Chapter 17
Risk Analysis (Part 3 of 3): Implementation

Summary

This chapter presents a shift from the general risk analysis theory to the application and implementation of the Food Fraud Prevention Strategy. The following chapter on Risk Assessment Application provides more detailed examples and case studies. This chapter will focus more specifically on the vulnerability assessments including preparing to address the problem, conducting a quick initial screening, expanding to a more detailed assessment where and when warranted, and finally connecting the assessment to all other enterprise-wide problems.

The Three Key Learning objectives are:

- **(1) Framing the Problem and Scope:** Define what question you are asking and exactly what information is needed to change a specific decision.
- **(2) Conducting a Prefilter or Initial Screening to Start:** At minimum, review the entire fraud opportunity to document an assessment. This will demonstrate a method to identify the most important problems.
- **(3) Conducting a Detailed Food Fraud Vulnerability Assessment (FFVA) Including Presentation in an Enterprise-Wide Assessment:** This final step will allow a detailed—and often spirited—debate of the conclusions and very specific discussions about countermeasure and control systems.

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. 17.1).

Introduction

This chapter will expand on risk analysis to specific vulnerability assessment concepts. It is important to build upon a theoretically sound foundation to establish the overall principles and finally to make sure the concepts are coordinated and

J. W. Spink, *Food Fraud Prevention*, Food Microbiology and Food Safety,
https://doi.org/10.1007/978-1-4939-9621-6_17

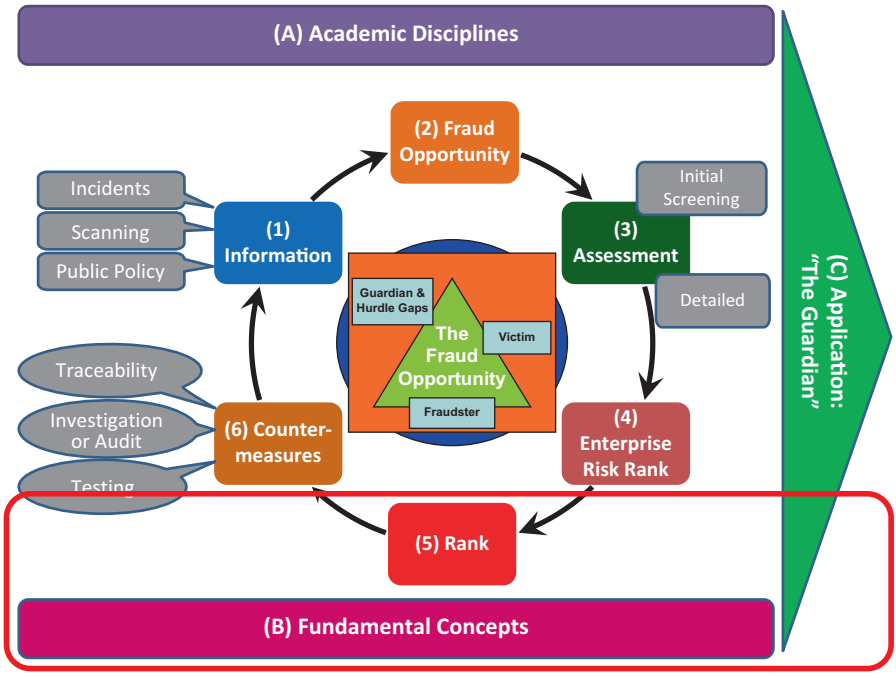

Fig. 17.1 Food Fraud Prevention Cycle—where this chapter applies to the overall concept: "(B) fundamental concepts" and "(5) risk". (Copyright Permission Granted) (Spink 2014; Spink et al. 2019)

calibrated all the way to actual implementation (Fig. 17.2). Too many times academics study one part of a process—ad infinitum to way beyond the point of diminishing return—but leave the integration to some anonymous "others." There is often an empty and unsupported claim that "can be used by decision-makers" or "is valuable to support decision-making." The "decision" is never clearly defined, and the "decision-makers" are often generic "risk assessors." *General* recommendations *generally* help while *specific* recommendations *specifically* help. This general approach to answering non-correlated research questions is similar to creating separate links in a chain but never checking that the entire chain actually connects and can support the weight of the lift. Without framing the problem and scope of the application or value of the new research cannot be judged… *at all*.

To consider more details of the Food Fraud Vulnerability Assessment and decision-making, there is a flow from the beginning with a consideration of the issue through decision-making (Fig. 17.3). There are specific steps required to advance from an assessment through processing to supporting an actual resource-allocation decision.

As is presented in the Business Decision-Making chapter, the COSO managerial accounting practice of Enterprise Risk Management is based on an assessment in a

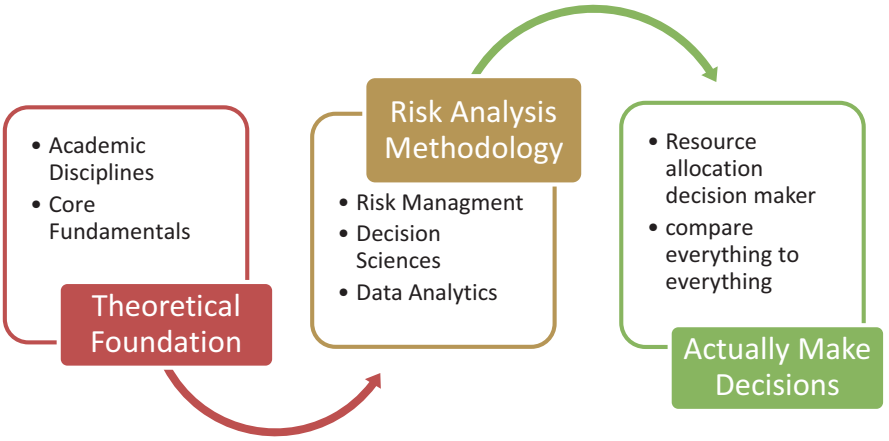

Fig. 17.2 Process from theoretical foundation through risk analysis methodology to actual decision-making

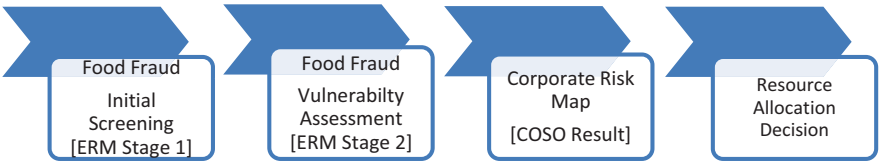

Fig. 17.3 The role of the Food Fraud Initial Screening (FFIS) in the Food Fraud Risk Continuum. (Copyright Permission Granted) (Spink et al. 2016)

two-stage process. The first is a qualitative, prefilter, or quick "initial screening" following more detailed assessments only as required for the specific question and resource-allocation decision. In many cases, more assessment is not needed. The third step is to include the assessment in some sort of enterprise-wide calibration system. This new problem must be compared to other enterprise-wide problems. Finally, the assessments and analysis have a definitive role in supporting resource-allocation decision-making. The entire system is refined to both increase the efficiency of the assessments and also support the final decision-making.

Key Learning Objective 1: Framing the Problem and Scope

This section reviews framing the problem and scope which is referred to in ISO 31000 as "Establishing the context" (ISO 2009). Specifically, the preparation is critical to consider what really needs to be completed and how the resource-allocation decision-making can best be conducted.

The Key Learning Objectives are:
- (1) Prepare and review scope which is not just to authenticate but to prevent.
- (2) Internal and external resources such as to spend 10-minutes on Google Scholar can save 2 weeks of laboratory research or project work.
- (3) Needs of the boss and many decisions are based on very little data.

Prepare and Review

If you do not identify the specific question in detail, then there is really no way to judge the efficiency of countermeasures and control systems. Aspirin is good, taking an aspirin must be good, then taking ten aspirins would seem to be better, right? If A = B and B=C, then A = C? However, for a broken leg or acne, that is not a very efficient risk treatment. If you clearly identify the problem (broken leg or facial acne), then the urgency of response can be defined and defended. Also, the most efficient and effective risk treatment can be identified and explained. For the broken leg, immediately call an ambulance to go to an emergency room to set the broken leg. For acne, maybe begin to try using acne soap and face cream for a month. Aspirin is good but never considered as a recommended treatment for either problem.

