to entry: In many cases, particularly in smaller organizations, independence can be demonstrated by the freedom from responsibility for the **activity** (3.1) being audited.

458. **Internal control (GAO Green):** A process effected by an entity’s oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved (paragraph OV1.01)

459. **Internal control system (GAO Green):** A continuous built-in component of operations, effected by people, that provides reasonable assurance—not absolute assurance—that an entity’s objectives will be achieved (paragraph OV1.04)

460. **Internal control system (GAO Green):** A continuous built-in component of operations, effected by people, that provides reasonable assurance—not absolute assurance—that an entity’s objectives will be achieved (paragraph OV1.04)

461. **Internal Controls (COSO/ERM):** A process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effective and efficiency of operations, reliability in financial reporting, and compliance with applicable laws and regulations. An internal control system is a synonym for internal controls applied in an entity.”

462. **International supply chain** (ISO 22380): **supply chain** (3.251) that at some point crosses an international or economic border; Note 1 to entry: All portions of this chain are considered international from the time a purchase order is concluded to the point where the **goods** (3.98) are released from customs control in the destination country or economy; Note 2 to entry: If treaties or regional agreements have eliminated customs clearance of goods from specified countries or economies, the end of the international supply chain is the port of entry into the destination country

or economy where the goods would have cleared customs if the agreements or treaties had not been in place.

463. **Interoperability (DNI):** The ability of systems, units or forces to provide data, information, materiel and services to and accept the same from other systems, units or forces and to use the data, information, materiel and services so exchanged to enable them to operate effectively together. … Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the lifecycle and must be balanced with IA.

464. **Interoperability** (ISO 22380): ability of diverse systems and **organizations** (3.158) to work together

465. **Interoperability (NIST2):** The capability to communicate, to execute programs, or to transfer data among various functional units under specified conditions.

466. **Intrinsic authentication element (ISO 12931):** authentication element which is inherent to the material good, e.g., an attribute of a food such as a DNA test, ionization of water, etc.

467. **Intrinsic authentication element** (ISO 22380): **authentication element** (3.17) which is inherent to the **material good** (3.139)

468. **Intrusion Detection (DNI):** The process of monitoring the events occurring in a computer system or network, detecting signs of security problems.

469. **Intrusion Detection System, IDS (DNI):** A technical security system designed to detect an attempted or actual unauthorized entry into a secure facility or information system and alert responders.

470. **Invocation** (ISO 22380): act of declaring that an **organization's** (3.158)**business continuity** (3.24) arrangements need to be put into effect in order to continue delivery of key **products or services** (3.181)

471. **ISO/IEC 17011:2004 (GFSI):** An International Standards Organization recognized and final standard 17011 on "Conformity assessment -- General Requirements" for accreditation bodies accrediting conformity assessment bodies that was last updated in 2004 (ISO 2004)

472. **Key performance indicator, KPI** (ISO 22380): quantifiable measure that an **organization** (3.158) uses to gauge or compare **performance** (3.167) in terms of meeting its strategic and operational **objectives** (3.153)

473. **Knowledge (DNI):** Information from multiple sources integrated with common, environmental, real-world experience.

474. **Known or reasonably foreseeable hazard (FSMA-PC Guide):** A potential biological, chemical (including radiological), or physical hazard that is known to be, or has the potential to be, associated with the facility or the food.

475. **Known or Reasonably Foreseeable Hazard FDA, FSMA, PC rule): "**We [FDA] proposed to define the term "known or reasonably foreseeable hazard" to mean a biological, chemical (including radiological), or physical hazard that has the potential to be associated with the facility or the food."

476. **Law (Black's Law):** 1. Regime that orders human activities and relations through systematic application of the force of politically organized society, or through social pressure, backed by force, in such a society; the legal system. 2. The aggregate legislation, judicial precedents, and accepted legal principles; the body of authoritative ground of judicial or administrative action, 3. The set of rules or principles dealing with a specific are of a legal system <copyright law>, 4. The judicial or administrative process; legal action and proceedings, 5. A statute <Congress passed a law>.

477. **Law, Statutory (Black's Law):** the body of law derives from statutes rather than from constitutions or judicial decisions. – also termed statute law; legislative law; ordinary law. (See statutes)

478. **Level of Protection (DNI):** Extent to which protective measures, techniques, and procedures must be applied to Information Systems (IS) and networks based on risk, threat, vulnerability,

system interconnectivity considerations, and information assurance needs. Levels of protection are: (1) Basic: IS and networks requiring implementation of standard minimum-security countermeasures. (2) Medium: IS and networks requiring layering of additional safeguards above the standard minimum-security countermeasures. (3) High: IS and networks requiring the most stringent protection and rigorous security countermeasures.

479. **Liability (Black's law):** 1. The quality or sate of being legally obligated or accountable; legal responsibility to another or to society, enforceable by civil remedy or criminal punishment. 2. A financial or pecuniary obligation; debt.
480. **Liability, Civil (Black's law):** 1. liability imposed under the civil, as opposed to criminal, law. 2. The state of being legally obligated for civil damages
481. **Liability, Contingent (Black's law):** A liability that will occur only if a specific event happens; a liability that depends on the occurrence of a future and uncertain event.
482. **Liability, Strict (Black's law):** Liability that does not depend on actual negligence or intent to harm, but that is based on the breach of an absolute duty to make something safe strict liability most often applies either to ultra-hazardous activities or in products-liability cases. – also termed "absolute liability"; "liability without fault".) (See Safe Food)
483. **Liability, Vicarious (Black's law):** Liability that a supervisory party (such as an employer) bears for the actionable conduct of a subordinate or association (such as an employee) based on the relationship between the two parties.
484. **Lifetime** (ISO Guide 30): <of a reference material (RM)> time interval during which RM properties retain their assigned values within their associated uncertainties; Note 1 to entry: The lifetime is often determined retrospectively, i.e. after RM properties no longer retain assigned values or attributes.
485. **Likelihood (DHS Lexicon 2017):** "chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities."
486. **Likelihood (ISO 31000):** "chance of something happening; NOTE 1 In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period). NOTE 2 the English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English." [ISO Guide 73:2009, definition 3.6.1.1]
487. **Lisbon Agreement/ Geographic Origins (WTO):** Treaty, administered by the World Intellectual Property Organization (WIPO), for the protection of geographical indications and their international registration.
488. **Logical structure** (ISO 22380): arrangement of data to optimize their access or processing by given user (human or machine)
489. **Long-term stability** (ISO Guide 30): <of a reference material (RM)> stability of a reference material property over an extended period of time.
490. **Madrid Agreement/ Source (WTO):** Treaty, administered by the World Intellectual Property Organization (WIPO), for the repression of false or deceptive indications of source on goods.
491. **Management** (ISO 22380): coordinated **activities** (3.1) to direct and control an **organization** (3.158)
492. **Manufacturers (GMA BP):** are businesses that produce goods for the consumer.

493. **Market (Black's law):** 1. a place of commercial activity in which goods and services are bought and sold. 2. A geographic area or demographic segment considered as a place of demand for particular goods or services; especially prospective purchasers of goods.
494. **Material (DNI):** Elements, constituents, or substances of which something is composed or can be made. It includes, but is not limited to, raw and processed material, parts, components, assemblies, fuels, and other items that may be worked into a more finished form in performance of a contract. AND (2) Materiel: Equipment, apparatus, and supplies used by an organization or institution.
495. **Material good (ISO 22300)**: manufactured, grown product or one secured from nature;
496. **Material good life cycle** (ISO 22380): stages in the life of a **material good** (3.139) including conception, design, manufacture, storage, service, resell and disposal
497. **Matrix reference material** (ISO Guide 30):reference material that is characteristic of a real sample; EXAMPLE: Soil, drinking water, metal alloys, blood; Note 1 to entry: Matrix reference materials may be obtained directly from biological, environmental or industrial sources; Note 2 to entry: Matrix reference materials may also be prepared by spiking the component(s) of interest into an existing material; Note 3 to entry: A chemical substance dissolved in a pure solvent is not a matrix material; Note 4 to entry: Matrix materials are intended to be used in conjunction with the analysis of real samples of the same or a similar matrix.
498. **Maximum acceptable outage, MAO** (ISO 22380): time it would take for adverse **impacts** (3.107), which can arise as a result of not providing a product/service or performing an **activity** (3.1), to become unacceptable; Note 1 to entry: See also **maximum tolerable period of disruption** (3.142).
499. **Maximum tolerable period of disruption, MTPD** (ISO 22380): time it would take for adverse **impacts** (3.107), which can arise as a result of not providing a product/service or performing an **activity** (3.1), to become unacceptable; Note 1 to entry: See also **maximum acceptable outage** (3.141).
500. **Measurement** (ISO 22380): **process** (3.180) to determine a value
501. **Metadata (DNI):** Information that describes a number of characteristics, or attributes, of data; that is, data that describes data. For any particular datum, the metadata may describe how the datum is represented, ranges of acceptable values, it should be labeled, as well as its relationship to other data. Metadata also may provide other relevant information, such as the responsible steward, associated laws and regulations, and access management policy. The metadata for structured data objects describes the structure, data elements, interrelationships, and other characteristics of information, including its creation, disposition, access and handling controls, formats, content, and context, as well as related audit trails.
502. **Metadata** (ISO 22380): **information** (3.116) to describe audiovisual content and data essence in a defined format; EXAMPLE: Time and date, text strings, location identifying data, audio and any other associated, linked or processed information.
503. **Microorganisms (FSMA-PC Guide):** Yeast, molds, bacteria, viruses, protozoa, and microscopic parasites and includes species that are pathogens. The term "undesirable microorganisms" includes those microorganisms that are pathogens, that subject food to decomposition, that indicate that
504. **Minimum business continuity objective, MBCO** (ISO 22380): minimum level of services and/or products that is acceptable to an **organization** (3.158) to achieve its business **objectives** (3.153) during a **disruption** (3.70)
505. **Minimum sample size, minimum sample intake** (ISO Guide 30): lower limit of the amount of an RM, usually expressed as a mass quantity, that can be used in a measurement process such that the values or attributes expressed in the corresponding RM documentation are valid
506. **Misbranded Foods (FD&C Act, Ostroff Summary, 2017):** "offered for sale under the name of another food", "labelling is false or misleading", and "ingredient labeling."

