Chapter 15
Risk Analysis (Part 1 of 3): Basic Fundamentals

Summary

This chapter presents risk assessment and the broader concept of risk analysis. This chapter will introduce the foundational concepts as well as general applications, review key issues such as hazard identification, risk assessment, risk management, and risk communication. In addition this will include the information used to conduct the assessments such as data analytics ("Big Data") as it relates to decision-making and the role in food fraud prevention.

The Key Learning Objectives of this chapter are

- (1) **Fundamentals:** Understand the fundamentals of risk analysis that apply to food fraud.
- (2) **Adaptation to Food Fraud:** Understand how those fundamentals are adapted to the unique attributes of the variables.
- (3) **Tools and Models:** Finally, understand current tools or models.

On the Food Fraud Prevention Cycle (FFPC), this chapter addresses the "(0) Fundamental Concepts" beyond what is risk analysis to the details of risk assessment as applied to food fraud prevention (Fig. 15.1).

Introduction

Risk assessment is a specific function within the concept of risk analysis. The entire process includes gathering information and processing it into a useful and reliable form. The fraud opportunity for food—and more generally to all product fraud—is unique and adds multiple layers of complexity. That is, there are multiple systems that interact to increase the complexity of the problem and sophistication needed to put efficient and effective countermeasures and control systems in place. For example, food safety risk assessment deals with a specific set of hazards and variables. Traditional supply chain management looks within finite systems and deals with a

J. W. Spink, *Food Fraud Prevention*, Food Microbiology and Food Safety,
https://doi.org/10.1007/978-1-4939-9621-6_15

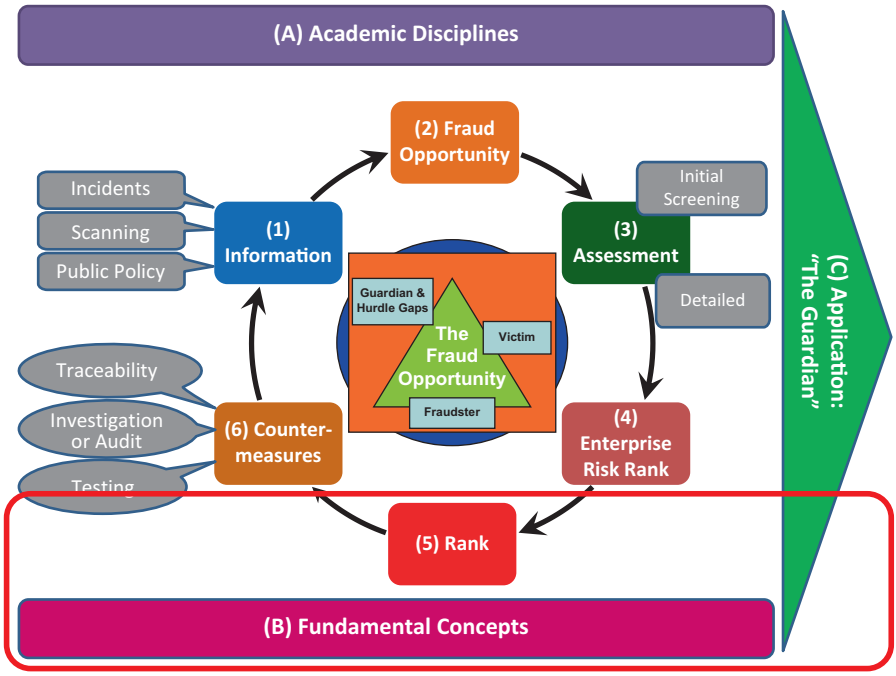

Fig. 15.1 Food Fraud Prevention Cycle—where this chapter applies to the overall concept: "(B) Fundamental Concepts" and "(5) Risk". (Copyright Permission Granted) (Spink 2014; Spink et al. 2019)

different set of variables. To consider the root cause—the human adversaries—this adds a new set of variables from criminology. Then, when decision sciences apply all the variables, the complexity expands again.

In general, the risk analysis and basic assessment concepts are essential for food fraud prevention because:

- Foundation: There needs to be an underlying foundation to understand and evaluate the vulnerability.
- Value of Information: Without a deeper understanding of the usefulness of the information, subsequent assessments could be misleading or false.
- Unique Considerations: There are unique considerations that must be defined before even considering modeling. These include risk versus vulnerability and mitigation versus prevention.
- Share Best Practices: Finally, rather than starting with a novel approach, it is best to adapt other currently implemented systems to food fraud prevention.

This chapter is a key component in the theoretical foundation of food fraud prevention.

Key Learning Objective 1: Introduction to Risk

This section reviews the fundamentals of risk analysis, the concepts such as risk versus vulnerability, and then the founding discipline of decision sciences.

The Key Learning Objectives of this section are

- (1) Risk analysis
- (2) Review of terminology
- (3) Review of the many types of risks

Introduction to Risk Analysis

The overall risk analysis is not a quantitative analytical number or value—through a specific tool could present a ranking for a specific question—but judgement of "what could happen, how likely it is to happen, and what the consequences are if it does happen" (Kaplan 1997; CFSAN 2002, 2003; FDA 2003; CFSAN 2005; CBER 2006; CFSAN/FDA 2007). Risk analysis consists of four concepts including hazard identification, risk assessment, risk management, and risk communication (Figs. 15.2 and 15.3). This is a cycle that is constantly in motion and continually adjusted.

A significant challenge for starting risk analysis for a new type of risk such as food fraud is breaking from a current paradigm and standard scope and method (e.g., a traditional food safety risk assessment or a traditional crime assessment). New risks are initially attempted to be addressed, logically, by currently implemented

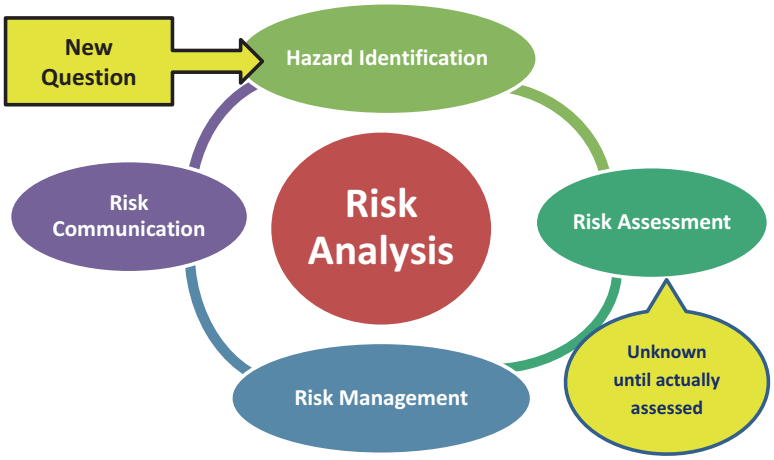

Fig. 15.2 Risk analysis cycle including hazard identification, risk assessment, risk management, and risk communication

Fig. 15.3 Hierarchy of information and response: suspicious activity/question, problem, vulnerability, risk, and hazard

systems. These previous systems address them until it is proven a new paradigm is needed.