An example of defining the problem in detail is presented here (Spink 2017):

- **Problem:** Counterfeit or substandard vodka poisoning consumers, undermining consumer confidence, and possibly reducing the demand and price for local vodkas.
- **Market:** An entire country.
- **Goal:** There is a hierarchy of needs that get synthesized for specific agencies or countermeasures and control systems.
  - What is the problem?
    - Stop e-commerce? No.
    - Detect fraud? Yes.
    - Deter fraudsters? Yes.
    - Stop consumers getting cheated? Yes, and now getting more specific.
    - Stop consumers getting hurt? Yes, and now getting even more specific.
    - Reduce public health harm from fraudsters? Yes, getting yet even more specific.
    - Reduce consumer victimization? Yes, a final key focus.
    - "Prevent it all violations?"—Ok, this is more of an aspiration and is good as a vision, but what is "it" again?
      - Prevent all health harms from all e-commerce? No.
      - Address illegal e-commerce alcohol and specifically vodka? Yes.
- Review the updated project scope: The problem statement is to address counterfeit or substandard vodka poisoning dangers which undermine consumer confidence and possibly reducing the demand and price for locally produced vodkas.

Thus, a first step is to conduct a risk assessment to identify the root causes of the vulnerabilities so that a prioritized focus can be concluded.

After following this detailed process, the research question is clearly and precisely defined. If this is written, then it can be shared, edited, discussed, debated, and refined. Now that there is a very specific research question, a response can be identified and evaluated. This type of detail is helpful to identify success metrics and then also support a resource-allocation decision.

Sidebar: Detail on Starting to Address the Problem (Starting from a Blank Page)

Of course, if there is an actual, live incident, then addressing that problem is the priority. If there is a known or suspected public health threat that gets the immediate focus. If there is no specific incident or suspected public health threat, the first step is *not* to "respond to risks" or to select countermeasures and control systems. Before selecting countermeasures and control systems, there is a methodical approach to frame the question.

Overall, there will appear to be similar theoretical concepts that keep presenting themselves between the ISO (e.g., ISO 9000, ISO 22380, and ISO 22000), criminology (e.g., SARA method and Situational Crime Prevention), and the business management (e.g., COSO, Total Quality Management (TQM), and Generally Accepted Accounting Principles (GAAP)).

Risk assessment process based on the COSO managerial accounting practices state that "The ERM risk assessment process is outlined here" (COSO 2011):

"1. Identify risks. These might impact the enterprise (external or internal)."

"2. Develop assessment criteria. Assessment criteria are often difficult to develop as it is very difficult to compare and aggregate risk across the enterprise. Such criteria often focus on the relative likelihood of an enterprise experiencing a specific risk as well as the impacted financials and all other negative consequences that might occur. Since risks might have negative consequences across functions/business units/etc., it is important these different constituencies within the enterprise have an understanding of the breadth of risks and their impact and such that consistent interpretations of risk/consequences can be developed."

"3. Assess risk. This is accomplished in two stages that include:

- '(1) A qualitative initial screening is driven by categories of likelihood/impact (e.g., this risk as a high likelihood and a moderate impact).
- '(2) A more detailed quantitative assessment of those risks that were deemed most consequential in the initial screening."

"4. Assess risk interactions. This step focuses on understanding the enterprise risk portfolio in an integrated or holistic way by examining how iden-

(continued)

tified risks positively or negatively are influenced by specific changes/processes that might occur within the enterprise. For example, efforts to reduce the potential for supply chain disruption might involve bringing in new raw material suppliers. Such a change might increase the risk of food fraud within the firm (e.g., unadulterated product, more difficult to audit each supplier, etc.)."

"**5. Prioritize risks.** This step includes evaluating risks against "predetermined target risk levels and tolerance thresholds [later referred to as risk appetite]." It is important in this step that the potential holistic impact of a given risk is included when prioritizing the importance of a given risk. For example, beyond the financial loss, other important criteria such as the health and safety, brand reputation, etc. should be carefully considered."

"**6. Respond to risks.** In this step, risk responses (accept, reduce, share, and avoid) are determined and implemented. These steps create the foundation for the assessment. The next step is creating the vulnerability scales."

An example of the continuum from an initial screen to the detailed assessment is provided (Fig. 17.4).

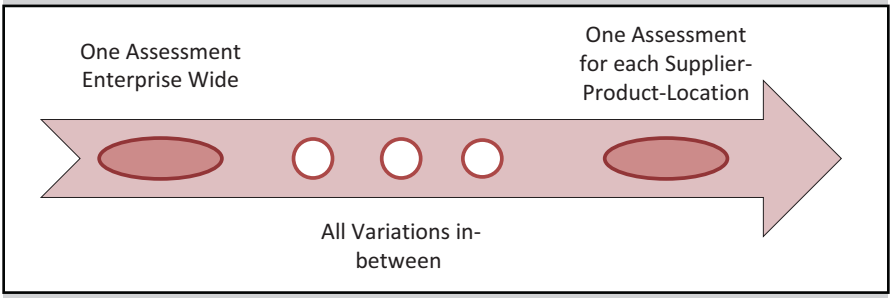

Fig. 17.4 Continuum of the ERM two-stage process of risk assessments from "initial screen" to "detailed assessment"

This is a detailed list that helps define the start of the risk assessment process which helps with the following step of "how to start." It is important to emphasize that framing the question and identifying "how to start" creating a strategy are important before selecting or implementing countermeasures.

Risks of Conducting Risk Assessments

To continue to review "how to start," there is a need to define the end goal but also other ways that the process could start, such as testing for the fraudulent product (Spink et al. 2013; Spink 2019). There is a saying "If you are a hammer everything looks like a nail." That means that if a "hammer" is trying to complete a task, it will start by treating the problem like it is a "nail" and start banging. For food fraud

prevention, this could be a packaging manager recommending a packaging anti-counterfeiting component, a corporate security officer recommending investigating for suspicious activity, a law enforcement agency recommending investigation and prosecution, a customs officer recommending border inspections, a corporate lawyer recommending a lawsuit, or a food scientist recommending food authenticity tests. While each manager is trying to do the right thing and to make real progress on the problem, the most efficient way to start is with a risk assessor conducting an enterprise-wide assessment.

Next, it is important to understand the possible ramifications of any first action. While it may seem logical to "just start testing," there may be no consideration of what you might find. It would be illogical *not* to find *any* suspicious activity regardless of their actual vulnerability, risk, or hazard. Early in the process, there may be no assessment calibration or decision-making criteria; any and all suspicious activity or innuendo may require a response. A response could be a global product recall of all products related to the suspicious activity. A more scientifically or methodologically based decision-making process could consider all the suspicious activities—or vulnerabilities—but include a filter that reduces the situations that require the most urgent and comprehensive responses.

If you find something suspicious, you may need to act—if you suspect a health hazard or illegal act, then not acting may be literally criminal—and criminal for *you*, individually, not just for your corporation. Most times, the issue is just peculiar or odd but not dangerous. If you "just start testing" or "just start investigating," you may be inadvertently taking on new risks.

Another consideration is that there is even a risk of conducting risk assessments. At an early FFVA session that included senior food safety managers for food companies, there was a lack of awareness of the general liability in even just doing a prefilter assessment. The operations-focused personnel felt they were taking a science-based approach to more data gathering. They ignored and laughed off mentions of potential general legal liability. When the food scientists were asked "have you actually run this by your General Counsel," they responded "yes, yes"—it seemed apparent that they hadn't. In later sidebar discussion with a Deputy General Counsel, it was clear that the liability was a concern that was not fully understood by the food safety managers. The Deputy General Counsel was extremely concerned with the "risk of conducting risk assessments" and the liability of "just start testing product." To be clear, if there were any incident or suspected health hazard, there would be immediate action.

For example,

- Action: Consider a packaging summer intern employee at your company uses a published Food Fraud Vulnerability Assessment without full information, and the automated system concludes your company has "high" food fraud vulnerability.
- Response: So, "yes or no" does your "company" have knowledge of a "high" food fraud vulnerability? "Yes, but…" The fact is "yes."
- Consequence: This may be found during discovery during a lawsuit.

If you conduct an investigation and find *any—each and every*—suspicious activity, that concern *must* be further investigated. *Each and every* suspicious activity could be a public health threat or fraudulent product that would be illegal and unfit for commerce. Without a full system to assess the vulnerability, you may find a lot of "suspicious activity" that really is *not* a risk and actually within the risk tolerance. The suspicious activity may be just peculiar or odd but not dangerous or illegal.