507. **Misbranded Foods (FD&C Act, summary)**: Comment- Generally a false or misleading label. Stolen goods sold in commerce would be "Misbranded" or "Adulterated" (handling conditions cannot be confirmed). Other examples includes counterfeit labels, up-labeling (label designation a higher quality product than is in the package), incorrect manufacturers, incorrect country of origin.
508. **Misdescription, food product (CEN):** A mismatch between the actual food product characteristic and the corresponding food product claim; Note 1 to entry: Food product misdescription can be deliberate or accidental; Note 2 to entry: Misdescription on the label of a food product is often referred to as mislabelling, but the term mislabelling is also used to refer to when the label is not in accordance with relevant requirements or regulations. If the consumer product was a cod fillet and label just said "fish", that would not be a misdescription, but it would most likely be a violation of the labelling requirements that normally require the species to be explicitly specified on commercial labels; Note 3 to entry: Common types of misdescription or mislabelling include: When the stated geographical origin, species, or method of production or storage does not match the actual product characteristic, When processes that should have been declared (e.g. irradiation, freezing) were used when making the product, and not declared; When the stated production date does not match the actual production date; When the stated best before date, use by date, or expiration date does not match the respective dates calculated by the producer, using their normal methods; When the stated ingredient is not the actual ingredient; When the amounts stated for the ingredients do not correspond to the actual ingredient amounts used; When ingredients or adulterants that should have been declared (e.g. water, starch) were added to the product, but not declared
509. **Mitigation (0 Summary):** "…is intended to reduce the consequence of the event (ISO 2007a, ISO 2007, ISO 2007b, DHS 2013, Merriam-Webster 2004). This assumes the hazard event will occur so the goal is to mitigate or reduce the negative consequence. This focuses on reducing the risk that cannot be eliminated. " (Spink, Ortega, Chen & Wu, 2017).
510. **Mitigation** (ISO 22380): limitation of any negative **consequence** (3.46) of a particular **incident** (3.111)
511. **Modes of delivery (WTO):** How international trade in services is supplied and consumed. Mode 1: cross border supply; mode 2: consumption abroad; mode 3: foreign commercial presence; and mode 4: movement of natural persons.
512. **Monitor (FSMA-PC Guide):** To conduct a planned sequence of observations or measurements to assess whether control measures are operating as intended.
513. **Monitoring** (ISO 22000): determining the status of a system, a **process** (3.36) or an activity; Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe; Note 2 to entry: In the context of food safety, monitoring is conducting a planned sequence of observations or measurements to assess whether a process is operating as intended; Note 3 to entry: Distinctions are made in this document between the terms **validation** (3.44), **monitoring** (3.27) and **verification**(3.45): — validation is applied prior to an activity and provides information about the capability to deliver intended results; — monitoring is applied during an activity and provides information for action within a specified time frame; — verification is applied after an activity and provides information for confirmation of conformity.
514. **Monitoring** (ISO 22380): determining the status of a system, a **process** (3.180), a product, a service, or an **activity** (3.1); Note 1 to entry: For the determination of the status, there can be a need to check, supervise or critically observe.
515. **National Intelligence (DNI):** National Intelligence refers to all intelligence, regardless of the source from which derived and including information gathered within or outside the U.S., that: (A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and (B) that involves (i) threats to the United States, its people,

property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on United States national or homeland security.

516. **National Security (DNI):** The national defense or foreign relations of the United States.
517. **Nonconformity** (ISO 22380): non-fulfilment of a **requirement** (3.190);
518. **Object** (ISO 22380): single and distinct **entity** (3.79) that can be identified
519. **Objective** (ISO 22380): result to be achieved; Note 1 to entry: An objective can be strategic, tactical, or operational; Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental objectives) and can apply at different levels (such as strategic, organization-wide, project, product and **process** (3.180)); Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion or by the use of other words with similar meaning (e.g. aim, goal, or **target**(3.255)); Note 4 to entry: In the context of security operations **management** (3.233) systems, **security operations objectives** (3.234) are set by the organization, consistent with the **security operations policy** (3.236), to achieve specific results.
520. **Observer** (ISO 22380): **participant** (3.163) who witnesses the **exercise** (3.83) while remaining separate from exercise activities; Note 1 to entry: Observers may be part of the **evaluation** (3.81)**process** (3.180).
521. **Off-the-shelf authentication tool** (ISO 22380): **authentication tool** (3.20) that can be purchased through open sales networks
522. **On-line authentication tool** (ISO 22380): **authentication tool** (3.20) that requires a real-time on-line connection to be able to locally interpret the **authentication element** (3.17)
523. **Operational information** (ISO 22380): **information** (3.116) that has been contextualized and analysed to provide an understanding of the situation and its possible evolution
524. **Operations Security, OPSEC (DNI):** Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.
525. **Organization** (ISO 22380): person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its **objectives** (3.153); Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, **partnership** (3.165), charity or institution, or part or combination thereof, whether incorporated or not, public or private; Note 2 to entry: For organizations with more than one operating unit, a single operating unit can be defined as an organization;
526. **Organization in the supply chain** (ISO 22380): **entity** (3.79) that: — manufactures, handles, processes, loads, consolidates, unloads or receives **goods** (3.98) upon placement of a purchase order that at some point crosses an international or economy border; — transports goods by any mode in the **international supply chain** (3.127) regardless of whether their particular segment of the **supply chain** (3.251) crosses national (or economy) boundaries, or; — provides, manages or conducts the generation, distribution or flow of shipping **information**(3.116) used by customs agencies or in business practices.
527. **Outsource** (ISO 22380): make an arrangement where an external **organization** (3.158) performs part of an organization's function or **process** (3.180); Note 1 to entry: An external organization is outside the scope of the **management system** (3.137), although the outsourced function or process is within the scope.
528. **Overt authentication element** (ISO 22380): **authentication element** (3.17) that is detectable and verifiable by one or more of the human senses without resource to a tool (other than everyday tools which correct imperfect human senses, such as spectacles or hearing aids)

529. **Owner** (ISO 22380): **entity** (3.79) that legally controls the licensing and user rights and distribution of the **object** (3.151)associated with the unique identifier **(UID)** (3.269)
530. **Packaging (GFSI v7.2, Glossary):** Material or package which provides protection, tampering resistance, and special physical, chemical, or biological needs to maintain food safety.
531. **Parallel Imports (Black's law):** Goods bearing valid trademarks that are manufactured abroad and imported into the US to compete with domestically manufactured goods bearing the same valid trademarks. Domestic parties commonly complain that parallel imports compete unfairly in the US market. But US trademark law does not prohibit the sale of most parallel imports. –Also termed "gray-market goods". See "Gray Market" under "Market".
532. **Parallel imports/ parallel trade (WTO):** When a product made legally (i.e. not pirated) abroad is imported without the permission of the intellectual property right-holder (e.g. the trademark or patent owner). Some countries allow this, others do not.
533. **Paris Convention/ Patents (WTO):** Treaty, administered by the World Intellectual Property Organization (WIPO), for the protection of industrial intellectual property, i.e. patents, utility models, industrial designs, etc.
534. **Participant** (ISO 22380): person or **organization** (3.158) who performs a function related to an **exercise** (3.83)
535. **Partnering** (ISO 22380): associating with others in an **activity** (3.1) or area of common interest in order to achieve individual and collective **objectives** (3.153)
536. **Partnership** (ISO 22380): organized relationship between two bodies (public–public, private–public, private–private) which establishes the scope, roles, **procedures** (3.179) and tools to prevent and manage any **incident**(3.111) impacting on **security** (3.223) and **resilience** (3.192) with respect to related laws
537. **Patent (Black's Law):** 1. The governmental grant of a right, privilege, or authority. 2. The official document so granting.
538. **Patent** (TRIPs)**:** "shall confer on its owner the following exclusive rights… to prevent third parties not having the owner's consent from the acts of: making, using, offering for sale, selling, or importing6 for these purposes that product". This is "available for any inventions, whether products or processes, in all fields of technology, provided that they are new, involve an inventive step and are capable of industrial application" (REF TRIPS). This generally covers "Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof" and the duration is "20 years from date of filing [utility/ plant] and 14 years from patent grant [design]" (REF USPTO)
539. **Patent, Design (Black's law):** A patent granted for a new, original, and ornamental design for an article of manufacture; a patent that protects a products appearance or non-functional aspects. Design patents – which, unlike utility patents, have a term of only 14 years from the date the patent is granted – are similar to copyrights.
540. **Patent, Utility (Black's Law):** A patent granted for one of the following types of inventions: a process, a machine, a manufacture, or a composition of matter (such as a new chemical). Utility patents are the most commonly issued patent.
541. **Penetration (DNI):** A successful unauthorized access to a computer system.
542. **Penetration Testing (DNI):** A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.
543. **People integrity (Manning):** can be described as the honesty and morals exhibited by an individual and/or
544. **Performance** (ISO 22380): measurable result; Note 1 to entry: Performance can relate either to quantitative or qualitative findings; Note 2 to entry: Performance can relate to

the **management** (3.135) of **activities** (3.1), **processes**(3.180), products, services, systems or **organizations** (3.158).

545. **Performance evaluation** (ISO 22380): **process** (3.180) of determining measurable results

546. **Period of validity** (ISO Guide 30): <of a reference material (RM)> time interval during which the producer of the RM warrants its stability; Note 1 to entry: The period of validity may be expressed as a specific date or an otherwise defined period of time; Note 2 to entry: The period of validity is designed to be within the lifetime of an RM.

547. **Persistence (NIST2):** The placement/storage of data in a medium design to allow its future access.

548. **Personnel** (ISO 22380): people working for and under the control of an **organization** (3.158)

549. **Piracy/ copyright (WTO):** Unauthorized copying of materials protected by intellectual property rights (such as copyright, trademarks, patents, geographical indications, etc) for commercial purposes and unauthorized commercial dealing in copied materials.

550. **Pirated copyright goods** (TRIPs)**:** "shall mean any goods which are copies made without the consent of the right holder or person duly authorized by the right holder in the country of production and which are made directly or indirectly from an article where the making of that copy would have constituted an infringement of a copyright or a related right under the law of the country of importation."

551. **Policy** (ISO 22380): intentions and direction of an **organization** (3.158) as formally expressed by its top **management** (3.263)

552. **Portability (NIST2):** The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported.

553. **Precautionary principle (WTO):** Member countries are encouraged to use international standards, guidelines and recommendations where they exist. When they do, they are unlikely to be challenged legally in a WTO dispute. However, members may use measures which result in higher standards if there is scientific justification. They can also set higher standards based on appropriate assessment of risks so long as the approach is consistent, not arbitrary. And they can to some extent apply the "precautionary principle", a kind of "safety first" approach to deal with scientific uncertainty. Article 5.7 of the SPS Agreement allows temporary "precautionary" measures.

554. **Precision (Capra):** "how two measurements agree with each other regardless of the "accuracy"". The quote is: "The precision of an analytical procedure expresses the closeness of agreement (degree of scatter) between a series of measurements obtained from multiple sampling of the same homogeneous sample under the prescribed conditions. Precision may be considered at three levels: repeatability, intermediate precision and reproducibility. Precision should be investigated using homogeneous, authentic samples. However, if it is not possible to obtain a homogeneous sample it may be investigated using artificially prepared samples or a sample solution. The precision of an analytical procedure is usually expressed as the variance, standard deviation or coefficient of variation of a series of measurements." (REF)

555. **Precision (DNI):** Refers to the level of measurement and exactness of description in a geographic information system (GIS) database. Precise locational data may measure position to a fraction of a unit. Precise attribute information may specify the characteristics of features in great detail. It is important to realize, however, that precise data - no matter how carefully measured - may be inaccurate. Surveyors may make mistakes or data may be entered into the database incorrectly. Therefore, a distinction is made between precision and accuracy.

556. **Preparedness** (ISO 22380): **readiness**

557. **Preparedness, readiness (ISO 22380): activities** (3.1), programmes, and systems developed and implemented prior to an **incident** (3.111)that can be used to support and enhance prevention,

protection from, mitigation of, response to and recovery from **disruptions** (3.70), **emergencies** (3.77) or **disasters** (3.69)

558. **Prerequisite programs (FSMA-PC Guide):** Procedures, including Current Good Manufacturing Practices (CGMPs), that provide the basic environmental and operating conditions necessary to support the Food Safety Plan.