As there is more awareness of novel or evolving risks, the old methods may become ill-fitting tools. When a new topic is addressed, there is often a lack of historical data or even a lack of knowledge of how the information will be used (Cruz 2002; Van Der Fels-Klerx et al. 2002). "A common challenge faced in risk assessment is a lack of appropriate historical data, a basic lack of knowledge important in decision-making and data that is not yet available" (Spink 2009). Also, "One common method used for taking the first step is peer consultation or expert panels" (Spink 2009). Peer consultation has been standardized in the "Delphi Method" which was originally developed by the RAND Corporation after World War II (RAND 2018).

A danger when dealing with new or emerging risks is that the previous methods—and even the assumptions about the availability of the "right" data—no longer apply. Underlying issues include understanding the nature of risk, uncertainty, and vulnerability.

For food fraud prevention, the entire cycle should be understood as well as the challenge of including a new hazard as well as new needs for data collection.

Introduction to Risk and Vulnerability: Foundational Terms

While it seems very simplistic to provide definitions for the most basic concepts, it has been determined by experience as a critical first step when addressing food fraud. Often there are different definitions—often unknowingly—applied. There is an expectation that "everyone" knows what that word means. While you may not agree with the exact definition provided, you at least can clearly see how the term is being used.

A first consideration is how do we refer to new information or concerns. Criminology has a logical starting point with a consideration that it applies to all responses not just the actions or responsibilities of the police (Clarke and Eck 2005):

- **Problem:** "…the basic unit of police works rather than a crime, a case, calls, or incidents. A problem is something that concerns or causes harm to citizens, not just the police. […] Addressing problems means more than quick fixes: it means dealing with conditions that create problems" (Goldstein 1990).

These next definitions are from a previous research project was conducted on the definition and scope of several key terms (see that article for full citation details that are within the quoted sections) (Spink et al. 2017):

- **Event:** "An event is essentially something that occurs (summarizing: ISO31000; CNSSI 2010; Merriam-Webster 2004). There is no evaluation yet of the change in the consequence."
- **Incident:** "A type of event is an incident that has occurred and evaluated, and that could have a negative consequence (DHS 2008; ANSI 2009; CNSSI 2010)."
- **Vulnerability:** "[A] weakness or flaw that creates opportunities for undesirable events related to the system ("system design") (ISO 2007a; ISO 2002, 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 e this influence the likelihood (NRC 2009)."
- **Risk:** "Risk 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 2014, 21 CFR 50 (A) (.3)(k), Merriam-Webster 2004)."
- **Hazard:** "Also, a hazard 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. A new note to add is that the US FDA further defines an unacceptable level of protection as a "hazard that requires a preventive control" (FDA 2015) (for more on the appropriate level of protection see (WTO 1995; CODEX 2003))."
- **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; PAS 96 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."

- **Mitigation:** "…is intended to reduce the consequence of the event (ISO 2007a, b; ISO 2007; 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."
- **Prevention:** "…is intended to reduce or eliminate the likelihood of the event occurring (ISO 2007; ISO 2007a, b; ISO 2008; Merriam-Webster 2004). This focuses on identifying and eliminating or reducing vulnerability."

Building on these definitions and applying to food fraud (Spink et al. 2017):

- **Food fraud vulnerability:** "…is the susceptibility of a system to food fraud (e.g., milk is not tested for adulterants such as water).
- **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."
- **Food fraud risk:** "…is the combined likelihood and consequence e that considers the threat and vulnerability e of food fraud. This is a function of the vulnerability and threat; e.g., an estimate of the likelihood and vulnerability and threat; e.g., an estimate of the likelihood and consequence of milk diluted with water, sold to a deceived customer."

From this review of definitions, there is more clarity on the current activities (focus on risk and mitigation) and the ideal future state (focus on vulnerability and prevention).

Other related terms defined in ISO 31000 include (ISO 2009):

- **Control:** "measure that is modifying."
  - "Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk."
  - "Note 2 to entry: Controls may not always exert the intended or assumed modifying effect."
- **Probability:** "measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty."
- **Frequency:** "number of events or outcomes per defined unit of time."
  - "Note 1 to entry: Frequency can be applied to past events or to potential future events, where it can be used as a measure of likelihood/probability."

When focusing on how to address risks and determine "how much is enough" for countermeasures and control systems, ISO 31000 Risk Management presents several key concepts (ISO 2018):

Addressing risk perception (ISO 2018):

- **Residual risk:** risk (2.1) remaining after risk treatment (2.25) [SOURCE: ISO Guide 73:2009, definition 3.8.1.6]
- **Risk acceptance:** informed decision to take a particular risk (1.1) [ISO Guide 73]; Note 1 to entry: Risk acceptance can occur without risk treatment (3.8.1) or

during the process of risk treatment; Note 2 to entry: Accepted risks are subject to monitoring (3.8.2.1) and review (3.8.2.2).
- **Risk aggregation:** a combination of a number of risks into one risk (1.1) to develop a more complete understanding of the overall risk [ISO Guide 73] [Note: also referred to as risk summing or risk overview.]
- **Risk appetite:** amount and type of risk (1.1) that an organization is willing to pursue or retain [ISO Guide 73]
- **Risk attitude:** organization's approach to assess and eventually pursue, retain, take or turn away from risk (1.1) [ISO Guide 73]
- **Risk aversion:** attitude to turn away from risk (1.1) [ISO Guide 73]
- **Risk perception:** stakeholder's (3.2.1.1) view on a risk (1.1) [ISO Guide 73]; Note 1 to entry: Risk perception reflects the stakeholder's needs, issues, knowledge, belief, and values.
- **Risk review:** activity 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 (2.3), risk management process (2.8), risk (2.1) or control (2.26)." [ISO Guide 73:2009, definition 3.8.2.2]
- **Risk tolerance:** organization's or stakeholder's (3.2.1.1) readiness to bear the risk (1.1) after risk treatment (3.8.1) in order to achieve its objectives [ISO Guide 73]; Note 1 to entry: Risk tolerance can be influenced by legal or regulatory requirements.

While the definitions of many terms seem to be "common sense," it is still relevant to research terms and considers formal references.

Types of Risks

Excerpts from "Analysis of Counterfeit Risks and Development of a Counterfeit Product Risk Model" (Spink 2009)

There are general risk analysis guides that are important to consider when developing food fraud prevention theories. One such resource is the types of risks identified by many authors. This type of general list provides insight into the challenge of classifying or categorizing product fraud or counterfeit products – they could fall into several or many categories.

- ***"Catastrophic risk (Nader):*** This affects industries and firms whose financial assets are exposed to catastrophic natural perils, such as earthquakes, hurricanes, volcanic eruption, and so on…. Although catastrophic risk is usually considered as an outcome of natural perils, one nonnatural peril, terrorism, has emerged in recent years as a source of risk whose conse-

(continued)

quences for the insurance industry appear increasingly capable of attaining the same dimensions as those of catastrophic risk."