Research Internal and External Resources

It is amazing how the little background research is often conducted before implementing big food fraud projects such as a lack of awareness of the value of criminology before addressing the human criminal adversary. Also, the general lack of risk analysis focuses on defining the problem and understanding the decision-making method. There is a mantra to "just get started." There is an ignorance or lack of perspective that just because you have not heard of a problem before that, the vulnerability does not exist. Some companies and industries continuously create a completely new system from scratch or "reinvent the wheel." Usually, they reinvent a poorer version of "the wheel." The first inclination should be that:

- '(1) Someone else has been studying this.
- '(2) The available systems probably do not exactly apply to food fraud prevention.

The action to "just get started" could lead you down a long and winding path to a dead end. While "analysis paralysis" is the other end of the spectrum, for food fraud prevention there are guides and recommended paths forward.

In many (most) situations, there is new technology development that "is a solution looking for a problem." This is backward. If you clearly understand your problem, then you can seek out or develop an optimal solution. If you don't know your problem, then it is "dumb luck" if the technology or solution you select actually meets your needs (see section on Diagnosis, Treatment, Prognosis, and Decision).

There is a joke in academia that "two weeks in the laboratory can save you one day in the library"—yes, it is intended in that illogical order. With the Internet, the "1 day in the library" is probably about "10 minutes online." A little background research could help you find previous work and both learn from the past and also start your work in an optimal direction.

After clearly defining and documenting the definition and scope of the research question, it is important to review currently available internal and external insight, methods, or resources. While fraud may be new to the food industry, product fraud prevention is not new to all of industry. There are 30+ years of experience addressing some aspects of fraud prevention-related work in many industries such as pharmaceuticals, personal care products, luxury goods, apparel, or even currency.

Because the question is new to you or your industry does not mean it is new for the world.

There are several examples of technology moving faster than the understanding of the root cause and the resource-allocation decision-making mechanism. For example, around 2006, radio-frequency identification (RFID) technologies were the hot technology that was perceived to be the magic bullet solution for traceability. As food safety traceability is a regulatory push in 2017 (re FSMA and previously the "one step forward and one step back" in the Bioterrorism Act of 2002), the US Prescription Drug Marketing Act of 1987 was that push due to mandated serial number-based traceability systems (as of 2018, the PDMA is still in limited stages of implementation not because of the package level capabilities but more straightforward challenges such as a single coding system, interoperability, data sharing concerns, and database security). Later in 2006, Wal-mart made a big push stating their "early adopter" intent to apply machine-readable automatic identification (Auto-ID) and RFID technologies. The number of Auto-ID or RFID vendors at the PackExpo packaging exposition boomed over about 2 years to the point there was an entire floor of the massive Chicago McCormick Place conference center dedicated to just the technology. While the frenzy has passed with little of the projected benefits, there is a wealth of experience and expertise in selecting, implementing, and managing new technology or solutions. The food industry can learn from the previous projects implementation successes and failures.

For food fraud prevention, systems and services are being developed to support a wide range of prevention needs. Some products or services provide insight on incidents while others help with assessments and then others support enhanced traceability.

To find case studies or successful implementation examples, an extensive literature and marketplace search is very efficient if you have your needs and scope clearly defined. You may find that the most efficient and effective resource is from outside your industry.

Product fraud is new to the food industry, but it is not new to all industry. Since at least the early 2000s, the pharmaceutical industry—including the drug side of the US Food and Drug Administration—has been conducting coordinated internal and external security activities. The drug industry has a long history of traceability, serialization of products, and end-to-end digital traceability. The US Prescription Drug Marketing Act of 1987 was the first effort to create this program. Additional US laws and regulations have further refined the focus and activities such as the Drug Supply Chain Security Act (DSCSA) of 2013 (Public Law 113-54 2011). The food industry—including the "food" side of agencies such as the EU DG-SANCO and US Food and Drug Administration—can learn a lot from their counterparts. By reviewing the past—the good and the less efficient—hopefully the food industry can both avoid pot-holes but also leapfrog to the next generation of prevention-focused activities.

Any proposal or project that does not begin with a thorough literature or research review is beginning as a guess and hoping for "dumb luck" to succeed.

Key Learning Objective 2: A Prefilter or Food Fraud Initial Screening (FFIS)

This section reviews the prefilter or Food Fraud Initial Screening tool (FFIS) which was created and published in response to an unmet research need (Spink et al. 2016). While there are many ways an assessment can be started, the FFIS began with understanding the need (e.g., compliance for GFSI, ISO 31000, FSMA, Sarbanes-Oxley, and others), acceptance of the very limited human and financial resource allocation (e.g., often a new assignment piled on top of other food quality or food safety job responsibilities), the limited and uncertain base incident data available or collected, and the other Food Fraud Vulnerability Assessment products, services, tools, and methods.

The Key Learning Objectives of this section are:
- (1) Review the foundational concepts of the FFIS.
- (2) Conduct a brief overview of the FFIS tool and method.
- (3) Consider the final presentation of the assessment and address the resource-allocation decision-making process.

The next sections will present the methods including the initial screening and detailed vulnerability assessment.

Introduction to the COSO Initial Screening: Food Fraud Initial Screening Tool (FFIS)

For vulnerability assessments, there is a range of actions from very casual and qualitative to the other extreme of very formal and quantitative. The COSO Enterprise Risk Management system describes a two-stage process of an initial screening and then a detailed assessment (COSO 2011). From COSO:

- "This [risk assessment following the event identification] may be accomplished in two stages where an initial screening of the risks is performed using qualitative techniques followed by a more quantitative analysis of the most important risks."
- "Risk assessment is often performed as a two-stage process. An initial screening of the risks and opportunities is performed using qualitative techniques followed by a more quantitative treatment of the most important risks and opportunities lending themselves to quantification (not all risks are meaningfully quantifiable)."

This theory and terminology were used to create the Food Fraud Initial Screening Tool (FFIS) (Spink et al. 2016). The initial screen has also been referred to as a prefilter or first-step assessment. While the desired outcome for risk mitigation planning includes detailed vulnerability assessments, broader initial screening can

make the process much more manageable. Often a detailed, by-individual-product assessment is not practical due to the nature of the risk, the time allotted, or the detail needed for resource allocation and decision-making (Spink et al. 2016).

The FFIS is an efficient way to start with a review of the entire company. The important step is to complete the first assessment to identify where the more detailed investigation is necessary. Also, many compliance requirements already require "an" assessment but have no specification for the depth or breadth. For example, the basic GFSI requirements published in 2017 only require that an assessment is conducted and documented. A conversation was overheard at a conference where a company said: "our detailed vulnerability assessment will take five years"… the response was "that's nice, but it was due two months ago."

Introduction to the COSO Detailed Assessment: Food Fraud Vulnerability Assessment

The initial screening addresses the assessment from an overarching view of the entire operation, while the FFVA builds up from reviews of specific assessments by product/supplier/manufacturing location (Table 17.1).

Table 17.1 Attributes of the FFIS and FFVA

Food Fraud Initial Screening (FFIS)	Food Fraud Vulnerability Assessment (FFVA)
Initial screen/prefilter	Detailed assessment
Company level perspective downward	Supplier/product level perspective upward
Minimum acceptable activity as small as a group of subject matter experts	Maximum activity as detailed as an assessment for every supplier, product, package style, manufacturing location, and supply route
Qualitative	Quantitative (if each data point is generated from a test of some kind) though some are semiquantitative, but actually most would be still considered qualitative (since the individual questions may also be qualitative (Note 1))
Number of assessments: minimum one assessment matrix for raw materials and one for finished goods. The FFIS typically has a minimum of 25 cells per matrix. With a two-matrix process, this would be 50 assessments with a likelihood and consequence that equates to the overall, enterprise-wide risk assessment	Number of assessments: maximum could be for every supplier/product/manufacturing locations/supply logistics item. A medium-sized food company with 100 ingredients from 3 suppliers and 3 logistics methods could reach 900 assessments. If the FFVA has 30 questions each, then there could be 27,000 data points

Note 1: See Fejes and Spink, 2011, presented in the sidebar section "So, How Big Is the Food Fraud Problem? *Unknowable*!" That publication found that each of the quantitative estimates of the economic impact of counterfeiting and piracy was either without a citation or based on a core estimate of "5–7% of world trade." Thus, the high-level statistical analysis conducted was based on a guess where a 1% error for the 2017 World Trade Organization estimate of world trade exports at $15 trillion would be plus or minus $150 billion

Once a holistic and all-encompassing FFIS assessment is conducted that covers the entire enterprise, then the specific additional data collection needs can be determined.