559. **Prevention (0 Summary):** "…is intended to reduce or eliminate the likelihood of the event occurring (ISO 2007, ISO 2007a, ISO 2007b, ISO 2008, Merriam-Webster 2004). This focuses on identifying and eliminating or reducing vulnerability." (Spink, Ortega, Chen & Wu, 2017)

560. **Prevention** (ISO 22380): measures that enable an **organization** (3.158) to avoid, preclude or limit the **impact** (3.107) of an **undesirable event** (3.268) or potential **disruption** (3.70)

561. **Prevention of hazards and threats** (ISO 22380):

562. **Preventive action** (ISO 22380): action to eliminate the cause of a potential **nonconformity** (3.149) 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** (3.54) is taken to prevent recurrence.

563. **Preventive control (GAO Green):** An activity that is designed to prevent an entity from failing to achieve an objective or addressing a risk (paragraph 10.04)

564. **Preventive controls (FDA, FSMA, CFR):** means those risk-based, reasonably appropriate procedures, practices, and processes that a person knowledgeable about the safe manufacturing, processing, packing, or holding of food would employ to significantly minimize or prevent the hazards identified under the hazard analysis that are consistent with the current scientific understanding of safe food manufacturing, processing, packing, or holding at the time of the analysis.

565. **Preventive Controls (FDA, FSMA, US CODE):** The term 'preventive controls' means those risk-based, reasonably appropriate procedures, practices, and processes that a person knowledgeable about the safe manufacturing, processing, packing, or holding of food would employ to significantly minimize or prevent the hazards identified under the hazard analysis conducted under subsection (b) and that are consistent with the current scientific understanding of safe food manufacturing, processing, packing, or holding at the time of the analysis.

566. **Preventive controls (FSMA-PC Guide):** Those risk-based, reasonably appropriate procedures, practices, and processes that a person knowledgeable about the safe manufacturing, processing, packing, or holding of food would employ to significantly minimize or prevent the hazards identified under the hazard analysis that are consistent with the current scientific understanding of safe food manufacturing, processing, packaging, or holding at the time of the analysis.

567. **Preventive controls qualified individual (FDA, FSMA, CFR):** means a qualified individual who has successfully completed training in the development and application of risk-based preventive controls at least equivalent to that received under a standardized curriculum recognized as adequate by FDA or is otherwise qualified through job experience to develop and apply a food safety system.

568. **Preventive controls qualified individual (PCQI) (FSMA-PC Guide):** A qualified individual who has successfully completed training in the development and application of risk-based preventive controls at least equivalent to that received under a standardized curriculum recognized as adequate by FDA or is otherwise qualified through job experience to develop and apply a food safety system.

569. **Primary measurement standard** (ISO Guide 30):measurement standard that is designated or widely acknowledged as having the highest metrological qualities and whose property value is accepted without reference to other standards of the same property or quantity, within a specified context; Note 1 to entry: See also ISO/IEC Guide 99:2007.[1]

570. **Prioritized activity** (ISO 22380): **activity** (3.1) to which priority is given following an **incident** (3.111) in order to mitigate **impacts**(3.107); Note 1 to entry: Terms commonly used to describe these activities include critical, essential, vital, urgent and key.
571. **Privacy (NIST2):** The assured, proper, and consistent collection, processing, communication, use and disposition of data associated with personal information and PII throughout its life cycle.
572. **Probability** (ISO 22380): measure of the chance of occurrence expressed as a number between 0 and 1 where 0 is impossibility and 1 is absolute certainty; Note 1 to entry: See also **likelihood** (3.133).
573. **Probability (ISO 31000):** Not defined, but under likelihood noted "NOTE 2 The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English. [ISO Guide 73:2009, definition 3.6.1.1]"
574. **Procedure** (ISO 22380): specified way to carry out an **activity** (3.1) or a **process** (3.180); Note 1 to entry: Procedures can be documented or not; Note 2 to entry: When a procedure is documented, the term "written procedure" or "documented procedure" is frequently used. The document that contains a procedure can be called a "procedure document".
575. **Process (CEN):** A set of interrelated or interacting activities which transforms inputs to outputs (ISO 22000). [NOTE: the CEN standard often refers to citations from other standards such as ISO.]
576. **Process** (ISO 22380): set of interrelated or interacting **activities** (3.1) that use inputs to deliver an intended result
577. **Process integrity (Manning): "**the activities undertaken to produce the food item encompassing the design, assurance, monitoring and verification of processes within the product life-cycle to ensure that they remain authentic and intact, i.e. extrinsic characteristics;"
578. **Process** (3.180), practices, techniques, materials, products, services or **resources** (3.193) used to avoid, reduce, or control **hazards** (3.99) and **threats** (3.259) and their associated **risks** (3.199) of any type in order to reduce their potential **likelihood** (3.133) or **consequences** (3.46)
579. **Product - End product** (ISO 22000):**- product** (3.37) that will undergo no further processing or transformation by the **organization** (3.31); Note 1 to entry: A product that undergoes further processing or transformation by another organization is an end product in the context of the first organization and a raw material or an ingredient in the context of the second organization.
580. **Product (CEN):** An output that is a result of a process (ISO 22000), Note 1 to entry: Product can be an intermediate, material, semifinished or final product.
581. **Product** (ISO 22000): **-** output that is a result of a **process** (3.36); Note 1 to entry: A product can be a service.
582. **Product identifier (ISO 22300):** The term `product identifier' means a standardized graphic that includes, in both human-readable form and on a machine-readable data carrier that conforms to the standards developed by a widely recognized international standards development organization, the standardized numerical identifier, lot number, and expiration date of the product.
583. **Product information sheet (ISO Guide 30):** <of a reference material (RM)> document containing all the information that is essential for using an RM other than a CRM
584. **Product Integrity (CRS2018):** Ensuring product integrity was the key task of FDA's predecessors in the early 1900s. Protecting the supply chain from counterfeit, diverted, subpotent, substandard, adulterated, misbranded, or expired drugs remains an essential concern of the agency. […] FDA monitors product integrity beyond the drug's initial manufacture. It continues as the drug moves throughout the supply chain from its manufacturer to one or more wholesale distributors to the entity that dispenses it to the patient. Title II of the Drug Quality and Security Act of 2013 (DQSA;

P.L. 113-54), the Drug Supply Chain Security Act, established track-and-trace requirements for prescription drugs, to be implemented over a period of 10 years. Among other things, the law requires manufacturers and repackagers to a put a product identifier, including a standardized numerical identifier, on each package and homogenous case.62"

585. **Product integrity** (Manning): "the inherent quality attribute of totality or completeness [2] i.e. intrinsic characteristics"
586. **Product or service** (ISO 22380): beneficial outcome provided by an **organization** (3.158) to its customers, recipients and **interested parties** (3.124); EXAMPLE: Manufactured items, car insurance, or community nursing. [See goods, material goods]
587. **Product tampering (Davidson):** This is defined as intentional alteration of a product, or the labelling or container with an intent to cause harm (Canadian Food Inspection Agency, 2014)
588. **Production batch, batch, lot** (ISO Guide 30): definite amount of material produced during a single manufacturing cycle, and intended to have uniform character and quality; Note 1 to entry: The uniform conditions of manufacture or production of the batch or lot must be such as to ensure a homogeneous product; Note 2 to entry: In statistics, an entire batch may be considered a finite population (totality of items under consideration); Note 3 to entry: See also "lot" in ISO 3534-2:2006.[6]; Note 4 to entry: See also the IUPAC Compendium of Analytical Nomenclature.[5];
589. **Promisor (Black's law):** One who makes a promise; especially, a party who undertakes a contractual obligation.
590. **Property attribute** (ISO Guide 30): <of a reference material (RM)> value or non-numerical descriptor corresponding to a qualitative characteristic representing a physical, chemical or biological property of an RM
591. **Property value** (ISO Guide 30): <of a reference material (RM)> value corresponding to a quantity representing a physical, chemical or biological property of an RM
592. **Protect (DNI):** To keep information systems away from intentional, unintentional, and natural threats: 1) preclude an adversary from gaining access to information for the purpose of destroying, corrupting, or manipulating such information; or (2) deny use of information systems to access, manipulate, and transmit mission-essential information.
593. **Protection** (ISO 22380): measures that safeguard and enable an **organization** (3.158) to reduce the **impact** (3.107) of a potential **disruption** (3.70)
594. **Prudent Person (Black's law):** See "Reasonable person." (Comment- this term is used in US food laws.)
595. **Public warning** (ISO 22380): **notification** (3.150) and **alert** (3.4) messages disseminated as an **incident response** (3.115)measure to enable responders and **people at risk** (3.166) to take safety measures
596. **Public warning system** (ISO 22380): set of protocols, **processes** (3.180) and technologies based on the **public warning** (3.183)**policy**(3.171) to deliver **notification** (3.150) and **alert** (3.4) messages in a developing **emergency** (3.77)situation to **people at risk** (3.166) and to first responders
597. **Purity (SQF):** The absence of contaminants that could cause a food safety hazard.
598. **Purpose-built authentication tool** (ISO 22380): **authentication tool** (3.20) dedicated to a specific **authentication solution** (3.19)
599. **Qualified Auditor (FDA, FSMA, CFR):** means a person who is a qualified individual as defined in this part and has technical expertise obtained through education, training, or experience (or a combination thereof) necessary to perform the auditing function as required by 117.180(c)
600. **Qualified Individual (FDA, FSMA, CFR):** means a person who has the education, training, or experience (or a combination thereof) necessary to manufacture, process, pack, or hold clean and safe food as appropriate to the individual's assigned duties. A qualified individual may be, but is not required to be, an employee of the establishment.

601. **Qualified individual (FSMA-PC Guide):** A person who has the education, training, or experience (or a combination thereof) necessary to manufacture, process, pack, or hold clean and safe food as appropriate to the individual's assigned duties. A qualified individual may be, but is not required to be, an employee of the establishment.
602. **Quality control material** (ISO Guide 30): <of a reference material (RM)> reference material used for quality control of a measurement
603. **Quality information (GAO Green):** Information from relevant and reliable data that is appropriate, current, complete, accurate, accessible, and provided on a timely basis, and meets identified information requirements (paragraph 13.05)
604. **Raw material (GFSI):** A component of a food, feed or packaging that has not undergone processing.
605. **Reasonable assurance (GAO Green):** A high degree of confidence, but not absolute confidence (paragraph OV1.04)
606. **Reasonable Person (Black's Law):** 1. A hypothetical person used as a legal standard, especially to determine whether someone acted with negligence; specifically, a person who exercises the degree of attention, knowledge, intelligence, and judgment that society requires of its members for the protection of their own and others interests. The reasonable person acts sensibly, does things without serous delay, and takes proper but not excessive precautions. –Also termed "reasonable man"; "prudent person"; "ordinarily prudent person"; "reasonably prudent person"; "highly prudent person"." 2. Archaic. A human being.
607. **Record** (ISO 22380): **document** (3.71) stating results achieved or providing evidence of **activities** (3.1) performed
608. **Record based methods for (food product) authentication, food product (CEN):** Methods and procedures for investigating the veracity, consistency or likelihood of claims, based on recordings made in the supply chain for the food product in question; Note 1 to entry: These methods largely focus on identifying discrepancies in recorded data; on identifying sets of claims that are mutually contradictory; Note 2 to entry: The record based methods for food product authentication can be applied on aggregate level, e.g. for countries, regions, or industry sectors, or they can be applied in specific supply chains or companies. When applied in specific supply chains or companies, the claims are normally extracted from the traceability system; Note 3 to entry: A common record based method for food product authentication is material flow analysis / mass balance accounting, which is based on the mass balance principle; that matter is conserved in any system, and thus input is equal to output mass. Another common record based method for food product authentication is input output analysis, where claims relating to transactions between trading partners are examined for consistency (if A claimed that 1000 kg of a product was sent to B then there should be a corresponding claim at B stating that 1000 kg of the same product was received from A).
609. **Recovery** (ISO 22380): restoration and improvement, where appropriate, of operations, **facilities** (3.90), livelihoods or living conditions of affected **organizations** (3.158), including efforts to reduce **risk** (3.199) factors
610. **Reference material certificate** (ISO Guide 30): document containing the essential information for the use of a CRM, confirming that the necessary procedures have been carried out to ensure the validity and metrological traceability of the stated property values; Note 1 to entry: The required and recommended content of a reference material certificate is described in ISO Guide 31.[4]
611. **Reference material certification** (ISO Guide 30): action of a reference material (RM) producer that formally establishes the certified values of a CRM and states them in an RM certificate Note 1 to entry: RM certification is a first-party attestation in accordance with the definition of the term "declaration" (ISO/IEC 17000:2004, 5.4[11]) whereas certification is a third-party attestation in accordance with the definition of the term "certification" (ISO/IEC 17000:2004, 5.5[11]).