- ***"Foreseeable risk* (Nader):** This is primarily a legal definition derived from the concept of "foreseeability." Accordingly, the *foreseeable risk* is any risk whose consequences can reasonably be expected to occur, by a person of ordinary prudence."
- ***"Fraud risk (Nader)*** [also categorized by Nader as *security risk*]: This may be defined as the entity's total exposure to the probable misconduct, dishonesty, and deceit by internal as well as external parties…. What is peculiar about *fraud risk* is that it can never generate any returns to the party at risk. Therefore, no business entity acting rationally should ever voluntarily bear or expose itself to any type or amount of *fraud risk*. However, we live in an imperfect world, and it is unrealistic to expect that total elimination of *fraud risk* can be achieved."
- ***"Fundamental risks* (Nader):** This is impersonal in nature, and any person affected by such risks is exposed to losses that do not arise from that person's own individual choice or behavior, but from events beyond his or her control. Examples of such events include natural disasters, political and social developments, economy-wide phenomena, industry-wide phenomena, and so on."
- **"*Legal risk* (Nader):** This is one of the risks of doing international business. It arises from the weaknesses, incompleteness, nonenforceability, and other similar problems with a foreign country's laws and its legal-judiciary machinery…. Such problems increase the probability that the legal system will fail to provide adequate protection of physical and intellectual property rights or remedies against breaches of contracts and other violations of contractual rights."
- "***Liability risk (Nader):*** This is applied to a very broad category of *pure risks*, many of which are *insurable*…. Liability risk arises whenever one party is exposed to possible loss of present or future assets or income as a result of causing one or more of the following events to another party or to assets owned by another party, whether those events (torts) are caused by the first party willfully or through negligence."
- "***Marketing risk* (Nader):** This is used to describe the uncertainty that surrounds the future demand for a firm's products as a result of numerous variables which affect this demand, but may be unpredictable or not entirely under the firm's control. Marketing Risks arise from unanticipated or uncontrollable shift in any of the factors which affect the firm's marketing mix (which are product, price, place, and promotion)."
- *"**Particular risks* (Nadar):** These are those types of risk whose consequences affect individuals separately, and are not so pervasive (as in the case of *fundamental risks*) as to affect an entire group of individuals. *Particular risks* arise from personal actions or events that are under an

individual's control, and are therefore considered to be the responsibility of the individual, rather than the responsibility of society as a whole."

- ***"Property risks (Nadar):*** These encompass all events which carry a possibility of loss, to a property owner, of one or more of the following: the value of property (direct loss), the use of property (indirect loss), and the future income generated by property (indirect loss)."
- "***Pure risk*** **(Nadar):** This is defined as any risk which can only result in a loss or no loss, but can never generate any gains to the party at risk. In other words, a pure risk consists entirely of downside risk and does not contain any upside risk component…. The designation of some risks as *pure risks* is useful for setting apart those risks that are normally *insurable risks* from *speculative risks*, which are normally *uninsurable risks*."
- ***"Speculative risk (Nadar):*** As distinguished from pure risk, is a term applied to describe all risky situations that, in addition to carrying the possibility of loss, also carry the possibility of gain to the party at risk. In other words, speculative risks incorporate not only a downside risk component but an upside risk component."

When the specific threat or response is hard to classify – such as from product fraud or product counterfeiting – there could be a problem if there is a debate about who "owns" the problem. The application to food fraud prevention is that it really doesn't matter how the risk or vulnerability is categorized. There is a process to review new or changing enterprise-wide risks or vulnerabilities. When connected to enterprise-risk management this enables in the Food Fraud Prevention Cycle."

Sidebar: Meeting Dr. Kenneth Arrow—The Godfather of Uncertainty Assessment

In 2009 I was fortunate to meet with Dr. Kenneth J. Arrow at a Society for Risk Analysis meeting. We had a chance to discuss how he saw the uncertainty principles applying to a wide range of risks and vulnerabilities. To step back, Dr. Kenneth Arrow is a Nobel Prize-winning economist—and five of his students were also a Nobel award winner—who is regarded as one of the greatest economists. He was the researcher who developed one of the fundamental concepts of business and economics of "moral hazard" as it relates to risk, uncertainty, and decision-making.

To review, a ***moral hazard*** is a situation where an actor may take greater risks if they receive rewards from the activity but do not personally suffer the consequence of a related loss—it is insinuated that it is immoral to take more risk with someone else's money than you would with your own (Arrow 1951, 1963, 1966, 1968). Applied to food fraud prevention, a buyer may receive a

(continued)

bonus for purchasing the inexpensive product but not be penalized for the cost of a product recall or other re-work expenses. It is argued that the term "moral" is ill-fitting since, unless the activity is illegal or there is some other fraudulent deception, the actor is maximizing the set parameters or specifications, so their activity is not "immoral."

His most significant impact is the "general equilibrium theory." Basically, the idea is that many other factors throughout the economy influence a single decision. The decision to purchase a product (or commit a fraud act) is not only based on if you have money in your wallet (or have other fraud opportunities including do nothing). This was a core to the food fraud strategy goal to "connect everything to everything." Of course, there are direct and indirect variables as well as a wide range of the impact of those variables. He not only developed the idea, but he proved the existence of the equilibrium in the form of a mathematical proof (a mathematical formula that demonstrates and confirms the theory).

An especially interesting and important idea that is applied to food fraud prevention—and defines how it is different from food safety or even food defense—is "social choice theory." This concept is not to be confused with criminology theories such as "rational choice theory," but they are similar. Arrow modeled individuals (a person) as "rational in a narrow sense." The individual has a unique set of decision criteria (e.g., the person sells beef and horsemeat), but it is influenced by society-wide (the entire population) criteria (e.g., the beef commodity price increases). So, if "A" is preferred to "B" and "B" is preferred to "C," then does everyone prefer "A" to C"? Maybe but not necessarily.

In later publications, Dr. Arrow expanded the social choice theory and general equilibrium to "risk" and "uncertainty." The same product in a different "state of the world" or changing market condition is really a different product. He saw that there were more variables involved or "contingent commodities"—commodities that are influenced by when and where they are in the world. Horsemeat within a national border—and not subject to customs inspections—is a different commodity than horsemeat outside the country which would be required to cross a border that would include different laws and face possible inspection. Horsemeat to a company that sells a wide range of meat is a different commodity that for someone who sells wrist watches.

To summarize Dr. Arrow's theories, there is a consideration of several concepts. To apply to food fraud prevention, then consider the "commodity" as a "fraud opportunity":

- Commodity as it relates to the *entire world*.
- Commodity as it is a value to an *individual*.
- Commodity as it is a value to an *individual in a specific situation*.

- Moreover, information that influences that specific situation ["fraud opportunity"] including risk and uncertainty that could be a fraudster concern they might get caught. This is an especially critical contribution to the food fraud prevention theories.

The application to food fraud prevention is that while the fraud opportunity is influenced by macroeconomic factors such as pricing, the real decision is by an individual who is in a specific situation.

That seems like "well, duh, of course," but until that was mathematically proven, it was not considered a real theory. It is important to note that Dr. Arrow applied his theories to market and economic decisions and not to public policy. "He laughed when we asked him how he applied sophisticated mathematical modeling to public policy. His answer was that he did not" (Greenberg and Lowrie 2010). In general, Dr. Arrow considered his theories as a foundation and starting point that could be applied to a wide range of new and emerging risks. Meeting with him encouraged our quest to continue to adapt current models or tools to the unique needs of food fraud prevention.

I am personally grateful for the patience and willingness of someone such as Dr. Arrow to spend a few minutes with a "grad student" talking about some crazy topic such as anti-counterfeiting. He said, "Well, my research would seem to apply." Yes, Dr. Arrow, it does.

Key Learning Objective 2: Fundamentals of Risk Analysis and Risk Communication

This section reviews the academic discipline of decision sciences as a structured way to review the basic risk analysis concepts used to conduct assessments and define the strength of the data and then the recommendations for presenting the findings.

