Reference: Spink, JohnF9hLtO4yfvaRzPLradS9ILwnkC5E2SU/edit?usp=sharing&ouid=106328742619920569986&rtpof=true&sd=true

Chapter 13: Cybersecurity

1 Overview of Cybersecurity (based on the NIST requirements and ISO 27000 Information Security & 27032 Cybersecurity) – includes an introduction to ISO 27000 & ISO 27032.
2 Detail of NIST requirements.
3 Cybersecurity in Iso 28000 supply chain security (the role of the SCM manager in Cybersecurity) – includes an introduction to ISO 28000.
4 Cybersecurity in ISO 22000 Food Safety Management (includes an introduction to ISO 22000).
5 Summary and Call to Action
6 References

////

Chapter 13 – Section 4: Cybersecurity in ISO 22000 Food Safety Management

Since first published in 2015, Iso 22000 has been the foundational standard for food safety management. The most widely adopted requirements are based on the Global Food Safety Initiative (GFSI) benchmark built upon ISO 22000. In 2018 the ISO 22000 standard was updated to acknowledge "external issues," including "cybersecurity and food fraud." But what is "cybersecurity"? Why is cybersecurity included in the same concept as food fraud? Do they intend to present two separate topics of "cybersecurity" and separately "food fraud" or both together in "cybersecurity and food fraud"? Does it matter?

This review will focus on the cybersecurity part of the question. Let's start with some basics questions:

For ISO 22000 Food Safety Management:

- What is the scope?
- What is the definition of food safety (and related terms)?
- What is the cybersecurity requirement?
- How formal or direct is the cybersecurity requirement?
- What is the definition of cybersecurity (and food fraud)?

- What is the compliance role of a Food Safety Management system in Cybersecurity?

What is ISO 22000, including the scope?

To gain insight into applying a term used in a standard, it is essential to understand the overall focus. *The scope is on preventing or managing food safety hazards – situations that, if left unchecked, could lead to public health harm.*

- "Introduction - 0.2, FSMS principles: Food safety is related to the presence of food safety hazards at the time of consumption (intake by the consumer). Food safety hazards can occur at any stage of the food chain. Therefore, adequate control throughout the food chain is essential."

Also, ISO 22000 takes a Hazard Analysis, and Critical Control Point plan (HACCP) focused on operational processes. This is combined with acknowledging other activities such as Pre-Requisite Programs (PRPs), as included in ISO 22002. *The scope includes activities within the food operations or related internal or external activities.*

- "Introduction - 0.3.3.3 Hazard analysis — Operational processes: The concept of risk-based thinking based on the HACCP principles at the operational level is implicit in this document. The subsequent steps in HACCP can be considered as the necessary measures to prevent hazards or reduce hazards to acceptable levels to ensure food is safe at the time of consumption."

What is the ISO 22000 definition of food safety (and related terms)?

The standard includes defining foods safety, food safety hazard, significant food safety hazard, and acceptable level. *The scope is on hazards that occur during the intended use of the food that exceeds the acceptable level and thus is determined to be a significant food safety hazard.*

- "3.21 Food Safety: 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."
  "3.22 Food Safety Hazard: biological, chemical or physical agent in food with the potential to cause an adverse health effect."
- "3.40 Significant Food Safety Hazard: food safety hazard, identified through the hazard assessment, which needs to be controlled by control measures; Note 1 to entry: The term "hazard" is not to be confused with the term "risk" 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."

- "3.1 Acceptable Level: level of a food safety hazard not to be exceeded in the end product provided by the organization."
- Note: careful reading of these definitions clarifies the use of "hazard" and "risk" that may be different than used by many food safety professionals. Risk is often used to mean anything bad and unacceptable, but that is an overstatement. This definition of hazard and risk is consistent with other ISO standards such as ISO 31000 Risk Management. Some risks are not a hazard. Some hazards are not so bad that they must be mitigated or prevented. A food safety professional might say "all risk is unacceptable" when they are referring to "all significant food safety hazards are unacceptable."

What is the cybersecurity requirement for ISO 22000 compliance?

The overall scope of ISO 22000:2018 is presented in the "4.1 Understanding the organization and its context." *The scope includes anything that could lead to a food safety-based adverse health effect.*

- "The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended results of its food safety management system. The organization shall identify, review and update information related to these external and internal issues."

Then Section 4.1, Note 1 clearly defines food fraud within the scope of the standard. *The standard only mentions the term once and only in a "note."*

- "Understanding the context can be facilitated by considering external and internal issues including but not limited to legal, technological, competitive, market, cultural, social, economic environments, **cybersecurity,** and ***food fraud***, food defence and intentional contamination, knowledge, and performance of the organization, whether international, national, regional or local."

How formal or direct are the cybersecurity requirements?

There are no further details or explicit compliance requirements.

What is the definition of cybersecurity (and food fraud)?

Iso 22000 does not have a definition of cybersecurity. Iso 22000 also does not have a definition of food fraud.