612. **Reference material certification report** (ISO Guide 30): document giving detailed information, in addition to that contained in a reference material certificate, e.g. the preparation of the material, methods of measurement, factors affecting accuracy, statistical treatment of results, and the way in which metrological traceability was established; Note 1 to entry: See also the IUPAC Compendium of Analytical Nomenclature.[5]
613. **Reference material producer** (ISO Guide 30): <of a reference material (RM)> body (organization or company, public or private) that is fully responsible for project planning and management; assignment of, and decision on property values and relevant uncertainties; authorization of property values; and issuance of a reference material certificate or other statements for the reference materials it produces
614. **Reference material, RM** (ISO Guide 30):material, sufficiently homogeneous and stable with respect to one or more specified properties, which has been established to be fit for its intended use in a measurement process; Note 1 to entry: RM is a generic term; Note 2 to entry: Properties can be quantitative or qualitative, e.g. identity of substances or species; Note 3 to entry: Uses may include the calibration of a measurement system, assessment of a measurement procedure, assigning values to other materials, and quality control; Note 4 to entry: ISO/IEC Guide 99:2007[1] has an analogous definition (5.13), but restricts the term "measurement" to apply to quantitative values. However, Note 3 of ISO/IEC Guide 99:2007, 5.13 (VIM), specifically includes qualitative properties, called "nominal properties".
615. **Reference method, reference procedure** (ISO Guide 30): <of a reference material (RM)> measurement method, that has been shown to have the appropriate trueness and precision for its intended use and has been officially defined as reference method by a competent body; Note 1 to entry: See also "reference measure procedure" in ISO/IEC Guide 99:2007.[1]
616. **Regulation (Black's Law):** 1. the act or process of controlling by rule or restriction. 1. Bylaw. 3. A rule or order, having legal force, usually issued by an administrative agency. – also termed "agency regulation"; "Subordinate regulation"; "delegated legislation."
617. **Reliability (DNI):** The ability of a system and its parts to perform its mission without failure, degradation, or demand on the support system under a prescribed set of conditions.
618. **Requirement** (ISO 22380): need or expectation that is stated, generally implied or obligatory; Note 1 to entry: "Generally implied" means that it is custom or common practice for the **organization** (3.158) and **interested parties** (3.124) that the need or expectation under consideration is implied; Note 2 to entry: A specified requirement is one that is stated, for example in documented **information**(3.116).
619. **Residual risk (COSO/ERM):** the remaining risk after management has taken action to alter the risk's likelihood or impact.
620. **Residual risk** (ISO 22380): **risk** (3.199) remaining after **risk treatment** (3.215); Note 1 to entry: Residual risk can contain unidentified risk; Note 2 to entry: Residual risk can also be known as "retained risk";
621. **Resilience** (ISO 22380): ability to absorb and adapt in a changing environment
622. **Resource** (ISO 22380): asset, **facility** (3.90), equipment, material, product or waste that has potential value and can be used
623. **Response plan** (ISO 22380): documented collection of **procedures** (3.179) and **information** (3.116) that is developed, compiled and maintained in readiness for use in an **incident** (3.111)
624. **Response programme** (ISO 22380): plan, **processes** (3.180), and **resources** (3.193) to perform the **activities** (3.1) and services necessary to preserve and protect life, property, operations and critical **assets** (3.10); Note 1 to entry: Response steps generally

include **incident** (3.111) recognition, **notification** (3.150), assessment, declaration, plan execution, communications, and resources **management** (3.135).

625. **Response team** (ISO 22380): group of individuals responsible for developing, executing, rehearsing, and maintaining the **response plan** (3.194), including the **processes** (3.180) and **procedures** (3.179)
626. **Retailers (GMA BP):** are the stores selling merchandise or services directly to the public.
627. **Review** (ISO 22380): **activity** (3.1) undertaken to determine the suitability, adequacy and **effectiveness** (3.76) of the **management system** (3.137) and its component elements to achieve established **objectives** (3.153)
628. **Rights holder** (intellectual property rights) (ISO 22380): legal **entity** (3.79) either holding or authorised to use one or more intellectual property rights
629. **Risk (0 Summary): "…**is an uncertainty of an outcome that is assessed in terms of likelihood and consequence (ISO 2007a, NIST 2002, CNSSI 2010, DHS 2013). Often the consequence is sub-divided to other factors such as onset, severity, or other. Risk is a based on factors of the probability of the threat and the susceptibility from vulnerability (NRC 2009). In other applications it is an unwanted outcome (DHS 2008, Codex Alimentarius 2014, 21 CFR 50 (A) (.3)(k), Merriam-Webster 2004)." (Spink, Ortega, Chen & Wu, 2017)
630. **Risk (DHS Lexicon 2017):** "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences [CTRA: Risk = frequency * consequence]"
631. **Risk (DNI):** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence.
632. **Risk (EFSA):** is the likelihood of a hazard causing harm; e.g. swimming with a shark is a risk, e.g. standing under a tree during a thunderstorm is a risk
633. **Risk (ERM/COSO):** is defined as "Risk – the possibility that an event will occur and adversely affect the achievement of objectives." (Ref COSO full document draft)
634. **Risk (EU178/2002):** means a function of the probability of an adverse health effect and the severity of that effect, consequential to a hazard;
635. **Risk** (ISO 22380): effect of uncertainty on **objectives** (3.153); Note 1 to entry: An effect is a deviation from the expected — positive and/or negative; Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process); Note 3 to entry: Risk is often characterized by reference to potential events and **consequences**(3.46), or a combination of these; Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence; Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.
636. **Risk Acceptance (DNI):** Informed decision to take a particular risk.
637. **Risk acceptance** (ISO 22380): informed decision to take a particular **risk** (3.199); Note 1 to entry: Risk acceptance can occur without **risk treatment** (3.215) or during the **process** (3.180) of risk treatment; Note 2 to entry: Accepted risks are subject to **monitoring** (3.147) and **review** (3.197).
638. **Risk acceptance (ISO 31000)**: "informed decision to take a particular risk"; Note 1 to entry: Risk acceptance can occur without risk treatment or during the process of risk treatment; Note 2 to entry: Accepted risks are subject to monitoring and review.
639. **Risk aggregation (ISO 31000)**: "combination of a number of risks into one risk to develop a more complete understanding of the overall risk."

640. **Risk analysis** (ISO 22380): **process** (3.180) to comprehend the nature of **risk** (3.199) and to determine the level of risk; Note 1 to entry: Risk analysis provides the basis for **risk evaluation** (3.206) and decisions about **risk treatment** (3.215); Note 2 to entry: Risk analysis includes risk estimation.
641. **Risk Analysis/Risk Assessment (DNI):** The process of examining all risks, then ranking those risks by level of severity. Risk analysis involves determining what you need to protect, what you need to protect it from, and how to protect it.
642. **Risk appetite (COSO):** is the amount of risk, on a broad level, an organization is willing to accept in pursuit of value. Each organization pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so."; Further: "Risk appetite should be descriptive enough to guide actions across the organization. Management and the board should determine whether compensation incentives are aligned with risk appetite, not only for top management but throughout the organization."
643. **Risk appetite (COSO/ERM):** the board-based amount of risk a company or other entity is willing to accept in pursuit of its mission (or a vision).
644. **Risk appetite** (ISO 22380): amount and type of **risk** (3.199) that an **organization** (3.158) is willing to pursue or retain.
645. **Risk appetite (ISO Guide 73)**: "amount and type of risk that an organization is willing to pursue or retain."
646. **Risk appetite (ISO)**: "amount and type of risk that an organization is willing to pursue or retain. […]Risk assessment is all about measuring and prioritizing risks so that risk levels are managed within defined tolerance thresholds without being over-controlled or forgoing desirable opportunities.
647. **Risk assessment** (ISO 22380): overall **process** (3.180) of **risk identification** (3.207), **risk analysis** (3.201) and **risk evaluation**(3.206); Note 1 to entry: Risk assessment involves the process of identifying internal and external **threats**(3.259) and vulnerabilities, identifying the **likelihood** (3.133) and **impact** (3.107) of an **event** (3.82)arising from such threats or vulnerabilities, defining critical functions necessary to continue the organization's (3.158) operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls.
648. **Risk Assessment (ISO 31000)**: "overall process of risk identification, risk analysis, and risk evaluation."
649. **Risk attitude (ISO Guide 73)**: "organization's approach to assess and eventually pursue, retain, take or turn away from risk."
650. **Risk aversion (ISO Guide 73)**: "attitude to turn away from risk."
651. **Risk Avoidance (DNI):** A risk-handling option that eliminates risk by eliminating or modifying the concept, requirements, specifications, or practices that create the unacceptable risk.
652. **Risk Based Programme (GFSI):** A documented programme developed by a competent person(s) based on risk assessment principles.
653. **Risk communication** (ISO 22380): exchange or sharing of **information** (3.116) about **risk** (3.199) between the decision maker and other **interested parties** (3.124); Note 1 to entry: The information can relate to the existence, nature, form, **probability** (3.178), severity, acceptability, treatment or other aspects of risk.
654. **Risk Control (DNI):** A risk-handling option that monitors a known risk and then takes specific actions to minimize the likelihood of the risk occurring and/or reduce the severity of the consequences.
655. **Risk Criteria (DNI):** Terms of reference against which the significance of risk is evaluated.