Sidebar: "Enterprise-Wide Assessment" or "COSO Enterprise Risk Management (ERM)"

Be careful when using new terms or phrases. The COSO/ERM concepts are new to many food safety risk assessors. COSO/ERM is a formal, regulatory, certification based concepts that often have legal ramifications. It is very important to be very careful with risk terminology.

A frequent conversation goes like this:

- Generalist: "Oh, I know all about enterprise-wide assessments."
- Expert: "Wow, I'm impressed you're experienced with managerial accounting regulations."
- Generalist: "Oh, not that."
- Expert: "(Silent but thinking) Ok, so you really do *not* know what you're talking about."

Yes, the idea of considering how risks are related to all the risks of an enterprise is a general concept, but it is not "Enterprise Risk Management (ERM)."

Another more dangerous conversation demonstrates an unintentional shift from general concepts to inadvertently offering legal, regulatory compliance advice is related to the Sarbanes-Oxley Act. A common statement could be "Now we will consider how the food fraud risk compares to other risks across the company. These impact the enterprise. Food fraud is an enterprise-wide risk. So we will now present Enterprise Risk Management." This seems like a natural flow, but the word "Enterprise Risk Management" shifts this casual statement to a formal term that possibly has legal ramifications. Using the term incorrectly might be like telling an FDA inspector that you have a plan to analyze and manage risks, so you cook your product to 160F. "It's a HACCP plan." Wait, is it a formal official auditable "HACCP" plan or just something you decided to do? In reality, it is *not* a HACCP plan. Stating it as a HACCP plan could create legal or regulatory liability. Thus, it is important to state whether the assessment is really ERM or just a general broad assessment.

Before moving on, and continuing here to review ERM/COSO, a question is "Does your job require expertise?" Is there a critical aspect that comes from years of experience? ERM/COSO is a formal regulatory requirement. Don't just assume your current expertise will suffice.

Sidebar: Developing Assessment Scales and Outputs

This section will build upon previous ISO and criminology discussion on qualitative and quantitative assessment to now review several basic aspects of model development.

Regarding the assessment scales, a quote from the FFIS research article is provided including "meaningful differentiation" and the recommended "five-point scales" (Spink et al. 2016):

> "Applied to the research question in this paper, an important aspect of developing assessment criteria is defining the ranking scales. 'Scales should allow meaningful differentiation for ranking and prioritization purposes. Five-point scales yield better dispersion than three-point scales. Ten point scale imply precision typically unwarranted in qualitative analysis, and assessors may waste time trying to differentiate between a rating of six or seven when the difference is inconsequential and indefensible' (COSO 2011). This statement presents several key concepts. First, meaningful differentiation refers to fidelity in the data meaning that the result provides a clear and appropriate presentation of the risks. Unless all the risks are the same or very similar, which could be the case, the risks should be presented on a scale that can quickly and visually present the differences." (Spink et al. 2016)

Regarding numbers versus words, a quote from the FFIS research article is provided (Spink et al. 2016):

> "Another important COSO concept for developing assessment scales is implied precision. This is the rationale for defining scale attributes with words (e.g., "Low") and not as number values (e.g., "3") (also see [REF Cox, 2009; Hassenzahl, 2006; Jablonowski, 1994]). Often the core data input for assessing food fraud vulnerabilities is qualitative incident data. This enables the FFVA to apply the qualitative judgment of what constitutes "very high" or "very low" risk. Numbers could be used to aggregate and sort the risk ranks, but the final presentation should shift back to qualitative or word results. Presenting numerical results could "imply precision" that is unjustified." (Spink et al. 2016)

Regarding "implied excessive precision," a quote is provided (Spink 2009):

> "Another key concept that is related to implied precision is indefensible values or positions. Managing enterprise risk can appropriately generate rigorous debate surrounding competing risks or countermeasures that often involve significant resource allocations. The decisions and the data must be defensible. As long as the foundation is clearly stated it is acceptable if such assessments are qualitative and have limited accuracy or precision. Data uncertainty is common in early stage assessments of risk, and thus evaluations should be considered qualitative, not quantitative."

Regarding quantitative and qualitative assessments addressed in government documents, a quote from a research article is provided (Spink 2009):

> "An example of this comes from the US Government Accountability Office (GAO). They reviewed the methods used to assess the economic impact of counterfeiting and piracy (GAO, 2010). The GAO report concluded that there were no quantitative, statistically supported methods to conduct such an assessment. The GAO report missed the opportunity to support qualitative assessments such as those espoused in COSO. The challenge for anti-counterfeiting research and assessment is that it con-

(continued)

> tinues to be presented as analytical, quantitative data. The assessments have been indefensible in some situations such as testimony by the Director of the US Office of the Intellectual Property Enforcement Coordinator (IPEC) to a US Senate subcommittee (see discussion and transcript highlights below and in (Spink and Levente Fejes 2012)). The estimates would probably be defensible if they were presented as qualitative." (Spink 2009)

Regarding an example of an actual challenge during an open Senate testimony (Spink and Levente Fejes 2012):

> "This need was reiterated in U.S. Senate Testimony by Victoria Espinel, the Director of the U.S. Office of the Intellectual Property Enforcement Coordinator (IPEC), Office of Management and Budget (Espinel, 2011). When pressed by the Senators for quantification or even an order of magnitude [of the economic impact], her response aligned with that GAO report: "So I would say it is very difficult to quantify precisely the impact of infringement on our economy because infringement… is illicit activity and it is difficult to quantify". (Senate Hearing 111-847, 2011)"

> "When further pressed for even 'Orders of magnitude, tens of millions of dollars, tens of billions of dollars, trillions of dollars?' She responded in 'It is not my nature or inclination to speculate without precise data.' Ms. Espinel did refer to upcoming U.S. International Trade Administration analysis (though both reports eventually only reviewed China) (USITC 2011, USITC 2011). The string of questions concluded with 'Well, let me jump in and ask that you conclude your answer on that in the form of a written response to a question for the record, to get back with whatever data you have.' IPEC and the Senate Subcommittee have not published a public response. Neither IPEC nor others have published or referred any new initiatives on assessing the economic impact of counterfeiting."

These examples consider the risk of presenting estimates as quantitative, analytical, or statistical where, when pressed, the underlying data set is often built on qualitative assessments or wild guesses. The application to food fraud prevention is that starting with a qualitative assessment—as long as the method and challenge of the underlying data set is explained—is an efficient and effective starting point. Once this starting point is achieved, the resource-allocation decision-makers can ask for more information if needed. Academics and scientists are more comfortable with precise analytical data sets, but often there is not enough time, the effort to gather "enough" data is too costly and requires a deep understanding of the underlying root cause. The FFIS combined with the resource-allocation decision-making method in ERM and presented in the Food Fraud Prevention Cycle provides a holistic and all-encompassing system.

It often seems that a prefilter or initial screening, a qualitative assessment, is way too simple, but it is a legitimate process and at least creates a manageable starting point.

Sidebar: Review of USITC 1988 Report on IPR Crime Impact on the US Economy (1541)

Title: Review of USITC's Foreign Protection of Intellectual Property Rights and the Effect on US Industry Trade Report of February 1988, by John Spink, Internal MSU Report, January 17, 2011

It appears that the earliest reference to quantifying the economic impact of counterfeiting and piracy is the US International Trade Commission (USITC) Foreign Protection of Intellectual Property Rights and the Effect on US Industry Trade Report of February 1998 (covering surveys for 1986). This does refer to previous Commission's study on The Effects of Foreign Product Counterfeiting on US Industry (USITC Pub. 1479, January 1984, "out of print" but hardcopy received through Freedom of Information Act request); however limitations were noting "the primary focus of that study was on foreign product counterfeiting; licensing revenues and service industries were not included in the study." The other early report is the Counterfeiting Intelligence Bureau report in 1997, which does not include mentions of other methods. As a reference for the time frame, the World Intellectual Property Organization (WIPO) defined counterfeiting in 1996 (CIB 1997). The World Trade Organization (WTO) first Trade-Related Aspects of Intellectual Property Agreement (TRIPs) definition was developed in 1993–1994. The CIB 1997 notes the earliest criminalization of counterfeiting in "the early 1980s," including the US Trademark Counterfeiting Act of 1984, and they refer to the future TRIPs agreement.

> "The [USITC] was asked to develop, to the extent possible, quantitative estimates of the distortions in the US trade associated with deficiencies in the protection provided by foreign countries to US intellectual property rights, including trademarks, copyrights, patents, trade secrets, semiconductor chip designs [also defined as mask work, or the design of the chip architecture], proprietary technical data [e.g. included in regulatory paperwork or patent requests] and other types of intellectual property rights."