The Key Learning Objectives of this section are

- (1) Introduction to decision sciences
- (2) Fundamental risk analysis concepts such as likelihood, consequence, and risk tolerance
- (3) Fundamental dataset characteristics such as accuracy, precision, certainty, and robustness

Introduction to Decision Sciences

As there is a closer review of food fraud prevention and the foundation, more core concepts are identified. One specific area is the decision sciences. The Decisions Sciences Institute publishes the peer-reviewed, refereed scholarly Decision Sciences Journal (Decision Sciences 2018). Beyond risk and vulnerability assessment or enterprise-wide management, decision-making is the underlying process of the science of decision-making. INSEAD University states (INSEAD 2018):

- "The area of Decision Sciences includes:
- Risk management,
- Decision making under uncertainty,
- Statistics and forecasting,
- Operations research,
- Negotiation and
- Auction analysis, and
- Behavioral decision theory."

Thus, beyond the behavioral science of how people make decisions, this focuses on the methods and processes to organize and assess information to support the exact question that is posed. A primary focus is on defining the specific and detailed question that is being addressed, so there can be an assessment of the right data to support the decision-making (Fig. 15.4).

Research is supported by agencies such as the US National Science Foundation (NSF) within their Division of Social and Economic Sciences which has a section on Decision, Risk, and Management Sciences (DRMS). Their funding focuses "in the areas of judgment and decision making; decision analysis and decision aids; risk analysis, perception, and communication; societal and public policy decision making; management science and organizational design" (NSF 2018).

There are four main goals for decision sciences study:

- (1) "Enrich the diverse disciplines of the decision sciences" meaning to connect and integrate multiple information exchange systems.
- (2) "Integrate these disciplines into bodies of knowledge that are effectively utilized for decision making" which is interoperability and basically to "connect everything to everything."
- (3) "Develop theoretical bases for such fundamental processes as implementation, planning, and design of decision systems" which is studying and refining the process or method to create harmonization and enable sharing of best practices.
- (4) "Improve educational programs and instruction in the decision sciences" which is sharing information through publications and also educating new scientists?

The application to food fraud prevention is that decision sciences emphasizes:

- (1) The need to be very specific in defining the question that is being asked

Fig. 15.4 The hierarchy of decision-making: enterprise risk management to risk analysis to decision sciences

- (2) To focus on the process or method of gathering information and supporting that final decision

The core focus is on what exact decision is being made, such as to put the product on hold and conduct authenticity tests, implement a product recall, cancel a supplier contract, report a suspicious activity to a government agency, etc. Moreover, another consideration is what specific information would change a decision, such as "parmesan cheese has had incidents of this type of cheese fraud" versus "the US FDA just issued a warning letter to one of our suppliers regarding swapping types of cheese fraud." These questions "Establishing the context" of the question to be asked to help identify what and how much data is needed.

Risk, Risk Attitude, Likelihood, and Consequence: ISO 31000—Clarity and Conflict

ISO 31000 Risk Management was published in 2009 after years of a consensus-driven process involving national standards organizations. Even though this was a comprehensive and interdisciplinary approach, it was not without critics. There was support with seemingly simultaneous criticism such as "The consequence of this is that certain ideas about risk and its management have got a boost in credibility and prominence while others have lost out" (Leitch 2010). The meaning is that while the field of risk management received credibility from an ISO standard and future research that was more harmonized, there were also some fields that would have to change their current terminology to be compliant. In some cases this is easy, but

often they are very formalized and in-depth research using one or another of the terms. An example may be the early research on food fraud and economically motivated adulteration. Some research was published using economically motivated adulteration, but the later research shifted to food fraud—there could be confusion or a lack of prestige from those who changed their terminology. This was true for some of the risk assessments and use of terms such as probability versus likelihood, severity versus consequence, and prevention versus mitigation.

Other than the common terminology, the two major steps were to (1) identify that risk could lead to a benefit (consider a financial investment in a high-risk product that results in a higher rate of return) and (2) a standardized methodology for assessing and managing risks.

From ISO 31000 there are some key definitions (including a few terms that have been presented and defined earlier in this book) (ISO 2009):

- ***"Risk:*** effect of uncertainty on objectives;
  - NOTE 1: An effect is a deviation from the expected — positive and/or negative.
  - NOTE 2 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 Risk is often characterized by reference to potential events (2.17) and consequences (2.18), or a combination of these.
  - NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (2.19) of occurrence. ISO 31000:2009(E)"
- ***"Risk attitude*** (referred to in later ISO documents or COSO as 'risk tolerance' or 'risk appetite'): organization's approach to assess and eventually pursue, retain, take or turn away from risk [ISO Guide 73:2009, definition 3.7.1.1]"
- ***"Consequence:*** outcome of an event 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]"
- ***"Likelihood:*** 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]"

This is published in coordination with other ISO standards including:

- ISO Guide 73:2009, Risk management—Vocabulary: A thorough glossary of terms with detailed definitions.
- ISO/IEC 31010:2009, Risk management—Risk assessment techniques: A further review of the process of analyzing and managing risks.

ISO 31000 has a focus on the sources of risks or broadly how they are generated, root cause analysis and then an integrated focus on how best to implement and manage a risk treatment.

- **"Risk source:** element which alone or in combination has the intrinsic potential to give rise to risk, NOTE: A risk source can be tangible or intangible. [ISO Guide 73:2009, definition 3.5.1.2]"

For food fraud prevention, the focus on root cause analysis supports the focus on social science and criminology. While these are new disciplines for a food safety group to consider, this is the most efficient method to reduce or address the root cause—the human adversary. Also, some risks such as stolen goods may seem to have countermeasures and control systems far outside the normal scope of a Food Safety Management System, but the simplest way to reduce the food safety risk is to focus on the risk source which is that the product is stolen. Again, the concept of "accountable" versus "responsible" is important where a Food Fraud Vulnerability Assessment would naturally include stolen goods and the actual controls of securing the inventory would be the "responsibility" of corporate security or plant management.

When the Food Fraud Vulnerability Assessment guidances were being completed, one company estimated it would take 5 years to complete the process. That is interesting, but the GFSI compliance requirements were due in 12 months. "[There are often] disconnects between the available scientific data and the information needs of decision makers also hinder the use of risk assessment as a decision-making tool" (NRC 2009).

Also, "The depth, extent, and detail of the uncertainty and variability analyses should be commensurate with the importance and nature of the decision to be informed by the risk assessment and with what is valued in a decision. This may best be achieved by early engagement of assessors, managers, and stakeholders in the nature and objectives of the risk assessment and terms of reference (which must be clearly defined)" (NRC 2009).

ISO 31000 includes a consideration for the preliminary or general assessments that may not require data that is very detailed, accurate, precise, certain, or robust decisions. What is often important is that "a" risk assessment is conducted as long

as the specification of the low certainty and low robustness is clearly defined. For food fraud prevention decisions, there may not be a lot of detail needed for a decision, or there may not be details provided (at least not yet).

It is very important and a great value that ISO 31000 Risk Management provides a common set of terms and methods so risk assessors across many industries can share insight and expertise. The bottom line is that ISO 31000 is an implemented and standardized system, so it is inefficient and illogical *not* to follow the guidance or definitions.