656. **Risk criteria** (ISO 22380): terms of reference against which the significance of a **risk** (3.199) is evaluated; Note 1 to entry: Risk criteria are based on organizational **objectives** (3.153), and external and internal context; Note 2 to entry: Risk criteria can be derived from standards, laws, policies and other **requirements**(3.190).
657. **Risk evaluation** (ISO 22380): **process** (3.180) of comparing the results of **risk analysis** (3.201) with **risk criteria** (3.205) to determine whether the **risk** (3.199) and/or its magnitude is acceptable or tolerable.
658. **Risk identification** (ISO 22380): **process** (3.180) of finding, recognizing and describing **risks** (3.199)
659. **Risk Management (DNI):** Coordinated activities to direct and control an organization with regard to risk.
660. **Risk management** (ISO 22380): coordinated **activities** (3.1) to direct and control an **organization** (3.158) with regard to **risk** (3.199); Note 1 to entry: Risk management generally includes **risk assessment** (3.203), **risk treatment**(3.215), **risk acceptance** (3.200), and **risk communication** (3.204).
661. **Risk Maps, heat map (COSO/ERM):** These are usually two-dimensional representations of impact plotted against likelihood. […] These rankings may then be adjusted based on other considerations such as vulnerability, speed of onset, or detailed knowledge of the nature of the impact. […] They can also depict other relationships such as impact versus vulnerability. For even richer information, the size of the data points can reflect a third variable such as speed of onset or the degree of uncertainty in the estimates. [...] When using numerical ratings in a qualitative environment, it's important to remember that the numbers are labels and not suitable for mathematical manipulation although some entities do multiply the ratings, such as for impact and likelihood, to develop a preliminary ranking.
662. **Risk Mitigation (DNI):** The practice of putting controls into place to mitigate the risk once an incident occurs.
663. **Risk monitoring (ISO 31000)**: "continual checking, supervising, critically observing or determining the status to identify a change from the performance level required or expected ; NOTE: Monitoring can be applied to a risk management framework, risk management process, risk or control."
664. **Risk owner** (ISO 22380): **entity** (3.79) with the accountability and authority to manage a **risk** (3.199)
665. **Risk owners (COSO/ERM):** ultimately bear responsibility for the assessed levels of risk and defining and implementing risk response plans to bring risks within tolerance.
666. **Risk perception (ISO Guide 73)**: "stakeholder's view on a risk."; Note 1 to entry: Risk perception reflects the stakeholder's needs, issues, knowledge, belief, and values.
667. **Risk prioritization (COSO/ERM):** is the process of determining risk management priorities by comparing the level of risk against predetermined target risk levels and tolerance thresholds. Risk is viewed not just in terms of financial impact and probability, but also subjective criteria such as health and safety impact, reputational impact, vulnerability, and speed of onset.
668. **Risk Profile (GFSI v7.2, Glossary):** The result of the process of risk evaluation which has been undertaken by a competent authority, who has considered all appropriate criteria.
669. **Risk reduction** (ISO 22380): actions taken to lessen the **probability** (3.178) or negative **consequences** (3.46), or both, associated with a **risk** (3.199)
670. **Risk register** (ISO 22380): **record** (3.186) of **information** (3.116) about identified **risks** (3.199)
671. **Risk review (ISO 31000)**: "activity is undertaken to determine the suitability, adequacy, and effectiveness of the subject matter to achieve established objectives NOTE Review can be applied to a risk management framework, risk management process, risk or control."

672. **Risk sharing** (ISO 22380): form of **risk treatment** (3.215) involving the agreed distribution of **risk** (3.199) with other parties; Note 1 to entry: Legal or regulatory **requirements** (3.190) can limit, prohibit or mandate risk sharing; Note 2 to entry: Risk sharing can be carried out through insurance or other forms of contract; Note 3 to entry: The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements; Note 4 to entry: Risk transfer is a form of risk sharing.
673. **Risk source** (ISO 22380): element which alone or in combination has the intrinsic potential to give rise to **risk** (3.199); Note 1 to entry: A risk source can be tangible or intangible.
674. **Risk tolerance** (COSO): is defined as: The acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as those used to measure the related objective. In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Operating within risk tolerances helps ensure that the entity remains within its risk appetite and, in turn, that the entity will achieve its objectives."; Further: "Risk tolerances guide operating units as they implement risk appetite within their sphere of operation. Risk tolerances communicate a degree of flexibility, while risk appetite sets a limit beyond which additional risk should not be taken."
675. **Risk tolerance (COSO/ERM):** the acceptable variation relative to the achievement of an objective.
676. **Risk tolerance (GAO Green):** The acceptable level of variation in performance relative to the achievement of objectives (paragraph 6.08)
677. **Risk tolerance** (ISO 22380): **organization's** (3.158) or interested party's readiness to bear the **risk** (3.199) after **risk treatment**(3.215) in order to achieve its **objectives** (3.153)
678. **Risk treatment** (ISO 22380): **process** (3.180) to modify **risk** (3.199); Note 1 to entry: Risk treatment can involve: — avoiding the risk by deciding not to start or continue with the **activity** (3.1) that gives rise to the risk,; — taking or increasing risk in order to pursue an opportunity; — removing the **risk source** (3.213), changing the **likelihood** (3.133); — changing the **consequences** (3.46); — sharing the risk with another party or parties (including contracts and risk financing), and; — retaining the risk by informed decision; Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "**risk reduction** (3.210)"; Note 3 to entry: Risk treatment can create new risks or modify existing risks.
679. **Risk treatment (ISO 31000):** "process to modify risk."; Note 1: Risk treatment can involve: avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; taking or increasing risk in order to pursue an opportunity; removing the risk source (2.16); changing the likelihood (2.19); changing the consequences (2.18); sharing the risk with another party or parties (including contracts and risk financing); and Retaining the risk by informed decision.; Note 2: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation," "risk elimination," "risk prevention," and "risk reduction."; Note 3: Risk treatment can create new risks or modify existing risks.
680. **Robustness (FDA):** "The robustness of an analytical procedure is a measure of its capacity to remain unaffected by small, but deliberate variations in method parameters and provides an indication of its reliability during normal usage"
681. **Robustness** (ISO 22380): ability of a system to resist virtual or physical, internal or external **attacks** (3.11); Note 1 to entry: Particularly, the ability to resist attempted imitation, copy, intrusion or bypassing.
682. **Rome Convention/ Copyright, performances (WTO):** Treaty, administered by the World Intellectual Property Organization (WIPO), United Nations Educational, Scientific and Cultural

Organization (UNESCO) and International Labour Organization (ILO), for the protection of the works of performers, broadcasting organizations and producers of phonograms.

683. **Safe food** (Elliott Review): "…is defined under EU food law as food which is not injurious to health or unfit for human consumption (EU Regulation 178/2002 General Food Law). A food can become injurious to health by: Adding an article or substance to it; Using an article or substance as an ingredient in its preparation; Abstracting (which means "taking away") any constituent from it; or Subjecting it to any other process or treatment. The Regulation prohibits food being placed on the market if it is unsafe. Unsafe food must be withdrawn from sale or recalled from consumers if it has already been sold." (See Safe Food (EU178/2002)

684. **Safe food (GFSI v7.2, Glossary):** Food which not injurious to health or unfit for human consumption.

685. **Safe food (GFSI): "**Food which not injurious to health or unfit for human consumption"

686. **Safe Food/ Unsafe Food (Food safety requirements) (EU178/2002):** Comment- "Safe Food" is not specifically defined; "It is therefore necessary to establish general requirements for only safe food and feed to be placed on the market, to ensure that the internal market in such products functions effectively"; "unsafe" is expressed; "1. Food shall not be placed on the market if it is unsafe, 2. Food shall be deemed to be unsafe if it is considered to be: (a) injurious to health; (b) unfit for human consumption. 3. In determining whether any food is unsafe, regard shall be had: (a) to the normal conditions of use of the food by the consumer and at each stage of production, processing and distribution, and (b) to the information provided to the consumer, including information on the label, or other information generally available to the consumer concerning the avoidance of specific adverse health effects from a particular food or category of foods. / 5. In determining whether any food is unfit for human consumption, regard shall be had to whether the food is unacceptable for human consumption according to its intended use, for reasons of contamination, whether by extraneous matter or otherwise, or through putrefaction, deterioration or decay.

687. **Safety (the state of being safe) (DNI):** Freedom from unacceptable risk of harm. NOTE: In standardization, the safety of products, processes and services is generally considered with a view to achieving the optimum balance of a number of factors, including non-technical factors such as human behaviour that will eliminate avoidable risks of harm to persons and goods to an acceptable degree.

688. **Sample (ISO Guide 30):** <of a reference material (RM)> portion (amount) of material taken from a batch; Note 1 to entry: The sample should be representative of the batch with respect to the property or properties being investigated; Note 2 to entry: The term may be used to cover either a unit of supply or a portion for analysis; Note 3 to entry: The portion taken may consist of one or more sampling units (such as subsamples or units) and the batch may be considered to be the population from which the sample is taken; Note 4 to entry: See also the IUPAC Compendium of Analytical Nomenclature.[5]

689. **Sampling - Simple random sampling** (ISO Guide 30): sampling where a sample of n sampling units is taken from a batch in such a way that all the possible combinations of n sampling units have the same probability of being taken; Note 1 to entry: In bulk sampling, if the sampling unit is an increment, the positioning, delimitation and extraction of increments is such that all sampling units have an equal probability of being selected.

690. **Sampling - Stratified sampling** (ISO Guide 30): sampling such that portions of the sample are drawn from the different strata and each stratum is sampled with at least one sampling unit; Note 1 to entry: In some cases, the portions are specified proportions determined in advance. If the stratification is done after the sampling, the specified proportions would not be known in advance; Note 2 to entry: Items from each stratum are often selected by random sampling.

691. **Sampling - Stratified simple random sampling (ISO Guide 30):** simple random sampling from each stratum; Note 1 to entry: If the proportions of items drawn from the differing strata are equal to the proportions of population items in the strata, it is called proportional stratified simple random sampling.
692. **Scenario** (ISO 22380): pre-planned storyline that drives an **exercise** (3.83), as well as the stimuli used to achieve exercise project **performance** (3.167)**objectives** (3.153)
693. **Scheme (GFSI):** A documented food safety scheme, which has specified requirements, specific rules and procedures.
694. **Scheme Owner (GFSI):** An organisation, which is responsible for the development, management and maintenance of a scheme.
695. **Secondary measurement standard** (ISO Guide 30): measurement standard whose property value is assigned by comparison with a primary measurement standard of the same property or quantity; Note 1 to entry: See also ISO/IEC Guide 99:2007.[1]
696. **Secret** (ISO 22380): data and/or knowledge that are protected against disclosure to unauthorised entities
697. **Security (DNI):** A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.
698. **Security (ISO 22380):** state of being free from danger or **threat** (3.259)
699. **Security (NIST2):** Protecting data, information, and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:
700. **Security aspect** (ISO 22380): characteristic, element, or property that reduces the **risk** (3.199) of unintentionally-, intentionally-, and naturally-caused **crises** (3.59) and **disasters** (3.69) which disrupt and have **consequences** (3.46) on the **products or services** (3.181), operation, critical **assets** (3.10) and **continuity** (3.49) of an **organization** (3.158) and its **interested parties** (3.124)
701. **Security cleared (ISO 22380): process** (3.180) of verifying the trustworthiness of people who will have access to **security sensitive information** (3.240)
702. **Security Controls (DNI):** The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
703. **Security declaration** (ISO 22380): documented commitment by a **business partner** (3.30), which specifies **security** (3.223) measures implemented by that business partner, including, at a minimum, how **goods** (3.98) and physical instruments of international trade are safeguarded, associated **information** (3.116) is protected and security measures are demonstrated and verified; Note 1 to entry: It will be used by the **organization in the supply chain** (3.159) to evaluate the adequacy of security measures related to the security of goods.
704. **Security management** (ISO 22380): systematic and coordinated **activities** (3.1) and practices through which an **organization** (3.158)optimally manages its **risks** (3.199), and the associated potential **threats** (3.259) and **impacts** (3.107)
705. **Security management objective** (ISO 22380): specific outcome or achievement required of **security** (3.223) in order to meet the security management**policy** (3.229); Note 1 to entry: It is essential that such outcomes are linked either directly or indirectly to providing the products, supply or services delivered by the total business to its customers or end users.
706. **Security management policy** (ISO 22380): overall intentions and direction of an **organization** (3.158), related to the **security** (3.223) and the framework for the control of

security-related **processes** (3.180) and **activities** (3.1) that are derived from and consistent with its **policy** (3.171) and regulatory **requirements** (3.190)

707. **Security management programme** (ISO 22380): **process** (3.180) by which a **security management objective** (3.228) is achieved

708. **Security management target** (ISO 22380): specific level of **performance** (3.167) required to achieve a **security management objective** (3.228)

709. **Security operation** (ISO 22380): **activity** (3.1) and function related to the **protection** (3.182) of people, and tangible and intangible **assets** (3.10); Note 1 to entry: **Security** (3.223) operations can require the carrying and operating a weapon in the **performance** (3.167) of their duties; Note 2 to entry: The concept includes the International Code of Conduct (ICoC)[5] definition of security services: guarding and protection of people and **objects** (3.151), such as convoys, **facilities** (3.90), designated sites, property or other places (whether armed or unarmed) or any other activity for which the **personnel** (3.169) of companies are required to carry or operate a weapon in the performance of their duties.