The report and estimates were developed from questionnaires sent to 736 US companies including all the largest 500 publically traded companies. It is very interesting and important that the USITC stated:

- "The data, therefore, represent estimates from a percentage of an unknown universe; the losses suffered by the US industry as a whole may well be much larger."
- A third of the respondents stated IP was *not* important to their business.
- "Infringing product sales" were in $9.5 billion, including copyright violations. The trademark violations were $5 billion in lost sales and $754.9 million in lost profit—it is a key point that they made the distinction of revenue versus profit. Later they state "counterfeit sales imply some loss of revenues."

(continued)

- The USITC continually emphasizes that the "discouragement of investment represents a social loss in that fewer new or improved products will be available in the future." The damages were very broad and beyond the usual sales numbers included:
  - Fees or royalties not paid.
  - Reduced profit margins.
  - Damage to reputation or trade name.
  - Research costs not recovered.
  - Research or business foregone (opportunity cost).
  - Weakening of sales of other product lines.
  - Enforced reduction in plant efficiency.

Interesting for future reference, the annual 1986 loss for pharmaceuticals was $1.9 billion, and loss for food and beverages was $86 million.

The surveys identified a loss of 5374 US jobs, with half in the software industry, 478 in electronics, and 22 in the pharmaceutical industry.

Regarding the methodologies, "The Commission could identify no better means of developing estimates than asking a broad range of firms in the industry's most probably affected for the core evidence on US losses from inadequate intellectual property protection – estimates that could admittedly be biased and self-serving."

Appendix F was titled "Calculating the Effects of Counterfeiting Sales on Output, Total Revenue, and Profits of Legitimate Producers." This Appendix included methodologies which focus on deceptive counterfeits (perfect substitutes of the genuine article) and that assumed the amount of counterfeits are known.

For a company to estimate their loss in revenue they would require the data inputs of:

- Sales in a defined market (usually known, includes diversion).
- Value of counterfeit sales in a market (usually not very well known, if at all able to quantify in any meaningful or statistically significant level).
- Profit per unit of sales (known).

Counterfeiting is described as to reduce demand by competing with the legitimate product. Further model development by other researchers (not the USITC researchers) often assumes counterfeits *are* a *perfect* substitute for the legitimate product, or what would be defined as deceptive versus non-deceptive counterfeits. This USITC model does not consider non-deceptive counterfeits since they are assumed not to reduce the sale of a genuine product.

> "For example, if counterfeit blue jeans are sold from the back of a truck on a street corner, they are actually different goods from blue jeans of the identical material and

styling sold in a fashionable retail outlet." The model appears to adapt supply and demand economics using the counterfeiter as the perfect substitute competitor."

Both methodologies are only presented, for example, and no assessments are included or used.

Appendix H (Protection of Losses from Inadequate Intellectual Property Protection for all US Industries) clearly states that this assessment is only for US companies impacted from international counterfeiting:

- "Because the [survey] sample did not provide a statistically verifiable basis on which to project this loss estimate (based on a sizeable but still fractional sample of the US firms) to the total of susceptible transactions, we did not attempt to make such a projection has not [sic] been included in the body of this report."[…]
- "The data collected by the Commission's questionnaire cannot be projected to US industry as a whole with any statistical validity. This is due to two characteristics of the samples and universe involved:
  - (1) The universe of all US businesses is unknown;
  - (2) The sample of questionnaire recipients was not randomly-drawn; and
  - (3) Those companies responding to not represent a random sample (of either all companies or all those sent questionnaires)."[…]
- "However, one can illustrate a likely range of aggregate losses from inadequate foreign intellectual property protection by making a number of assumptions concerning properties of both responding and non-responding companies. […] The range of possible estimates is wide. At the bottom end, to assume that companies not surveyed had no losses gives a $24 billion loss estimate. […] At the high end, to assume that firms not surveyed experienced the same ratio of losses to sales as those surveyed would give an estimate of $102 billion. Neither is this a reasonable assumption because our sample concentrated on industries and firms known to have the greatest problems with intellectual property losses."

From the extensive analysis, it was estimated that "For all [US company] respondents then, estimated losses would be 1.9% of worldwide sales." And "Thus, it is estimated worldwide losses to US industry would range from inadequate foreign protection of intellectual property rights would range from $43 billion to $61 billion. It should be stressed that this figure may be 'reasonable,' but its limitations and lack of statistical validity should be kept in mind." The Appendices and the report end on that statement.

The conclusion is that:

- There was a small response to the survey with 431 of 736 companies responding (58%).

(continued)

- Less than half of those who did report reported losses with 198 of the 431 companies (46%) reported the $23.8 billion in losses, whereas 233 companies did not report or did not report losses (54%).
- Although companies reported under oath, and a meta-analysis was conducted to review the estimates, there was no methodology outlined or defined for providing responses.

For reference, here is the full USITC 1988 text regarding the counterfeit product as a substitute (emphasis added):

- "At first face, the above analysis does not appear well suited to many counterfeit cases, because counterfeit goods often sell at a price that is much lower than that of the genuine article. However, on closer examination, this objection does not appear to seriously detract from the analysis. The counterfeit units used in the analysis are perfect-substitute equivalents of the more expensive genuine article. For example, if counterfeit blue jeans are sold from the back of a truck on a street corner, they are actually different goods from blue jeans of the identical material and styling sold in a fashionable retail outlet. Jeans bought from the retail outlet can usually be tried on for fit, and the consumer may be able to return the jeans if he finds later that they are flawed or if he simply changes his mind. Also, the retail outlet is likely to have a more pleasant ambiance, regular hours, and a well-advertised location. Locating the counterfeit supply may impose some information costs on the consumer because a well-advertised, stable location for the counterfeiter would increase the likelihood that he would be detected and punished. If the consumer knows the product is counterfeit, he may also feel moral qualms about engaging in an illicit transaction. These are all attributes of a good that makeup part of its price. If counterfeiters are able to supply an entire market with goods that are perfect-substitute equivalents and lower priced than the genuine article, we should expect to see the legitimate producer forced out of that market entirely."

Sidebar: Application of Qualitative, Quantitative, or Semiquantitative Assessments

At the start of research on food fraud, the assessments seemed to mirror quantitative, data-intense food safety risk assessments. As the food fraud assessments were first being considered, there seemed to be a belief or assumption that there was "enough" of the "right" data to conduct the detailed quantitative assessments (Spink et al. 2019). The food fraud assessments built upon food science methodologies that are not from the probably more appropriate crime assessments or business enterprise risk assessments.

For food fraud prevention there has been a focus on quantitative and by-individual-product assessments. These are valuable and are placed in the context of the stages of assessment. Some advantages and disadvantages of both qualitative and quantitative analyses are further described by COSO (COSO 2012):

- **"Qualitative**
  - Is relatively quick and easy to implement
  - Is easily understood by a large number of employees who may not be trained in sophisticated financial modeling techniques
  - Results in limited differentiation amongst levels of risk (e.g., a macro assessment)
  - Is imprecise—risk events that plot within the same risk level can represent substantially different amounts of risk.
- **Quantitative**
  - Allows for financial aggregation taking into account risk interactions when using an at-risk measure such as Cash Flow at Risk.
  - Can be time-consuming and costly especially at first during model development.
  - Other qualitative impacts or factors may be overlooked when they cannot be meaningfully quantified.
  - Quantification (e.g., rankings of "7" vs. "8" compared to "medium" vs. "low") may imply greater precision than the uncertainty of inputs justify."

Application of the Assessment and Supporting Resource-Allocation Decision-Making

The basic FFIS steps are to develop assessment criteria (e.g., details of likelihood and consequence), identify risks, assessment of risk components, combine the risk assessment, and then risk aggregation and evaluation in relation to all other enterprise-wide risks.

Prework is conducted before starting the assessment. Reviewing these concepts before considering any likelihood or consequence of judgment is important. If the vulnerability or risk assessment is presented early in the process, the risk assessors usually cannot help leaping ahead to consider risk treatments. It is recommended to separately and specifically "develop assessment criteria" *before* reviewing incidents.

Develop Assessment Criteria: Several factors are critical to the FFIS process.