Quantitative or Qualitative Analysis: Both Are Supported in ISO 31000

ISO 31000 repeatedly emphasizes to conduct the assessment that is most logical and efficient for the question being asked. This can be very formal and quantitative of more informal and qualitative (Purdy 2010). "Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances" (ISO 2009).

This is reiterated in the ISO 31000 standard:

- "The way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk should reflect the type of risk, the information available, and the purpose for which the risk assessment output is to be used. These should all be consistent with the risk criteria."
- "The confidence in determination of the level of risk and its sensitivity to preconditions and assumptions should be considered in the analysis, and communicated effectively to decision makers and, as appropriate, other stakeholders."
- "Risk analysis can be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data, and resources available. Analysis can be qualitative, semi-quantitative, quantitative, or a combination of these, depending on the circumstances."

The bottom-line summary is to select a system and specification that meets *your* needs. Occasionally levels of detail or methods are defined in standards; however, often they are not. For food fraud prevention, the FSMA, GFSI, COSO, or other standards are not very specific.

The general "risk treatments" are presented with flexibility for the risk assessor (ISO 2009):

> "Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:
>
> a) Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
> b) Taking or increasing the risk in order to pursue an opportunity;
> c) Removing the risk source;
> d) Changing the likelihood;
> e) Changing the consequences;

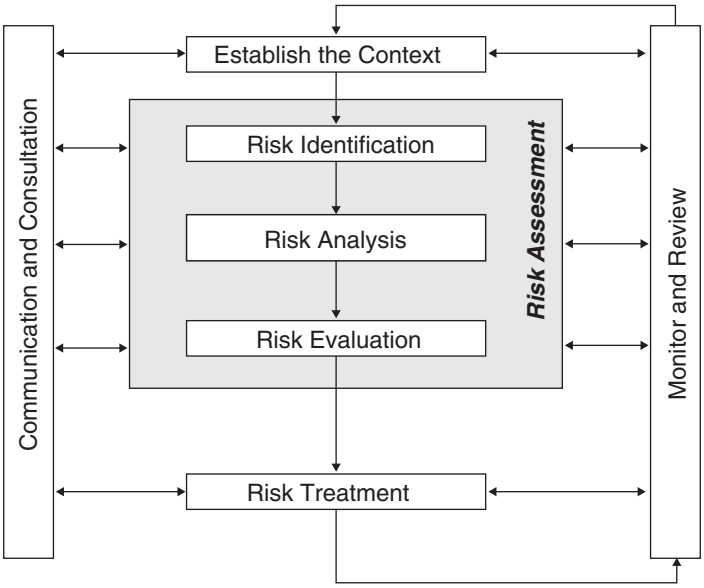

Fig. 15.5 Relationships between the risk management principles, framework, and process, Clause 5 Process. (Copyright Permission Granted) (ISO 2009)

f) Sharing the risk with another party or parties (including contracts and risk financing); and
g) Retaining the risk by informed decision."

For risk assessors in the security or food safety area, the thought of "retaining the risk" seems terrible, irresponsible, and absolutely illogical. In reality, there is no "zero risk" or "zero tolerance" situation, and actually approaching "zero risk" would be inefficient.

ISO 31000 also provides a basic framework that is a logical starting point (Fig. 15.5):

"Establishing the context" is one of the most important steps and is so basic that it is often overlooked by traditional food science risk assessors. Often an incident such as melamine is identified, and the risk assessors quickly use currently available and understood control measures to select and implement risk treatments. The incident is melamine in the product (risk identification), this is a product recall, so it is a problem (risk analysis and risk evaluation), and so applying traditional food safety controls would be to implement a melamine detection test (risk treatment). "Experts" who believe they are already familiar with the incident almost automatically jump to conclusions.

The key concepts for food fraud prevention include these adapted ISO 31000 steps including:

1. **"Establishing the context."** defining the external and internal parameters [context] to be taken into account when managing risk, and setting the scope and risk

criteria (2.22) for the risk management policy (2.4) [SOURCE: ISO Guide 73:2009, definition 3.3.1].

   a. ***For food fraud prevention:*** this would be defining the scope. For example, FSMA would focus only on health hazards. Also, GFSI would focus on vulnerabilities for all types of fraud and for all products.

2. **"Risk Identification":** in HACCP terms this would be hazard identification.

   a. ***For food fraud prevention:*** this would be an incident review and suspicious activity report.

3. **"Risk Analysis":** in HACCP terms this would be a combined step of hazard identification and hazard assessment.

   a. ***For food fraud prevention:*** Vulnerability assessment—review the hazards that were identified and conduct an assessment to define what requires further review.

4. **"Risk Evaluation":**

   a. ***For food fraud prevention:*** Risk assessment—conduct a more detailed review that includes likelihood and consequence.

5. **"Risk Treatment":** managing the system to reduce to within the risk tolerance.

   a. ***For food fraud prevention:*** this would be documented and managed within the Food Fraud Prevention Strategy and by using the Food Fraud Prevention Cycle.

This section provided insight into ISO 31000 Risk Management, presented the terms and concepts, and then presented the application to food fraud prevention. This is a valuable exercise to present the underlying consensus-based standards base and also to explain the logic of the process.

The ERM/COSO system is most efficient and effective for a company to utilize when calibrating the enterprise-wide risks and assessing the vulnerability in relation to the risk tolerance.

Those conclusions are logical if they consider past incidents and a food safety, public health risk-based approach. However, the "Establishing the context" may not be "detect melamine in the product that is being received." The best overall goal could be to "reduce the fraud opportunity of a range of adulterant-substances to be sent to the company."

Several related ISO risk terms include:

- **"Risk assessment:** overall process of risk identification (2.15), risk analysis (2.21) and risk evaluation (2.24) [ISO Guide 73:2009, definition 3.4.1]."
- **"Risk criteria:** terms of reference against which the significance of a risk (2.1) is evaluated [SOURCE: ISO Guide 73:2009, definition 3.3.1.3]

  – Note 1 to entry: Risk criteria are based on organizational objectives, and external (2.10) and internal context (2.11).

  - Note 2 to entry: Risk criteria can be derived from standards, laws, policies and other requirements."

- **"Risk management policy:** statement of the overall intentions and direction of an organization related to risk management (2.2) [SOURCE: ISO Guide 73:2009, definition 2.1.2]."
- **"External context:** external environment in which the organization seeks to achieve its objectives [SOURCE: ISO Guide 73:2009, definition 3.3.1.1]

  - Note 1 to entry: External context can include:
  - — the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
  - — key drivers and trends having impact on the objectives of the organization; and
  - — relationships with, and perceptions and values of external **stakeholders** (2.13)."

- **"Internal context:** internal environment in which the organization seeks to achieve its objectives [SOURCE: ISO Guide 73:2009, definition 3.3.1.2]

  - Note 1 to entry: Internal context can include:
  - — governance, organizational structure, roles, and accountabilities;
  - — policies, objectives, and the strategies that are in place to achieve them;
  - — the capabilities, understood in terms of resources and knowledge (e.g., capital, time, people, processes, systems, and technologies);
  - — information systems, information flows and decision-making processes (both formal and informal);
  - — relationships with, and perceptions and values of, internal stakeholders;
  - — the organization's culture;
  - — standards, guidelines, and models adopted by the organization; and
  - — form and extent of contractual relationships."