710. **Security operations objective** (ISO 22380): **objective** (3.153) sought, or aimed for, related to **security operations** (3.232); Note 1 to entry: Security operations objectives are generally based on the **organization's**(3.158)**security operations policy** (3.236); Note 2 to entry: Security operations objectives are generally specified for relevant functions and levels in the organization.

711. **Security plan** (ISO 22380): planned arrangements for ensuring that **security** (3.223) is adequately managed; Note 1 to entry: It is designed to ensure the application of measures that protect the **organization**(3.158) from a **security** (3.223)**incident** (3.111); Note 2 to entry: The plan can be incorporated into other operational plans.

712. **Security sensitive information, security sensitive material** (ISO 22380): **information** (3.116) or material, produced by or incorporated into the **supply chain** (3.251) security **process** (3.180), that contains information about the **security** (3.223) processes, shipments or government directives that would not be readily available to the public and would be useful to someone wishing to initiate a security incident

713. **Security threat scenario** (ISO 22380): means by which a potential **security** (3.223)**incident** (3.111) can occur.

714. **Sensitive information** (ISO 22380): **information** (3.116) that is protected from public disclosure only because it would have an adverse effect on an **organization** (3.158), national **security** (3.223) or public safety

715. **Severity (FSMA-PC Guide):** The seriousness of the effects of a hazard.

716. **Shadow Economy (Black's law):** Collectively, the unregistered economic activities that contribute to a country's gross national product. A shadow economy may involve legal or illegal production of goods and services, including gambling, prostitution, and drug-dealing, as well as barter transactions and unreported incomes. –Also termed "black economy"; "black market"; "Underground Economy".

717. **Significant food safety hazard** (ISO 22000): **food safety hazard** (3.22), identified through the hazard assessment, which needs to be controlled by **control measures** (3.8)

718. **Significantly minimize (FSMA-PC Guide):** To reduce to an acceptable level, including to eliminate.

719. **Simulation (Black's law):** 1. An assumption of an appearance that is feigned, false, or deceptive. 2. Civil law; a feigned, pretended act, usually to mislead or deceive.

720. **Smuggled Foods (FDA, FSMA, US CODE):** In this subsection, the term ''smuggled food'' means any food that a person introduces into the United States through fraudulent means or with the intent to defraud or mislead.

721. **Spent, partially spent or exhausted material (ASTA1):** "Spent, partially spent or exhausted material is the by-product of essential oil or oleoresin production. By-products may have had a valuable constituent, such as color removed or have lost their intrinsic bioactive characteristics completely or partially depending on the extraction method applied."
722. **Stability** (ISO Guide 30): <of a reference material (RM)> characteristic of a reference material, when stored under specified conditions, to maintain a specified property value within specified limits for a specified period of time; Note 1 to entry: See also the IUPAC Compendium of Analytical Nomenclature.[5]
723. **Stand-alone authentication tool** (ISO 22380): **authentication tool** (3.20) that is either used to reveal a covert **authentication element** (3.17) to the human senses for human **verification** (3.272) or that integrates the functions required to be able to verify the authentication element independently
724. **Standard (GFSI):** A normative document and other defined normative documents, established by consensus and approved by a body that provide, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.
725. **Standardization (ASTA1):** "See Definition for 'Blending/Mixing" [paraphrased is blending or mixing spcies to achieve a consistent color and/or flavor] [Note: this is different than a standardized test method such as from ISO, ASTM, etc.]
726. **Standardization (DNI):** Activity of establishing, with regard to actual or potential problems, provisions for common and repeated use, aimed at the achievement of the optimum degree of order in a given context. NOTE 1: In particular, the activity consists of the processes of formulating, issuing and implementing standards. NOTE 2: Important benefits of standardization are improvement of the suitability of products, processes and services for their intended purposes, prevention of barriers to trade and facilitation of technological cooperation.
727. **Standardized numerical identifier (DSCSA):** The term `standardized numerical identifier' means a set of numbers or characters used to uniquely identify each package or homogenous case that is composed of the National Drug Code that corresponds to the specific product (including the particular package configuration) combined with a unique alphanumeric serial number of up to 20 characters.
728. **Statute (Black's Law):** A law passed by a legislative body; specifically legislation enacted by any lawmaking body, including legislatures, administrative boards, and municipal courts. The term "act" is interchangeable as a synonym.
729. **Statute, Criminal (Black's Law):** 1. an act that defines, classifies, and sets forth punishment for one or more specific crimes. See Penal Code.
730. **Statute, Penal (Black's Law):** A law that defines an offense and prescribes its corresponding fine, penalty, or punishment. – Also termed penal law; punitive statute.
731. **Substandard (WHO IMPACT)**: also called "out of specification", these are authorized medical products that fail to meet either their quality standards or specifications, or both.
732. **Substitution (in the context of food fraud) (CEN):** The process of replacing a nutrient, an ingredient or part of a food with high value, with another nutrient, ingredient or part of food with lower value; Note 1 to entry: Substitution is a type of food product adulteration.
733. **Suppliers (GMA BP):** are businesses that sell raw materials and parts for products and the related packaging to manufacturers.
734. **Supply chain** (ISO 22380): two-way relationship of **organizations** (3.158), people, **processes** (3.180), logistics, **information**(3.116), technology and **resources** (3.193) engaged in **activities** (3.1) and creating value from the sourcing of materials through the delivery of **products or services** (3.181)

735. **Supply chain continuity management, SCCM** (ISO 22380): application of **business continuity management** (3.25) to a **supply chain** (3.251); Note 1 to entry: Business continuity management should be applied to all the tiers of an **organization's** (3.158) supply chain; Note 2 to entry: In practice, an organization usually would only apply it to the first tier of their suppliers and influence critical suppliers to apply SCCM to their suppliers.
736. **Supply Chain Control/ Supply-chain-applied control (FDA, FSMA, CFR):** Supply chain control means a preventive control for a hazard in a raw material or other ingredient when the hazard in the raw material or other ingredient is controlled before its receipt.
737. **Suspect product, suspicious product (DSCSA):** The term `suspect product' means a product for which there is reason to believe that such product: (A) is potentially counterfeit, diverted, or stolen; (B) is potentially intentionally adulterated such that the product would result in serious adverse health consequences or death to humans; (C) is potentially the subject of a fraudulent transaction; or (D) appears otherwise unfit for distribution such that the product would result in serious adverse health consequences or death to humans.
738. **Suspension (GFSI v7.2, Glossary):** The process by which a scheme is temporarily not recognised by GFSI." (Comment- for example if a standard or scheme does not address all aspects of the GFSI Guidance Document.)
739. **Syntactic interoperability** (ISO 22380): ability of two or more systems or services to exchange structured **information** (3.116)
740. **System Orchestrator (NIST2):** Organization or entity that defines and integrates the required data transformations components into an operational vertical system.
741. **TACCP – Threat Assessment and Critical Control Point plan (PAS96:2010): "**systematic management of risks through the process of assessment of threats, identification of vulnerabilities, and implementation of controls to raw materials, packaging, finished products, processes, premises, distribution networks and business systems by a knowledgeable and trusted team with the authority to implement changes to procedures; Also: It is the systematic assessment of threats, examination of processes to identify vulnerable points, and implementation of remedial action to improve resilience against malicious attacks by individuals or groups; And later: This PAS identifies three generic threats to food and drink: 1. Malicious contamination with toxic materials causing ill-health and even death; 2. Sabotage of the supply chain leading to food shortage; 3. Misuse of food and drink materials for terrorist or criminal purposes."
742. **TACCP – Threat Assessment and Critical Control Point plan (PAS96:2014): "**systematic management of risk through the evaluation of threats, identification of vulnerabilities, and implementation of controls to materials and products, purchasing, processes, premises, distribution networks and business systems by a knowledgeable and trusted team with the authority to implement changes to procedures (Comment- same as PAS96:2010); Deliberate acts against food and food supply take several forms. Clause 3 describes the characteristics of the main threats to food authenticity and safety – economically motivated adulteration (EMA) and malicious contamination, and outlines the nature of other threats." (Comment- expanded from PAS:2010 to include economically motivated adulteration) (see EMA-PAS96 definition)
743. **TACCP (GFSI/ FFTT, 2014):** prevention of intentional adulteration, ideologically motivated. One of three components under the GFSI Food Safety Management system which includes HACCP, TACCP, and VACCP. Comment- Food Defense assessments referring to "threats." This is similar to previous the PAS 96 TACCP plan addressing traditional Food Defense incidents.
744. **Tamper evidence** (ISO 22380): ability of the **authentication element** (3.17) to show that the **material good** (3.139) has been compromised.