- **Likelihood details for very high to very low:** This includes details such as the number of lost sales, the public health hazard level, amount of market share lost, regulatory penalty level, legal liability lawsuit level, etc.
  - **For incoming goods:**
    - **Products:** identify five types of products with one category including "other."
    - **Markets or channels:** identify five types of markets or channels with one category including "other." The market could be raw materials from a country or region (e.g., Canada, etc.) or a specific type of supplier (e.g., major food manufacturer, broker, etc.)
  - **For outgoing goods:**
    - **Products:** identify five types of products with one category including "other."
    - **Markets or channels:** identify five types of markets or channels with one category including "other." The market could be in the end markets for a country or region (e.g., Canada, etc.) or a specific type of supplier (e.g., major food retailer, broker, etc.)

Identify Risks: Next would be to conduct a review of risks. The level of certainty and robustness does not—repeat *not*—need to be high at the start. Consistent with COSO guidance, many successful programs started with nothing more than experts in a single meeting. It is important to note that the report should clearly identify an estimated level of "certainty," "robustness," and the risk assessment team.

Beyond expert insight, the events could include:

- Known food fraud incidents at this entity.
- Known food fraud incidents in a similar company, same industry, or related product.
- Product fraud incidents in other industries but for the somehow related product (e.g., liquid chemicals and liquid food products).
- Then vulnerabilities identified through scanning which could include market price fluctuations, supply irregularities, etc.
- Another factor is public policy changes where a new focus could lead to more oversight or testing that could increase detection.

Assessment of Vulnerability or Risk: The assessment is conducted for incoming goods and a separate assessment for outgoing goods. One matrix is created for each of the two types of goods (Fig. 17.5). Of course, more than five categories can be used, but more categories increase the complexity. Also, more detailed matrixes can be created. For example, consider that cell "A2" in the final incoming goods matrix one cell could be "meat" from "Europe." That could be expanded into another 5x5 matrix listing European countries versus different types of meat (e.g., beef/pork, poultry, seafood, ground meats, and processed meats/meal/powder/other).

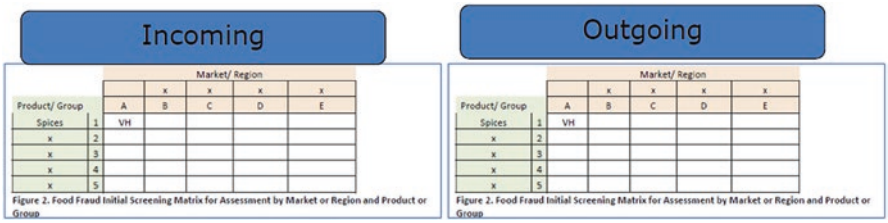

Fig. 17.5 Example of the FFIS matrices for incoming and outgoing goods. (Copyright Permission Granted) (Spink et al. 2016)

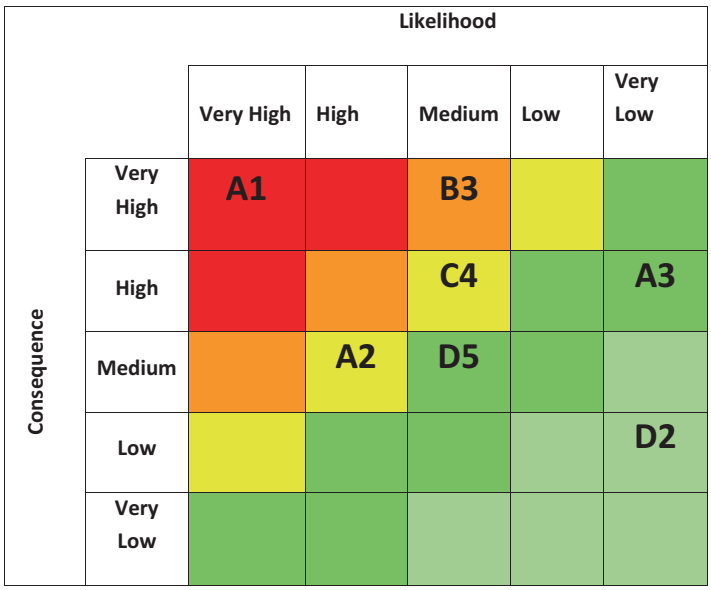

Fig. 17.6 Corporate risk map plotting Food Fraud Initial Screening risk assessments. (Copyright Permission Granted) (Spink et al. 2016)

Risk Assessment: Once the factors and categories are plotted on the matrix, then the risk assessment can occur. To start, a quick assessment of the entire matrix is efficient. Identifying the assessment certainty and robustness is important. For example, "Certainty: 1/10" and "Robustness: 1/10." It is important to document how each cell rank was determined and also if/what additional information is needed. For example, maybe none of the experts has experience selling a product in the country of India. For each cell, the "likelihood" and "consequence" would be estimated.

Risk Aggregation and Evaluation: A specific risk assessment is a static estimate that is not compared to any other problem in the enterprise. While the risk ranks were identified, the overall conclusions had not been calibrated or tested. To "connect everything to everything," it is recommended by COSO/ERM to plot the risks on an enterprise-wide assessment usually in a corporate risk map (or risk heat map) (Fig. 17.6) (COSO 2012). (Note: The corporate risk map originally included the

colors red/orange/green/blue but changed to red/orange/green/light green since a more complex COSO investment matrix uses the blue color for all positive return opportunities.)

The FFIS process is completed when the vulnerabilities or risks are plotted on the corporate risk map. The process is documented and the meeting attendees recorded (when considering an audit, it didn't occur if it wasn't documented"). For the full enterprise supply chain, this is a complete Food Fraud Vulnerability assessment, it is documented, it covers all types of products, and it addresses all types of fraud. Technically that meets the GFSI food fraud requirement.

Sidebar: ERM/COSO Examples and Definitions of the Likelihood and Consequence Details

An example of the likelihood details is provided from a COSO report (Table 17.2) (COSO 2012).

An example of the consequence details is provided from a COSO report (Table 17.3) (COSO 2012).

These are general examples of the likelihood and consequence provided by COSO and can be helpful in creating a starting point.

Table 17.2 Illustrative likelihood scale with definition from COSO (2012)

Likelihood	Detail
Very high	Up to once in 2 years or more
High	Once in 2 years up to once in 25 years
Medium	Once in 25 years up to once in 50 years
Low	Once in 50 years up to once in 100 years
Very low	Once in 100 years or more

Table 17.3 Illustrative impact scale with definition from COSO (2012)

Consequence	Detail
Very high	Financial loss of $X million or more International long-term negative media coverage; game-changing loss of market share Significant prosecution and fines, litigation including class actions, incarceration of leadership Significant injuries or fatalities to employees or third parties, such as customers or vendors Multiple senior leaders leave
High	Financial loss of $X million up to $X million National long-term negative media coverage; significant loss of market share Report to regulator requiring a major project for corrective action Limited in-patient care required for employees or third parties, such as customers or vendors Some senior managers leave, high turnover of experienced staff, not perceived as an employer of choice

Table 17.3 (continued)

Consequence	Detail
Medium	Financial loss of $X million up to $X million National short-term negative media coverage Report of breach to the regulator with an immediate correction to be implemented Outpatient medical treatment required for employees or third parties, such as customers or vendors Widespread staff morale problems and high turnover
Low	Financial loss of $X million up to $X million Local reputational damage Reportable incident to the regulator, no follow-up No or minor injuries to employees or third parties, such as customers or vendors General staff morale problems and increase in turnover
Very low	Financial loss up to $X million Local media attention quickly remedied Not reportable to the regulator No injuries to employees or third parties, such as customers or vendors Isolated staff dissatisfaction

Key Learning Objective 3: FFVA and Presentation of Results (5265)

This section reviews the preparation, management, and communication of the results of an assessment. This section is not intended to be a review or judgment of Food Fraud Vulnerability Assessment (FFVA) tools, methods, or systems since it would be inefficient to cover that detail here since the science and application are changing so quickly that the insight or recommendations would quickly be outdated. That said, there are some basic concepts or principles that will always apply.

Key Learning Objectives of this section are:

- (1) Review the Food Fraud Vulnerability Assessment and detailed assessment.
- (2) Consider sources of data and "how much is enough" for the current decision.
- (3) Corporate risk map summary and presentation.