Foundational Definitions: Accuracy, Precision, Certainty, and Robustness

Regarding this section, there is an applicable anecdote: "To be wrong with infinite precision"—Taleb. There is a tendency to very thoroughly analyze the information on-hand… often beyond what is appropriate. A very complex and intricate statistical assessment will insinuate that the underlying information is accurate, precise, and certain.

Several foundational definitions should be reviewed before going into more detail. While there are many possible references for these definitions, since the

research question here is focused on "food," then when possible the US FDA definitions are presented:

- ***Accuracy:*** "how close the measured result is to the actual result" (Capra and Canale 1998). 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***" (Teasdale et al. 2017).
- ***Precision:*** "how two measurements agree with each other regardless of the 'accuracy'" (Capra and Canale 1998). 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" (ICH 2005).
- **Bias (also referred to as Inaccuracy):** "is defined as systematic deviation from the truth" (Capra and Canale 1998). 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" (Merriam-Webster 2004). This term creates confusion due to the difference in scientific and popular definition.
- ***Uncertainty (Imprecision):*** "on the other hand, refers to the magnitude of the scatter" (see Certainty) (Capra and Canale 1998).
- ***Certainty:*** "[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]" (JCGM/WG1 2008). Is generally a statement of the confidence in a measurement. 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" (NIST 2018). A general dictionary definition is "1. fixed, settled, 2. of a specific but unspecified character, quantity, or degree, 3. dependable, reliable, indisputable, etc." (Merriam-Webster 2004).
  - ***Robustness:*** "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" (ICH 2005).

It is usually helpful to provide a case study to explain concepts, definitions, and most importantly how the terms relate to each other. Of course, without a methodi-

cal and thorough review, the accuracy and precision cannot be judged. What can be judged is the method and process to gather data (Re., seeking many, varied sources and considering insight and patterns) in relation to what is known about the overall data set (Re., all types of food fraud).

First, consider measuring the speed of a person jumping out of an airplane (emphasis added) (Capra and Canale 1998):

> Errors sometimes enter into an analysis because of uncertainty in the physical data upon which a model is based. For instance, suppose we wanted to test the falling parachutist model by having an individual make repeated jumps and then measuring his or her velocity after a specified time interval. Uncertainty would undoubtedly be associated with these measurements since the parachutist would fall faster during some jumps than during others. These errors can exhibit both inaccuracy and imprecision. If our instruments consistently underestimate or overestimate the velocity, we are dealing with an inaccurate, or biased, device. On the other hand, if the measurements are randomly high and low, we are dealing with a question of precision. (Capra and Canale 1998)

The accuracy and precision concepts are applied to a food fraud example in Table 15.1.

A visualization of the accuracy/inaccuracy and precision/imprecision is provided (Fig. 15.6):

For food fraud prevention, it is important that *you* know what accuracy and precision *you* need before *you* can judge the value of a data set. If the provider of a data set cannot define their accuracy and precision—as well as the 7 Vs of data analytics—then they may be "Just gathering whatever data you can find" (example "a" above).

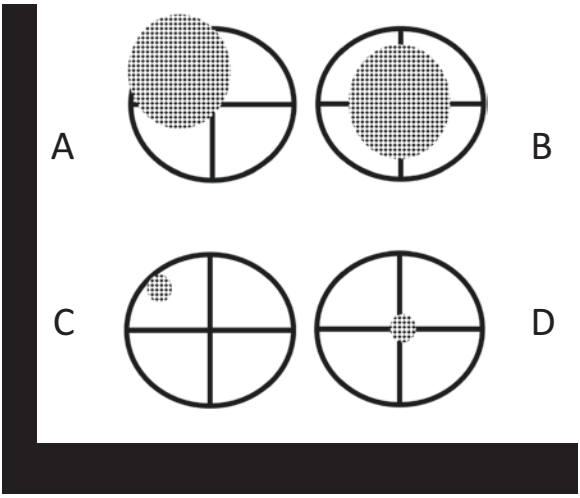

Fig. 15.6 Visual example. (Adapted from Capra and Canale (1998))

Table 15.1 Explanation and examples of accurate, inaccurate, precise, and imprecise with results and a food fraud example

Accuracy	Precision	Result	Food fraud example
Inaccurate	Imprecise	A *random* pattern that does *not* cluster around the center	Example (see figure position "a"): "Just gathering whatever data you can find." This could be a 5-minute internet search of the phrase "food fraud incident." Possibly one type of incident—or multiple mentions of the same incident—skews the focus away from the actual target
Accurate	Imprecise	A *random* pattern that *is* clustered around the center	Example (see figure position "b"): This could be gathering information from a source that covers a broader range of issues than the topic of concern. This could be using a database that records many incidents that are outside the specific scope of food fraud such as including fraud acts that are intentional and unintentional
Inaccurate	***Precise***	A *tight* pattern *not* around the center	Example (see figure position "c"): This could be analysis from only one type of test or only from one market. This could be referred to as being "uncertain with great precision." This could be a detailed assessment of one type of fraud and possibly one incident. This could be many tests of meat but from one grocery store or city
Accurate	***Precise***	A *tight* pattern that *is* around the center	Example (see figure position "d"): A thorough method to consider all types of incidents and then extensive development of the data set to provide insight from many incidents. This could be testing many products from many types of retail locations from a wide region and with a sampling plan that is designed to be holistic and all-encompassing

(Adapted from Capra and Canale (1998)

Key Learning Objective 3: Review Who Is of "Accountable" and "Responsible"

This section reviews the most important question of "who is accountable" which is quickly followed by "who is responsible." Once those questions are clear, then there can be more direct agreement what are the exact tasks that define competent "accountability" and "responsibility."

The Key Learning Objectives of this section are

- (1) Who is accountable and who is responsible?
- (2) What are the exact tasks for those who are accountable and who is responsible?
- (3) What are the metrics to define competence?

Who Is "Accountable" Versus Who Is "Responsible"

The concept of "accountable" and "responsible"—including explicit or de facto assignment—was fundamental to the concepts behind the Food Risk Matrix. The four cells represent the food risks that a company is "accountable" to manage regardless of their knowledge of the risk. Following ISO 31000, each new problem or incident *must* be put into one of the cells. Some must be identified as "accountable" for that cell and cannot give up their role until someone else acknowledges and agrees to take over the problem or incident. This also identifies that someone is "accountable" but delegates a task to someone "responsible" for implementation (emphasis added).

- ***Risk Owner:*** "person or entity with the accountability and authority to manage a risk [ISO Guide 73:2009]"
- ***Accountability:*** "The organization should ensure that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness, and efficiency of any controls. This can be facilitated by:
  - Identifying risk owners that have the accountability and authority to manage risks;
  - Identifying who is accountable for the development, implementation, and maintenance of the framework for managing risk;
  - Identifying other responsibilities of people at all levels in the organization for the risk management process;
  - Establishing performance measurement and external and/or internal reporting and escalation processes; and
  - Ensuring appropriate levels of recognition."
- **Stakeholder**: "person or organization that can affect be affected by, or perceive themselves to be affected by a decision or activity; *note* a decision maker can be a stakeholder [ISO Guide 73:2009, definition 3.2.1.1]"
- **Interested party:** "person or organization (3.32) that can affect, be affected by, or perceive itself to be affected by a decision or activity" (ISO 2005).