745. **Target** (ISO 22380): detailed **performance** (3.167)**requirement** (3.190), applicable to an **organization** (3.158) or parts thereof, that arises from the **objectives** (3.153) and that needs to be set and met in order to achieve those objectives
746. **Tariffication (WTO):** Procedures relating to the agricultural market-access provision in which all non-tariff measures are converted into tariffs.
747. **Tariffs (WTO):** Customs duties on merchandise imports. Levied either on an ad valorem basis (percentage of value) or on a specific basis (e.g. $7 per 100 kgs.). Tariffs give price advantage to similar locally-produced goods and raise revenues for the government.
748. **Technical barriers to trade, TBT (WTO):** Regulations, standards, testing and certification procedures, which could obstruct trade. The WTO's TBT Agreement aims to ensure that these do not create unnecessary obstacles.
749. **Terrorism, Agroterrorist act (US CODE):** The term "agroterrorist act" means an act that- (A) causes or attempts to cause- (i) damage to agriculture; or (ii) injury to a person associated with agriculture; and (B) is committed or appears to be committed with the intent to- (i) intimidate or coerce a civilian population; or (ii) disrupt the agricultural industry in order to influence the policy of a government by intimidation or coercion (7 USC 8901)
750. **Test** (ISO 22380): unique and particular type of **exercise** (3.83), which incorporates an expectation of a pass or fail element within the aim or **objectives** (3.153) of the exercise being planned; Note 1 to entry: The terms "test" and "**testing** (3.258)" are not the same as "exercise" and "exercising".
751. **Testing** (ISO 22380): **procedure** (3.179) for **evaluation** (3.81); a means of determining the presence, quality or veracity of something; Note 1 to entry: Testing may be referred to as a "trial"; Note 2 to entry: Testing is often applied to supporting plans.
752. **Threat (DHS Lexicon 2017):** natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
753. **Threat (DNI):** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [Note: future step to review vs. traditional food industry definition of hazard.]
754. **Threat** (ISO 22380): potential cause of an unwanted **incident** (3.111), which may result in harm to individuals, **assets**(3.10), a system or **organization** (3.158), the environment or the **community** (3.42)
755. **Threat (SQF):** An identified risk that has the potential, if not controlled, to affect the quality of a product.
756. **Threat : "…** is the cause of an unwanted event that includes generally known variables or attributes of the source of the negative consequence ("threat source") (ISO 2012, ISO 2002, 21 CFR 121, ANSI 2009, PAS96 2014, FSMA 2016, NIST 2002, CNSSI 2010, UNODC 2010, DHS 2013) – this includes incident, hazard, damaging potential, etc. In crime and security science this is often a person(s) who have the intent and capability to cause harm. This is often applied to intentional acts with the intent to harm. The result of a threat assessment is usually a quantitative probability that the event to occur – but not an assessment of the consequence." (Spink, Ortega, Chen & Wu, 2017)
757. **Threat Agent (DNI):** A means or method used to exploit a vulnerability in a system, operation, or facility.
758. **Threat Analysis (DNI):** A project to identify the threats that exist over key information and information technology. The threat analysis usually also defines the level of the threat and likelihood of that threat to materialize.

759. **Threat analysis** (ISO 22380): **process** (3.180) of identifying, qualifying and quantifying the potential cause of an unwanted **event**(3.82), which may result in harm to individuals, **assets** (3.10), a system or **organization** (3.158), the environment, or the **community** (3.42)

760. **Threat Assessment (DNI):** Process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

761. **Threat Source (DNI):** The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with Threat Agent.

762. **Tier 1 supplier** (ISO 22380): provider of **products or services** (3.181) directly to an **organization** (3.158) usually through a contractual arrangement.

763. **Tier 2 supplier** (ISO 22380): provider of **products or services** (3.181) indirectly to an **organization** (3.158) through a **tier 1 supplier** (3.261).

764. **Top management, resource-allocation decision-maker (ISO 22380):** person or group of people who directs and controls an **organization** (3.158) at the highest level; Note 1 to entry: Top management has the power to delegate authority and provide **resources** (3.193)within the organization; Note 2 to entry: If the scope of the **management system** (3.137) covers only part of an organization, then top management refers to those who direct and control that part of the organization; Note 3 to entry: For this purpose, an organization can be identified by reference to the scope of the implementation of a management system; Note 4 to entry: Top management may be referred to as the leadership of the organization; Note 5 to entry: Top management, especially in a large multinational **organization** (3.158), may not be personally involved as described in this document; however, top management accountability through the chain of command shall be manifest.

765. **Tort (Black's law):** 1. A civil wrong, other than breach of contract, for which a remedy may be obtained, usually in the form of damages; a breach of a duty that the law imposes on persons who stand in particular relation to one another. The branch of law dealing with such wrongs.

766. **Traceability** (ISO 22000): ability to follow the history, application, movement and location of an object through specified stage(s) of production, processing and distribution; Note 1 to entry: Movement can relate to the origin of the materials, processing history or distribution of the **food** (3.18); Note 2 to entry: An object can be a **product** (3.37), a material, a unit, equipment, a service, etc.

767. **Track and trace** (ISO 22380): means of identifying every individual **material good** (3.139) or lot(s) or batch in order to know where it has been (track) and where it is (trace) in the supply chain.

768. **Trade Secret (Black's law):** 1. A formula, process, device, or other business information that is kept confidential to maintain an advantage over competitors; information – including formula, pattern, compilations, program, device, method, technique, or process – that (1) derives independent economic value, actual or potential, from not being generally known or readily ascertainable by others who can obtain economic value from its disclosure or use, and (2) is the subject of reasonable efforts, under the circumstances, to maintain its secrecy.

769. **Trade Secret (Protection of Undisclosed Information)** (TRIPs)**:** "Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices" (REF TRIPS). This generally protects "Formulas, patterns, compilations, programs, devices, methods, techniques or processes" and the duration is "As long as they remain secret" (REF USPTO).

770. **Trademark (Black's law):** 1. A word, phrase, logo, or other graphic symbol used by a manufacturer or seller to distinguish its product or products from those of others. The main purpose of a trademark is to designate the source of goods or services. In effect, the trademark is the commercial substitute for one's signature. To receive federal protection, a trademark must be

(1) distinctive rather than merely descriptive or generic; (2) affixed to a product that is actually sold in the marketplace; and (3) registered with the USPTO. in its broad sense, the term "trademark" includes "service mark". Unregistered trademarks are protected under common-law only, and distinguish with the mark "TM"." See Langham Act.

771. **Trademark (TRIPs):** "The owner of a registered trademark shall have the exclusive right to prevent all third parties not having the owner's consent from using in the course of trade identical or similar signs for goods or services which are identical or similar to those in respect of which the trademark is registered where such use would result in a likelihood of confusion" (REF TRIPS). This is "Any sign, or any combination of signs, capable of distinguishing the goods or services of one undertaking from those of other undertakings, shall be capable of constituting a trademark" (REF TRIPS). This generally protects "All of the above & logo, banner, sound, smell, etc." and the duration is "10-year terms with 10-year renewal terms" (REF USPTO).

772. **Tradename (Black's law):** Intellectual property. 1. A name, style, or symbol used to distinguish a company, partnership, or business (as opposed to a product or service); the name under which a business operates.

773. **Traders/Distributors (ASTA1):** "Businesses that take title of product for resale to others in the marketplace."

774. **Trafficking (Black's law):** The act of transporting, trading, or dealing, especially in people or illegal goods.

775. **Transaction information (DSCSA):** The term `transaction information' means: (A) the proprietary or established name or names of the product; (B) the strength and dosage form of the product; (C) the National Drug Code number of the product; (D) the container size; (E) the number of containers; (F) the lot number of the product; (G) the date of the transaction; (H) the date of the shipment, if more than 24 hours after the date of the transaction; (I) the business name and address of the person from whom ownership is being transferred; and (J) the business name and address of the person to whom ownership is being transferred.

776. **Transaction statement (DSCSA):** The `transaction statement' is a statement, in paper or electronic form, that the entity transferring ownership in a transaction: (A) is authorized as required under the Drug Supply Chain Security Act; (B) received the product from a person that is authorized as required under the Drug Supply Chain Security Act; (C) received transaction information and a transaction statement from the prior owner of the product, as required under section 582; (D) did not knowingly ship a suspect or illegitimate product; (E) had systems and processes in place to comply with verification requirements under section 582; (F) did not knowingly provide false transaction information; and (G) did not knowingly alter the transaction history.

777. **Transparency (DNI):** The ability of systems or components of systems to hide the details of their implementations from other client or server systems or components of systems.

778. **Transparency of practices (WTO):** Degree to which trade policies and practices, and the process by which they are established, are open and predictable.

779. **Transparent of meetings (WTO):** Sharing information, in this case so all members know what is happening in smaller group meetings. In WTO negotiations and other decision-making, ideas are tested and issues are discussed in a variety of meetings, many of them with only some members present. Members approve of this process so long as information is shared. They also want the process to ensure they can have input into it ("inclusive"). The final decision can only be taken by a formal meeting of the full membership. See also "concentric circles", "inclusive".

780. **Transportation stability** (ISO Guide 30): <of a reference material (RM)> stability of a reference material (RM) property for the time period and conditions encountered in transportation to the user of the RM; Note 1 to entry: Transportation stability has often been referred to as "short term stability".

781. **TRIPS (WTO):** Trade-Related Aspects of Intellectual Property Rights agreement
782. **Trust (DNI):** Reliance on the ability of a system or process to meet its specifications.
783. **Trusted query processing function, TQPF** (ISO 22380): function that provides a gateway to trusted verification function (TVF) (3.267) and attribute management data system (ADMS); Note 1 to entry: This includes software running locally on a hand-held device.
784. **Trusted verification function, TVF** (ISO 22380): function that verifies whether a unique identifier (UID) (3.269) received is valid or not and manages a response according to rules and access privileges
785. **Uncertainty (ERM/COSO):** is defined as "The inability to know in advance the exact likelihood of future events"
786. **Uncertainty (Imprecision) (Capra):** "on the other hand, refers to the magnitude of the scatter (ref capra).
787. **Unconscionability (Black's Law):** 1. Extreme unfairness. Unconscionability is normally expressed by an objective standard: (1) one party's lack of meaningful choice, and (2) contractual terms that unreasonably favor the other party. 2. The principle that a court may refuse o enforce a contract that is unfair or oppressive because of procedural abuses during contract formation or because of overreaching contractual terms, especially terms that are unreasonably favorable to on party by precluding meaningful choice for the other party. Because unconscionably depends on circumstances at the time the contract is formed, a later rise in market price is irrelevant.
788. **Unconscionable (Black's Law):** 1. (Of a person) having no conscience; unscrupulous <an unconscionable used-car salesman>. 2. (Of an act or transaction) showing no regard for conscience; affronting the sense of justice, decency, or reasonableness
789. **Unconscionable Agreement (Black's Law):** An agreement that no promisor with any sense, and not under a delusion, would make, and that no honest and fair promise would accept.
790. **Unconscionable Bargain (Black's Law):** See unconscionable agreement under agreement
791. **Underground economy (Black's law):** See "Shadow Economy" or "Black Market."
792. **Undesirable event** (ISO 22380): occurrence or change that has the potential to cause loss of life, harm to tangible or intangible **assets**(3.10), or negatively **impact** (3.107) the human rights and fundamental freedoms of internal or external **interested parties** (3.124)
793. **Unfit for human consumption (GFSI v7.2, Glossary):** Food which is unacceptable for human consumption, according to its intended use, for reasons of contamination, whether by extraneous matter or otherwise, or through putrefaction, deterioration or decay.
794. **Unique identifier, UID** (ISO 22380): code that represents a single and specific set of attributes that are related to an **object** (3.151) or class of objects during its life within a particular domain and scope of an object **identification** (3.104) system
795. **Unregistered/unlicensed medical products (WHO IMPACT):** that have not undergone evaluation and/or approval by the National or Regional Regulatory Authority for the market in which they are marketed/distributed or used, subject to permitted conditions under national or regional regulation and legislation.
796. **Unsafe Food (Food safety requirements) (Eu178/2002):** See Safe Food.
797. **Upstream** (ISO 22380): handling, processing and movement of **goods** (3.98) that occurs before the **organization in the supply chain** (3.159) takes **custody** (3.68) of the goods.
798. **USC (U.S.C, US Code):** The United States Code is a consolidation and codification by subject matter of the general and permanent laws of the United States. It is prepared by the Office of the Law Revision Counsel of the United States House of Representatives.
799. **VACCP – Vulnerability Assessment and Critical Control Point plan (0 Summary):** Food Fraud assessments focusing on "vulnerabilities" rather than "risks." This provides a consistent nomenclature for referring to the different assessments.