Food Fraud Vulnerability Assessment (FFVA) Which Is a Detailed Assessment

Based on the ERM/COSO principles, there is a continuum for the two stages of vulnerability assessments from the first stage which is an "initial screen" and then a "detailed assessment" that is presented here as a Food Fraud Vulnerability

Assessment (FFVA). The full continuum spans from one vulnerability assessment for an entire enterprise to the other extreme which could be one assessment for each product/supplier/manufacturing location. A top 100 multinational food manufacturer could have 1000 suppliers and purchase an average of 10 products from each supplier. In turn, each supplier could have an average of three manufacturing facilities for each product. To address the detailed end of the spectrum, a food company would be required to conduct 30,000 individual and separate vulnerability assessments. It is estimated that just saying the name of each of those manufacturing facilities could take 25 hours (e.g., based on 30,000 names that take 3 seconds each to pronounce). This would be a realistically impossible task; alternatively, the human and financial resource justification would need to be very well defined and supported. There may be unique vulnerabilities, but there is probably a logical balance of specificity and reality. That said, there is a documented method to define why the level of detail decided was practical and logical.

Databases and Sources of Information

To review databases and sources of information, this section will focus on the overall specifications and utility rather than individual available databases. These food fraud products and services are not reviewed in detail since they are changing so fast that as soon as a book is published, the insight will be obsolete (actually, during the writing of this book, several of the commercially available food fraud incident databases underwent significant changes, reductions, expansions, or consolidations). The underlying needs and specifications of the user will be consistent.

As has been emphasized throughout this chapter and this book, the "right" data set is defined by assessment needs. The scope of the research question defines the assessment needs (e.g., adulterant substances or all types of food fraud), the decisions (e.g., presenting trends for discussion or initiative for a recall of products from around the world), or the needs of the resource-allocation decision-maker (e.g., some managers, or for some decisions, require more or less information).

In general, there are many sources of information that are logical even if they seem very casual or informal: subject matter insight, known incidents with the company, databases, and Internet searches (Table 17.4) (Spink et al. 2016).

While analysis of the specific databases is outside the scope of this work, it is essential to review the sources of information and types of data gathering methods (Table 17.5).

It is efficient to identify the research question and then start assessing the available data sources. There may be no single data set that includes all products or that is updated on a frequent enough basis (for more, see the section on Introduction to Data Analytics).

Table 17.4 Sources of data for the Food Fraud Initial Screening (FFIS) and Food Fraud Vulnerability Assessment (FFVA) (Spink et al. 2016)

Information source and detail
Subject matter expert insight
Known incidents within the company (i.e., internal sources) List incidents List details and costs if known
Databases (i.e., static external sources) Review product recall information (i.e., company, product group, industry, etc.) Review food fraud or related databases
Internet searches (i.e., dynamic external sources) General Internet searches (i.e., by individual products, etc.) Set up automated Internet keyword alerts (e.g., ongoing Google Alerts, etc.)

Note: This content would usually be described by regulators such as FDA as "science-based" since it is published in a peer-reviewed, refereed, scholarly journal. "Science-based" is not just "a group of scientists" who made a decision

Table 17.5 Review of FFIS information gathering details such as databases and sources of information

Databases and sources of information
Recall and incident information: These are public government statements, or their summaries consolidated by-product supplies.
Incident databases: These are reviews of information summarized and presented. The incidents could be from many sources and also include a wide range of detail. A key is to understand whether the database includes: 1. Your specific supplier/product/country item 2. The robustness of the data search 3. Frequency of assessment. For an urgent incident review, this could be a starting point that is supported by a review of current product recall information or an immediate internet search
Market monitoring: These are reviews of changes in the marketplace such as price changes, product shortages, or consumer concern on social media. These provide insight that possibly influences the macro-level "fraud opportunity."
Internet searches: An internet specific keyword search can evaluate a wide range of sources and identify if "anything" is publically known. This can be an excellent resource during an urgent incident review or research on suspicious activity.
Internet keyword alerts: An automated process can be to set up keyword alerts to be passively made aware of possible concerns.

Sidebar: Estimates of Product Counterfeiting—Same Challenges for Food Fraud

There is an Aesop's Fable "Belling the Cat" that proposes impossible solutions. In the fable, a group of mice proposes to put a bell on the pestering cat. The problem is that no one offered a solution as to how to get the bell around the cat's neck. The idea is excellent and effective, but there was no consideration of the implementation. Estimating the economic impact of counterfeiting and piracy sometimes seems like belling the cat.

(continued)

Before developing an assessment model, it is wise to consider the available data. A proposed utopian model may require a mythological data set that does not exist. A frequent misperception—regardless of what may be stated publically—is that most companies do *not* have the ability to quantify their product fraud risks or costs accurately. They know what has been reported to them, but they face the same challenges as their predecessors of gathering useful data. Over time, and based on identifying unmet needs, they can refine their process to understand their vulnerabilities better.

In many situations, this type of assessment is trying to quantify the "unquantifiable" or to try to "know" the "unknowable." Ok, it may be technically possible to gather enough data, but in reality, it would be cost prohibitive. A key consideration is "cost prohibitive" in comparison to "how much is enough" for the current resource-allocation decision-making.

Compared to other risk or threat assessments—such as food safety, food defense, or also terrorism—the fraudster does not "need" to act, so there is an undefined threat of the incident; there are a wide range of types of attacks, so the consequence is also usually undefined; and finally this combines to make the consequence very uncertain. However, this has not been an insurmountable hurdle because the shift from economic impact to vulnerability is a common factor already in place in a company under a CSO/ERM system.

Finally, the most important fallacy is that there is an assessment that already integrates into the resource-allocation decision-making system ("There must be? Right?"). There is a belief that "someone else" does that integration. Well, I would challenge to ask "who?" Do you "know or think" that someone does that integration? What is their name? Have you have confirmation that their key job responsibilities include meeting your exact question or the specific compliance requirement? Also, does your current risk assessment actually help them?

Any proposed model that does not include an application case study—including the final and actual resource-allocation decision-making—is not really that helpful. Hypothetical examples are often incomplete and cause either dangerous assumptions that it is already being conducted or frustration when the risk assessor cannot figure out how to answer the question.

Sidebar: Inconsistent Sources of Data

When researching the methods to assess the economic impact of counterfeiting and piracy, details of the inconsistent sources of data were determined (Spink and Levente Fejes 2012). Several examples are presented:

> "**Seizure data and interdiction rate**: 'Seizure data reports are not considered as core documents because they only represent what has been caught and not an estimate

of the entire counterfeit product marketplace.' A quote is from the US GAO 'We wouldn't consider the seizure rate to be a random sample of the extent of counterfeit goods coming in [to a country].' Moreover, then, the USITC stated 'The data, therefore, represent estimates from a percentage of an unknown universe.' "

Challenges of Using Seizure Data: Regarding seizure data and published reports, there are often even challenges of getting *any* data. While the most basic customs data such as seizure amounts and rates may seem like "just a fact," even sharing what seems like the most basic and sterile information or data is a challenge. For example, the customs survey used in the OECD counterfeiting and piracy survey was sent to 169 World Customs Organization members with 70 responses (OECD 2007). For the general country survey sent to the 30 OECD member countries, there were 20 responses. From the OECD report (OECD 2007):

- "Caution must, of course, be exercised in interpreting the results of surveys, as participants may not necessarily report fully or truthfully on their activities, particularly if these activities involve unlawful deeds. While these limitations need to be kept in mind, the value of surveys in suggesting patterns and changes over time should not be underestimated" (OECD 2007).
- "The general lack of data with respect to counterfeiting and piracy activities necessitates that more information on the phenomenon be developed. One of the most promising sources of information in this regard currently concerns seizure statistics as registered by customs authorities around the globe. Apart from being collected on a systematic basis, in most cases, these data also constitute the only official data that exist on infringement activities. Hence, despite their apparent shortcomings, they currently constitute the best foundation for measurement analyses as far as counterfeiting and piracy issues in a global context are concerned" (OECD 2007).
- "Answers to the survey ranged from being limited in their usefulness for developing information on infringement activities to being very detailed and thus of great value with respect to the analysis. Of the 70 responses received, only 45 economies [countries], provided information detailed enough to allow a more elaborate assessment of the counterfeiting and piracy activity. The number of data records submitted varied largely across economies" (OECD 2007).

The report noted analysis based on 19 reporting countries including "Andorra, Angola, Australia, Cyprus, Denmark, Estonia, France, Germany, Japan, Latvia, Mauritius, Netherlands, New Zealand, Portugal, Korea, Romania, Spain, the UK, and the USA." Notably missing some of the biggest economies in the world including China, Hong Kong, Brazil, Russia, India, as well as EU-15 countries of Austria, Belgium, Finland, Greece, Ireland, Italy, Luxembourg, Portugal, and Sweden.