Also from "Establishing Risk Management Policy" clearly identifies different individuals who are "accountable" and "responsible":

- "Commitment to make the necessary resources available to assist those accountable and responsible for managing risk;"

Moreover, "Preparing and Implementing Risk Treatment Plans" stated:

- "The information provided in treatment plans should include: … those who are accountable for approving the plan and those responsible for implementing the plan;"

At the end of the day, after an incident, you do not want to find out that you were the "accountable" person! If you know about food fraud, then you are now aware and may be legally liable for being "accountable" until you transfer this to another "risk owner."

Conclusion

The foundational risk analysis and risk assessment concepts in this chapter are very general and broad so as to add value during food fraud prevention. Building on the foundation and fundamentals identified in the previous chapters, there are specific methods—and adaptations of even more broad theories—that are effective and efficient. ***The first conclusion is*** that there are some basic, standardized, and codified terms and methods that are efficient and effective to utilize. There are also some commonly used risk analysis and risk assessment concepts and theories that absolutely do *not* apply. The use of a common definition and scope helps both the risk communication of food fraud as well as enables the application of expertise and insight from other fields. ***The second conclusion is*** that it is most efficient to build upon other currently implemented risk analysis systems but to adapt the methods based on the unique food fraud prevention needs and nature of the dataset. For the new topic of assessing and managing food fraud, it is most efficient to build upon previously understood and trusted systems to provide a mental anchor. For example, a Food Fraud Vulnerability Assessment can be described as "like HACCP but for food fraud vulnerabilities in VACCP." Another example is to state that "food fraud prevention strategy is just a specific application of the total quality management Six Sigma concepts of root-cause-analysis and plan-do-check-act." HACCP and Six Sigma are well known and trusted by a wide range of interested parties including the C-suite of companies and internal auditors who might be accountants by education and to financial analysts at investment firms. ***The final conclusion is*** that the risk assessment methods and analysis that applies to other food problems do *not* necessarily apply to food fraud. When food scientists or food safety professionals first address the food fraud problem, there is an assumption that there is "enough" of similar food safety data. The nature of the data generator is very different since it is a human, not a microbe. The human is an intelligent adversary that rapidly evolves to shifting fraud opportunities. Also, compared to food safety, there are many fewer incidents and few incidents that occur in the same way. This chapter provided a risk assessment foundation specific to food fraud prevention. There is a saying:

VACCP is like HACCP but for food fraud prevention.

Appendix: WIIFM Chapter on Risk Basics

This "What's In It For Me" (WIFFM) section explains why this chapter is important to you.

Business functional group	Application of this chapter
WIIFM all	This is an introduction to the basic risk analysis and risk assessment concepts to provide a thorough understanding of the basics as well as a common terminology and approach
Quality team	This provides insight on how auditees conduct an FFIS and ongoing RAs
auditors	This provides a basic definition and terms that should be used—e.g., utilizing common ISO 31000 Risk Management and ISO 9000 Quality Management terminology
Management	Same
Corp. decision-makers	The risk analysis terms may be new to you, but they are universally used and will reduce confusion

Appendix: Study Questions

This section includes study questions based on the key learning objectives in this chapter:

1. Discussion Question
   (a) Is "risk" tolerable when addressing a food safety?
   (b) Discuss the relationship between vulnerability, threat, and risk.
   (c) What are the challenges of data collection and assessment for food fraud?
2. Key Learning Objective 1
   (a) What is "moral hazard"?
   (b) Why is it more efficient to focus on "vulnerability" rather than "risk"?
   (c) Is "suspicious activity" a "risk"?
3. Key Learning Objective 2
   (a) What is "decision sciences"?
   (b) Why is ISO 31000 considered the definitive source for risk management?
   (c) What is the "impression of excessive precision"?
4. Key Learning Objective 3
   (a) What is "accountable" and "responsible"?

(b) Why is it important to define and assign "accountable" and "responsible" parties?
(c) What job function and position should be "accountable" for FF prevention?

References

ANSI, American National Standards Institute. (2009). Organizational resilience: Security, preparedness, and continuity management systems - requirements with guidance for Use, ANSI ASIS SPC.1-2009. https://www.asisonline.org/Standards-Guidelines/Standards/published/Pages/Organizational-Resilience-Security-Preparedness-and-Continuity-Management-Systems-%28Download%29.aspx.

Arrow, K. J. (1963). Uncertainty and the welfare economics of medical care. *The American Economic Review, 53*(5), 941–973.

Arrow, K. J. (1968). The economics of moral hazard: Further comment. *The American Economic Review, 58*(3), 537–539.

Arrow, K. J. (1951). *Social choice and individual values* Ph.D., Columbia University.

Arrow, K. J. (1966). *Exposition of the theory of choice under uncertainty, in Synthese* (pp. 253–269). Springer: Reidel Publishing Co., Dordrecht-I-Iolland.

Capra, S., & Canale, R. (1998). *Numerical methods for engineers*. Boston.

CBER, Center for Biologics Evaluation and Research. (2006). *Guidance for industry - Q9 quality risk management*. U. S. Food and Drug Administration, Center for Drug Evaluation and Research (CDER), Center for Biologics Evaluation and Research (CBER).

CFSAN, Center for Food Safety and Applied Nutrition. (2005). *Guidance for industry, submitting requests, under 21 CFR 170.39, threshold of regulation for substances used in food-contact articles*. U. S. Food and Drug Administration, Center for Food Safety and Applied Nutrition, Office of Food Additive Safety.

CFSAN, Center for Food Safety and Nutrition. (2002). *Initiation and conduct of all 'major' risk assessments within a risk analysis framework*. U. S. Food and Drug Administration, Center for Food Safety and Applied Nutrition.

CFSAN, Center for Food Safety and Nutrition. (2003). *Risk assessment for food terrorism and other food safety concerns*. U. S. Food and Drug Administration, Center for Food Safety and Applied Nutrition, Office of Regulations and Policy.

CFSAN/FDA, Center for Food Safety and Applied Nutrition. (2007). Carver+Shock software tool, Home Page. Retrieved June 16, 2007, from http://www.cfsan.fda.gov/~dms/carver.html

Clarke, R. V., & Eck, J. E. (2005). *Crime analysis for problem solvers in 60 small steps*. Washington, DC: Center for Problem Oriented Policing.

CNSSI, Committee on National Security Systems. (2010). Instruction 4009, CNSSI 4009. https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf.

CODEX, Codex Alimentarius. (2003). Guidelines on the judgement of equivalence of sanitary measures associated with food inspection and certification systems, 1, CAC/GL 53–2003, URL: file:///C:/Users/J/Downloads/CXG_053e.pdf

Codex Alimentarius, CODEX. (2014). *Procedural manual* (22nd ed.). Geneva/Rome: World Health Organization/Food and Agriculture Organization of the United Nations.

COSO, Committee of Sponsoring Organizations of the Treadway Commission. (2014). COSO Enterprise risk management – Integrated framework update project, Frequently Asked Questions (FAQ), http://www.coso.org/documents/COSO%20ERM%20FAQs%2011%205%2014.pdf.

Cruz, M. G. (2002). *Modeling, measuring and hedging operational risk*. New York: Wiley.

Decision Sciences. (2018). Home Page, URL: https://onlinelibrary.wiley.com/journal/15405915.

DHS, US Department of Homeland Security. (2008). DHS Risk Lexicon. Risk Steering Committee. https://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf.