To understand the use of these terms, it is helpful to review other ISO standards. There are directly applicable standards such as ISO 27032 Information technology Security techniques — Guidelines for cybersecurity. (ref)

- **Cybercrime** (ISO 27032, 4.18): a criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime.
- **Cybersafety** (ISO 27032, 4.19): condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational, or other types or consequences of failure, damage, error, accidents, harm, or any other event in the Cyberspace which could be considered non-desirable. (Note 1 to entry: This can take the form of being protected from the event or from exposure to something that causes health or economic losses. It can include protecting people or assets; Note 2 to entry: Safety, in general, is also defined as the state of being certain that adverse effects will not be caused by some agent under defined conditions.)
- **Cybersecurity** or **Cyberspace Security** (ISO 27031, 4.20): preservation of confidentiality, integrity, and availability of information in the Cyberspace. (Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability, can also be involved; Note 2 to entry: Adapted from the definition for information security in ISO/IEC 27000:2009.) (See sidebar on ISO 27000 related terms.)
- **the Cyberspace** (ISO 27031, 4.21): complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form

Since ISO 22000 presents the topic in the phrase “cybersecurity and food fraud,” both terms will be reviewed. ISO 22000 only mentions food fraud once, and there is no definition or further guidance. A related term of “product fraud” is defined in ISO 22380:2018 Security and resilience — Authenticity, integrity, and trust for products and documents — General principles for product fraud risk and countermeasures. The only mention of food fraud in an ISO standard, other than ISO 22000, is in a reference for ISO 22380 (citing “Spink J. Moyer D.C. Defining the Public Health Threat of Food Fraud. Journal of Food Science, 2011, 75 (9), pp. 57”). *The ISO definition of food fraud can be derived from product fraud. Other than some aspects of product fraud being enabled by electronic communication, the ISO definitions of cybersecurity and food fraud have no overlaps and are fundamentally different concepts that are only barely related.*

- **Product Fraud** (ISO 22380, 3.1): wrongful or criminal deception that utilizes material goods for financial or personal gain (Note 1 to entry: Fraud means wrongful or criminal deception intended to result in a financial or personal gain that creates social or economic harm; Note 2 to entry: Products include electronic media carried on material goods; Note 3 to entry: Fraud related to digitally transmitted electronic media shall be considered separately.)

/Sidebar: Start/

Sidebar: ISO 27000 definitions of terms related to information security

- **Information Security** (ISO 27000, 3.28): preservation of confidentiality (3.10), integrity (3.36) and availability (3.7) of information (Note 1 to entry: In addition, other properties, such as authenticity (3.6), accountability, non-repudiation (3.48), and reliability (3.55) can also be involved.)
- **Information Security Continuity** (ISO 27000, 3.29): processes (3.54) and procedures for ensuring continued information security (3.28) operations.
- **Information Security Event** (ISO 27000, 3.30): identified occurrence of a system, service, or network state indicating a possible breach of information security (3.28) policy (3.53) or failure of controls (3.14), or a previously unknown situation that can be security-relevant.
- **Information Security Incident** (ISO 27000, 3.31): single or a series of unwanted or unexpected information security events (3.30) that have a significant probability of compromising business operations and threatening information security (3.28)
- **Information Security Incident Management** (ISO 27000, 3.32): set of processes (3.54) for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents (3.31)
- **External Context** (ISO 27000, 3.22): external environment in which the organization seeks to achieve its objectives (3.49). (Note 1 to entry: External context can include the following: the cultural, social, political, legal, regulatory, financial, technological, economic, natural, and competitive environment, whether international, national, regional, or local; key drivers and trends having an impact on the objectives of the organization (3.50); relationships with, and perceptions and values of, external stakeholders (3.37). [SOURCE: ISO Guide 73:2009, 3.3.1.1]
- **Management System** (ISO 27000, 3.41): set of interrelated or interacting elements of an organization (3.50) to establish policies (3.53) and objectives (3.49) and processes (3.54) to achieve those objectives. (Note 1 to entry: A management system can address a single discipline or several disciplines.; Note 2 to entry: The system elements include the organization's structure, roles, and responsibilities, planning and operation; Note 3 to entry: The scope of a management

system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.)

/Sidebar End/

What is the compliance role of a Food Safety Management system in Cybersecurity?

ISO 22000 does require "Understanding the context can be facilitated by considering external and internal issues including but not limited to… cybersecurity and food fraud, …" for compliance. With no further details or guidance in ISO 22000, the scope can be identified in other ISO standards. The food safety management system requirement for cybersecurity can be derived from ISO 27000 Information Security and ISO 22380 Security and resilience — Authenticity, integrity, and trust for products and documents — General principles for product fraud risk and countermeasures.

CONCLUSION

The Key is "accountable" versus "responsible."

1. Accountable: you are to confirm your company meets ISO 22000
2. Accountable: for explaining to IT/ Cyber your Critical Information Infrastructure Protection (CIIP) and Critical Infrastructure Protection (CIP)
3. Not Responsible: IT/ Cyber is tasked with selecting and implementing the processes across the entire enterprise – this leads to a harmonized and coordinated approach that levels the enterprise-wide risk tolerance.
4. Responsible: that your team follows the IT/ cyber requirements such as updates and registering all ICT equipment.
5. **Interim Conclusion for a Food Safety Manager (From NIST, ISO 27000, ISO 27032):**
    a. **You are NOT accountable or responsible for conducting IT/ cybersecurity assessments or selecting/ implementing/ managing those systems.**
    b. **You ARE accountable for sharing your expert, functional-area insight on critical infrastructure protection (what processes are the most vulnerable, and why) – AND assuring your system is secured.**
    c. **You ARE accountable to make sure you are meeting the FSMA and GFSI requirements for considering all hazards including those of cybersecurity and e-commerce.**

/END/