800. **VACCP (GFSI/ FFTT, 2014):** prevention of intentional adulteration, economically motivated. One of three components under the GFSI Food Safety Management system which includes HACCP, TACCP, and VACCP.

801. **Validation (FDA, FSMA, CFR):** means obtaining and evaluating scientific and technical evidence that a control measure, combination of control measures, or the food safety plan as a whole, when properly implemented, is capable of effectively controlling the identified hazards.

802. **Validation** (ISO 22000): <food safety> obtaining evidence that a **control measure** (3.8) (or combination of control measures) will be capable of effectively controlling the **significant food safety hazard** (3.40); Note 1 to entry: Validation is performed at the time a control measure combination is designed, or whenever changes are made to the implemented control measures; Note 2 to entry: Distinctions are made in this document between the terms **validation** (3.44), **monitoring** (3.27) and **verification**(3.45): — validation is applied prior to an activity and provides information about the capability to deliver intended results; — monitoring is applied during an activity and provides information for action within a specified time frame; — verification is applied after an activity and provides information for confirmation of conformity.

803. **Validation FSMA Guide):** Obtaining and evaluating scientific and technical evidence that a control measure, combination of control measures, or the food safety plan as a whole, when properly implemented, is capable of effectively controlling the identified hazards.

804. **Value assignment** ((ISO Guide 30): process by which reference material (RM) property values or attributes obtained by characterization are combined and expressed in accompanying RM documentation

805. **Verification (FDA, FSMA, CFR):** means the application of methods, procedures, tests and other evaluations, in addition to monitoring, to determine whether a control measure or combination of control measures is or has been operating as intended and to establish the validity of the food safety plan.

806. **Verification (FSMA-PC Guide):** The application of methods, procedures, tests and other evaluations, in addition to monitoring, to determine whether a control measure or combination of control measures is or has been operating as intended and to establish the validity of the food safety plan.

807. **Verification (GFSI):** A confirmation, through the review of objective evidence that requirements have been fulfilled.

808. **Verification** (ISO 22000): confirmation, through the provision of objective evidence, that specified **requirements** (3.38) have been fulfilled; Note 1 to entry: Distinctions are made in this document between the terms **validation** (3.44), **monitoring** (3.27) and **verification** (3.45): — validation is applied prior to an activity and provides information about the capability to deliver intended results; — monitoring is applied during an activity and provides information for action within a specified time frame; — verification is applied after an activity and provides information for confirmation of conformity.

809. **Verification** (ISO 22380): confirmation, through the provision of objective evidence, that specified **requirements** (3.190) have been fulfilled

810. **Verification or verify (DSCSA):** The term `verification' or `verify' means determining whether the product identifier affixed to, or imprinted upon, a package or homogeneous case corresponds to the standardized numerical identifier or lot number and expiration date assigned to the product by the manufacturer or the repackager, as applicable in accordance with section 582.

811. **Vulnerability (0 Summary): "…**is a weakness or flaw that creates opportunities for undesirable events related to the system ("system design") (ISO 2007a, ISO 2002, ISO 2012, DHS 2013, NIST 2011, CNSSI 2010, NRC 2009, COSO 2014, Merriam-Webster 2004). The result of a vulnerability assessment is usually a qualitative statement of the susceptibility of the system – this influence the

likelihood (NRC 2009). FSMA uses the term vulnerability specifically as it applies a vulnerability assessment to food defense (21CFR 121, 21 USC)." (Spink, Ortega, Chen & Wu, 2017)

812. **Vulnerability (DHS Lexicon 2017):** physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptive to a given hazard.
813. **Vulnerability (DNI):** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.
814. **Vulnerability Analysis (DNI):** The systematic examination of systems in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.
815. **Vulnerability Assessment (DNI):** Systematic examination of an information system (IS) or product to determine the adequacy of security measures identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [Source: ISM Handbook]
816. **Vulnerability, vulnerability analysis, vulnerability assessment** (ISO 22380): **process** (3.180) of identifying and quantifying something that creates susceptibility to a source of **risk**(3.199) that can lead to a **consequence** (3.46).
817. **Wholesalers (GMA BP):** are middlemen, a person or business that buys large quantities of products and resells to its distributors rather than to the ultimate consumer.
818. **Within-unit homogeneity** (ISO Guide 30): uniformity of a specified property value within each unit of a reference material
819. **Written Procedures (FDA, FSMA, CFR):** for receiving raw materials and other ingredients means written procedures to ensure that raw materials and other ingredients are received only from suppliers approved by the receiving facility (or, when necessary and appropriate, on a temporary basis from unapproved suppliers whose raw materials or other ingredients are subjected to adequate verification activities before acceptance for use).

Appendix: Additional Definitions

Table: Criminal types and attributes applicable (in Spink, Moyer, Park, & Heinonen 2013, (Spink et al., 2010) adapted from (Hagan, 2010)) [Note: as of August 2018 now published in ISO 22380]

Types of criminals	Definition
Recreational	Action for entertainment or amusement
Occasional	Infrequent, opportunistic
Occupational	Incidents at their place of employment either as an individual act or in collaboration with the company
Professional	Crime fully finances their lifestyle
Note: Not Ideological	A domestic or international terrorist who commits this act to has a motivation of economic gain. They would use the economic gain for another action that is to achieve a goal or to make an ideological statement.

Table: Food Fraud Types, Definitions, and Examples (adapted from (Spink, 2011; GFSI, 2014, 2017; SSAFE Organization, 2015; PWC, 2016; Spink, 2016) [Note: As of May 2018, published in the Appendix of the GFSI Food Fraud Technical Document and used as a reference of all types of fraud covered by GFSI.]

GFSI (1) Type of Food Fraud	Definition from SSAFE (2)	Examples from GFSI FFTT (3)	General Type of Food Fraud
Dilution	The process of mixing a liquid ingredient with high value with a liquid of lower value.	• Watered down products using non-potable / unsafe water • Olive oil diluted with potentially toxic tea tree oil	Adulterant-substance (Adulterant)
Substitution	The process of replacing an ingredient or part of the product of high value with another ingredient or part of the product of lower value.	• Sunflower oil partially substituted with mineral oil • Hydrolyzed leather protein in milk	Adulterant-substance or Tampering
Concealment	The process of hiding the low quality of a food ingredients or product.	• Poultry injected with hormones to conceal disease • Harmful food colouring applied to fresh fruit to cover defects	Adulterant-substance or Tampering
Unapproved enhancements	The process of adding unknown and undeclared materials to food products in order to enhance their quality attributes.	• Melamine added to enhance protein value • Use of unauthorized additives (Sudan dyes in spices)	Adulterant-substance or Tampering
Mislabelling/ Misbranding	The process of placing false claims on packaging for economic gain.	• Expiry, provenance (unsafe origin) • Toxic Japanese star anise labeled as Chinese star anise • Mislabeled recycled cooking oil	Tampering
Grey market production/ theft/diversion	Outside scope of SSAFE tool.	• Sale of excess unreported product, • Product allocated for the US market appearing in Korea	Over-run, Theft, or Diversion (4)
Counterfeiting	The process of copying the brand name, packaging concept, recipe, processing method etc. of food products for economic gain.	• Copies of popular foods not produced with acceptable safety assurances • Counterfeit chocolate bars	Counterfeiting

Notes:
(1) GFSI – Global Food Safety Initiative
(2) SSAFE – Safe Secure and Affordable Food For Everyone
(3) GFSI FFTT – Global Food Safety Initiative: Food Fraud Think Tank
(4): Gray Market -- a market employing irregular but not illegal methods; Theft -- something stolen; Diversion/ Parallel Trade -- the act or an instance of diverting straying from a course, activity, or use

Table: Types of Offender Organizations (Spink, Moyer, Park & Heinonen 2013)

Type of Offender Organization	Definition or Explanation
Individual/ Small Groups:	"Although there are IPR cases involving solo or small groups of individuals who operate out of their homes, garages, or small storage facilities, there is little reporting and no actual analysis of the relative importance of such operators to the threat. … This lack of reporting and analysis may be a reflection of the fact that individuals and small operations are a less attractive target for law enforcement than larger enterprises engaging in more significant infringing activity or also committing other more serious offenses."
General Criminal Enterprises (Members):	An example used to identify this group is "an Asian criminal enterprise of 30 defendants charged with smuggling into the United States counterfeit cigarettes worth approximately $40 million and other counterfeit goods, including pharmaceuticals worth several hundred thousand dollars."
Organized Crime Members (Members):	"Organized crime groups are a specialized subset of criminal enterprises that maintain their position through the use of actual or threatened violence, corrupt public officials, graft, or extortion. For example, members of the Lim Organization, an Asian organized crime group in New York, trafficked in counterfeit goods and were charged with attempted murder and conspiracy to commit murder." An aspect of deterring this group is the use of violence and the risk of retaliation to a company or investigators (e.g., violence or sabotage).
Terrorist Organizations (Supporters):	"Terrorist supporters have used intellectual property crime as one method to raise funds. Central to this judgment is the distinction between terrorist supporters who merely provide funding and resources to a terrorist organization versus terrorist organization members who engage in the actual terrorist activities of violence. … It is widely reported terrorist supporters may use IPR crimes to provide indirect financial support to terrorist organizations, but little current evidence suggests terrorists are engaging directly in IPR crimes to fund their activities." There are many confirmed cases of product counterfeiting funding terrorist acts. For example, it was confirmed that the 1993 World Trade Center bombing was partially funded by the sale of counterfeit products (FBI, 2008).
Gangs in the United States (Supporters):	"According to the National Gang Intelligence Center (NGIC), there are three subtypes of gangs: street gangs, prison gangs, and outlaw motorcycle gangs of these three groups, street gangs most often engage in and profit from IP theft, therefore this analysis focuses exclusively on this subtype."
Foreign Government Offenders:	The primary motivation in this offender group is the theft of sensitive United States information including trade secrets and economic espionage. There are examples of state-sponsored counterfeits of branded products.
Warez Groups:	"[A] less common motivation for committing IPR [infringement] is personal fame and notoriety. These individuals are often members of Warez groups, sophisticated and hierarchical criminal groups operating in the United States and abroad that specialize in distributing infringing movies, music, and software via the Internet."
Note: Members: The individual criminals may be acting alone but have known ties to the organization and participate in the illegal activities of the group. An example is a gang member who separately produces and sells counterfeit DVDs.	
Note: Sympathizers or supporters: These may agree with the ideology of a group and provide financial support to the criminal organization, but do not participate in the primary criminal activities of the organization. An example is a criminal who contributes funds to a terrorist organization but does not him or herself, commit terrorist acts.	

The Food Fraud Prevention Think Tank LLC will continue to inform global stakeholders as to the relationship between Food Fraud and Economically Motivated Adulteration, Food Crime, Food Integrity, and Food Authenticity **in order to encourage a global set of terms and definitions that are consistent.**

Note: The Food Fraud Prevention Think Tank LLC conducts a wide range of teaching, research and outreach projects. The "FFP Report" series was created to review specific emerging topics or recent laws, regulations, certifications, standards, or best practices. The summary and insight is not legal advice and is not intended to replace the counsel of a food law expert.

Contact Information: www.FoodFraudPrevention.com or www.FoodFraudMOOC.com