DHS, Department of Homeland Security. (2013). The risk management process for federal facilities - an Interagency Security Committee Standard, August 2013, 1st edition. https://www.dhs.gov/sites/default/files/publications/ISC_Risk-Management-Process_Aug_2013.pdf.

FDA, U.S. Food and Drug Administration. (2003). Quantitative assessment of the relative risk to public health from Foodborne Listeria monocytogenes among selected categories of ready-to-eat foods, background and process, technical and scientific reviews of the FDA/FSIS risk assessment, richard whiting, Food and Drug Administration, December 4, 2003.

FDA, U.S. Food and Drug Administration. (2015). Current good manufacturing practice, Hazard analysis, and Risk-based preventive controls for human food, final rule, federal register, Docket NumberFDA-2011-N-0920, Wednesday, November 18, 2015, Accessed 5 Dec 2015, https://www.federalregister.gov/articles/2015/11/18/2015–29340/current-good-manufacturing-practice-hazard-analysis-and-risk-based-preventive-controls-for-human

FSMA, Food Safety Modernization Act. (2016). Mitigation strategies to protect food against intentional adulteration (FSMA-IA, Food Defense), Food and Drug Administration, Final rule, Federal Register, May 27 2016, https://www.regulations.gov/document?D=FDA-2013-N-1425-0146.

Goldstein, H. (1990). *Excellence in problem-oriented policing*. New York: U.S. Department of Justice, Center for Problem Oriented Policing.

Greenberg, M., & Lowrie, K. (2010). Kenneth J. Arrow: Understanding uncertainty and its role in the world economy. *Risk Analysis, 30*(6), 877–880.

ICH, International Conference on Harmonization. (2005). Validation of analytical procedures, text and methodology Q2 (R1)–ICH Harmonized Tripartite guideline, international conference on harmonization of technical requirements for registration of pharmaceuticals for human use, URL: https://www.ich.org/fileadmin/Public_Web_Site/ICH_Products/Guidelines/Quality/Q2_R1/Step4/Q2_R1__Guideline.pdf; URL: https://www.fda.gov/downloads/drugs/guidances/ucm073384.pdf

INSEAD, Institut Européen d'Administration des Affaires. (2018). Department of Decision Sciences, "Institut Européen d'Administration des Affaires" or European Institute of Business Administration.URL: https://www.insead.edu/faculty-research/academic-areas/decision-sciences

ISO, International Standards Organization, 73. (2002). *Risk management – Vocabulary – Guidelines for use in standards*. 2002

ISO, International Organization for Standardization. (2005). ISO 22000 Food safety management systems -- Requirements for any organization in the food chain. 2012, from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=35466

ISO, International Standards Organization. (2007). ISO/PAS 22399:2007 Societal security - Guidelines for incident preparedness and operational continuity management.

ISO, International Organization for Standardization. (2008a). ISO Homepage. from http://www.iso.org/iso/home.htm.

ISO, International Organization for Standardization. (2008b). *ISO/IEC Guide 98-3:2008 (JCGM/WG1/100), Uncertainty of measurement – Part 3: Guide to the expression of uncertainty in measurement (GUM:1995), URL: file:///C:/Users/J/Downloads/JCGM_100_2008_E.pdf.*

ISO, International Organization for Standardization. (2009). ISO 31000:2009 risk management-principles and guidelines.

ISO, International Organization for Standardization. (2018). ISO 31000:2018 risk management -- guidelines, url: https://www.iso.org/standard/65694.html

ISO, International Organization for Standardization. (2012). ISO/IEC 27000:2012, Information technology – Security techniques – Information security management systems. from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56891.

JCGM/WG1, Joint Committee for Guides in Metrology. (2008). Evaluation of measurement data—guide for the expression of uncertainty in measurement. JCGM 100: 2008, URL: Evaluation of measurement data — Guide to the expression of uncertainty in measurement (GUM), URL: https://www.bipm.org/utils/common/documents/jcgm/JCGM_100_2008_E.pdf. Citado en las 167.

Kaplan, S. (1997). The words of risk analysis. *Risk Analysis, 17*(4), 407–417.

Leitch, M. (2010). ISO 31000:2009—The new international standard on risk management. *Risk Analysis, 30*, 887–892.

Merriam-Webster. (2004). The Merriam-Webster dictionary -- New Edition.

NIST, US National Institute of Standards and Technology. (2002). Risk management guide for information technology systems – Special Publication 800-30, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

NIST, United States National Institute of Science and Technology. (2011). Managing information security risk – Organization, mission, and information system view, Special Publication 800-39, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

NIST, United States National Institute of Science and Technology. (2018). Measurement uncertainty, URL: https://www.nist.gov/itl/sed/topic-areas/measurement-uncertainty.

NRC, National Research Council. (1996). In P. C. Stern & V. Harvey (Eds.), *Understanding risk: Informing decisions in a democratic society, National Academy of Science NAS*. Fineberg: National Academies Press.

NRC, National Research Council. (2009). Science and decisions: advancing risk assessment. Washington, DC: National Academy of Sciences (NAS).

NSF, US National Science Foundation. (2018). Home Page, Decision, Risk and Management Sciences (DRMS), URL: https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5423

Purdy, G. (2010). ISO 31000:2009—Setting a new standard for risk management. *Risk Analysis, 30*, 881–886.

RAND, Rand Corporation. (2018). Delphi method Home Page, URL: https://www.rand.org/topics/delphi-method.html

Spink, J. (2009). *Analysis of counterfeit risks and development of a counterfeit product risk model*. PhD Dissertation Ph.D., Michigan State University.

Spink, J. (2014). Food fraud prevention overview, Introducing the Food Fraud Prevention Cycle (FFPC)/ Food Fraud Prevention System, GFSI China Focus Day 2014, Beijing.

Spink, J., Ortega, D., Chen, C., & Wu, F. (2017). Food fraud prevention shifts food risk focus to vulnerability. *Trends in Food Science & Technology, 62*, 215–220.

Spink, J., Zhang, G., Chen, W., & Speier-Pero, C. (2019). Introducing the food fraud prevention cycle (FFPC): A dynamic information management and strategic roadmap. *Food Control, 105*, 233–241.

Teasdale, A., Elder, D., & Nims, R. W. (2017). *ICH quality guidelines: An implementation guide*. Hoboken, NJ: Wiley.

UNODC, United National Office on Drugs and Crime. (2010). Guidance on the preparation and use of serious organized crime assessments (SOCTA), United Nations, http://www.csd.bg/fileadmin/user_upload/Countries/UN/09-86230_Ebook_appr.pdf.

Van Der Fels-Klerx, Ine, H. J., Goossens, L. H. J., Saatkamp, H. W., & Horst, S. H. S. (2002). Elicitation of quantitative data from a heterogeneous expert panel: Formal process and application in animal health. *Risk Analysis, 22*(1), 67–81.

WTO, World Trade Organization. (1995). Sanitary and phytosanitary measures: Text of the agreement, The WTO agreement on the application of Sanitary and Phytosanitary Measures (SPS Agreement), January 1, 1995, Note: Appropriate level of sanitary or phytosanitary protection — The level of protection deemed appropriate by the Member establishing a sanitary or phytosanitary measure to protect human, animal or plant life or health within its territory. NOTE: Many members otherwise refer to this concept as the “acceptable level of risk”.URL: https://www.wto.org/english/tratop_e/sps_e/spsagr_e.htm