(continued)

Data Representative of the Marketplace: Another consideration is if the data received is representative of the marketplace. From the World Customs Organization repoint on capacity building (2007) "An increase in seizures of counterfeit goods might mean that it has become more of a problem; or, more likely, it could mean that IPR enforcement has become more aggressive and thus successful"(WCO 2007). Essentially, more counterfeits are found after there is more effort to find counterfeits. Conversely, an increase in one type of counterfeit product does not necessarily mean that a specific problem is increasing. Often law enforcement or regulatory inspectors shift focus from one product to the next. If counterfeit electric cords were a priority in 1 year and then counterfeit watches in the next, it would be expected that the number of seized counterfeit electric cords would decrease and counterfeit watches would increase. This data of the change in seizures does *not* necessarily indicate a change in the rate of counterfeiting.

From a 2012 article that "A Review of the Economic Impact of Counterfeiting and Piracy Methodologies and Assessment of Currently Utilized Estimates" (Spink and Levente Fejes 2012):

- "Lack of historical data: 'The first challenge is that, compared to many other crimes or quality control defect assessments, there are a very few identified incidents.' Moreover, 'If there are limited or incomplete historical data, any model development would include formulation- or model-errors.' And then 'Furthermore, the counterfeiters evolve their operations quickly, and so there is a question of time-sensitive data perishability where an assessment at one time is not applicable or useful at a future time.'"
- "Data uncertainty: 'The second challenge is that for product counterfeiting, uncertainty refers to estimates that are not necessarily agreed upon as being accurate.' Also, 'These errors are caused by the physical data used to build the models or conduct the assessments that do not represent what is actually occurring.' And finally 'What is seized is not technically a statistically representative random sample of what was actually counterfeited, so there is probably no test of the marketplace that could provide a representative sample of the prevalence of actually counterfeit product.'"
- "Data input and uncertainty: 'The third challenge is that although some products or brands are counterfeited repeatedly, the details of how the infringement occurs can be nearly infinite.'"
- "Model uncertainty: 'A fourth challenge is that due to the evolving nature of the marketplace and the fraudsters, a model constructed from known types of infringements cannot possibly predict every risk.' Then 'Counterterrorism addresses this challenge by focusing on vulnerabilities in addition to assessment and mitigation of known risks.' However, then 'Although the data are uncertain and inaccurate, this is often not a

hindrance to governments and companies taking action in situations where the data are framed as uncertain.'"

In combination, these inconsistent sources of data undermine the ability to conduct advanced statistical analysis or analytics. The nature of the data supports a less formal review method such as a vulnerability assessment rather than something more advanced such as a probabilistic risk assessment.

Sidebar: A Review of the Economic Impact of Counterfeiting and Piracy Methodologies and Assessment (MSU-FFI 2018):

Title: So, How Big Is the Food Fraud Problem? *Unknowable*!

By John Spink • April 3, 2013 • Blog

Quantitative estimates of product fraud are elusive if not impossible to determine. The bad guys don't submit annual reports and don't share estimates of their activities – at least not outside their criminal organizations. We know what we caught, but we have no idea what we didn't catch. Did we only catch the sloppy or the unlucky? There are even legal and cultural debates on "what is fraud?"

This interest in the research question about the estimate of the economic impact of counterfeiting and piracy was sparked during an interview with the US Government Accountability Office (GAO) when they were developing its 2010 report on "Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods." That report found that no quantitative methodology is in use and that the government agencies relied upon industry estimates of counterfeiting. It stated, "it is difficult, if not impossible, to quantify the economy-wide impacts." This report is an important starting point for estimating food fraud and demonstrates the need for additional research, which we have begun through the MSU Food Fraud Initiative.

There is definitely a perception implied by many authors that the product fraud or counterfeiting estimates are quantitative and based on precise, accurate, and certain data. To review this, we conducted a research project on the estimates. The assessments all kept coming back to just three core sources [see Spink and Fejes (2011) A Review of the Economic Impact of Counterfeiting and Piracy Methodologies and Assessment of Currently Utilized Estimates, International Journal of Comparative and Applied Criminology]. In most cases these estimates are often considered quantitative their authors were very clear that their findings were "educated guesses" and one even stated that there were "no methods known to develop an overall estimate." While this research was for intellectual property rights violations of trademark, patent, or copyright, the findings also apply to food fraud.

(continued)

It cannot be emphasized enough that any seizure data is based only on what we caught and that there is probably no way to correlate this with the actual incidents in the marketplace. That is a bold and important statement. In our article, we stated: "The models being used to estimate the impact are being generated from extremely low-frequency events, or if the exact process and method of the counterfeiters is considered, events that have never occurred before." We went on to point out that the data uncertainty was based on:

"(1) The lack of historical data;
(2) The incomplete and often inaccurate nature of available data;
(3) The seemingly arbitrary infringements by the counterfeiters (data uncertainty created by the data generator which in this case is a human); and
(4) The model uncertainty which is also referenced as formulation errors."

Thus, a survey of the marketplace can be valuable as a snapshot of activity in a known, infiltrated, high-counterfeit activity setting… however, a random sampling of the globe would require millions of samples to even approach being considered anywhere near statistically significant.

Even though the quantitative, statistically significant estimates are unknown or unknowable… we do know the vulnerabilities. We can assess how counterfeit or diverted product did get into a marketplace. Although that exact type of fraud incident may not occur again, we can assess whether the system is still vulnerable.

Although the estimates of product counterfeiting and product fraud lack accuracy and precision, this should not be an impossible hindrance to governments or companies taking action. It is important to note that governments do require more quantitative rigor when deciding which projects to fund, but this lack of data hasn't hindered resource commitment in areas such as homeland security or human trafficking.

It is critical that the estimates be framed as based on "uncertain" data and be viewed more as an evaluation of the vulnerability rather than an exact estimate of the threat. Once we evaluate the vulnerabilities, we can begin protecting the supply chain gaps. A first step in determining the appropriate, strategic, and efficient food fraud prevention program – beyond what is technically required by law – is to evaluate the vulnerabilities that allowed past incidents to occur.

Incident Reviews

To consider the incident reviews, insight from a research article is provided (Spink et al. 2016):

> "In [the data gathering], incidents or suspicious activity is reviewed. There are many acceptable sources for the information including subject matter expert insight. This is a very efficient starting point that can quickly identify whether there is a lack of information or

where the enterprise decision-makers will need more data. For example, an enterprise considering the start of a food fraud strategy needs fewer details than a situation where competing and costly risk tactics are being evaluated. This is the process to gather and assess historical or emerging threats. Currently, there are no explicit or detailed process steps for gathering and sorting data. Government regulation and industry standards refer to experts, or a qualified person, to assess hazards and assign risk ranks. Also, many key terms are not defined such as the FSMA concept of a 'known or reasonably foreseeable hazard'." (Spink et al. 2016).

There are many ways to sort or organize known incidents. Encoding data, establishing a typology, or using a data cluster tool are all acceptable methods to organize and analyze incident data. One method developed for product fraud is the "Product-Counterfeiting Incident Clustering Tool" (PCICT) that is codified in an ISO standard (see the section on "Product-Counterfeiting Incident Clustering Tool") (Spink et al. 2014; ISO 2018).

"After conducting the incident review step, there can be information relating to a realization of an inherent risk requiring an immediate redefinition of the overall project (i.e., not simply performing an FFIS). This is a natural opportunity to review the overall Food Fraud Prevention Plan and development process."

Presentation: Corporate Risk Map

COSO/ERM recommends the presentation of the assessment results on a corporate risk map or also referred to as a risk map or heat map. The single figure is well recognized by a Board of Directors, Risk Audit Team, or Internal Audit Team. It is efficient and important to present the assessment in the terminology and format of those enterprise leaders. The subject is introduced previously in this chapter and in the chapter on Business Decision-Making. Several case studies are provided including a hypothetical county level FFIS and a product-specific FFIS.

Sidebar: Case Study—FFIS for an Entire Country Including All Products and All Fraud (Yes, It Can Be Done)

This exercise was to refine the process and to demonstrate the utility of a final assessment. This assessment covered the entire market for all products and all types of fraud (Fig. 17.7). The creation of the countrywide completed assessment enables a review of specific issues rather than the more conceptually difficult first step in conducting the broad assessment. Also, once issues are identified as "high" or "very high," there is often an intense engagement and questioning of the assessment. Presenting the assessment usually creates motivation from other stakeholders or interested parties to engage in the process. (Note: refer to ISO definitions of key terms such as interested parties, organization, management, management system, and other.)

(continued)

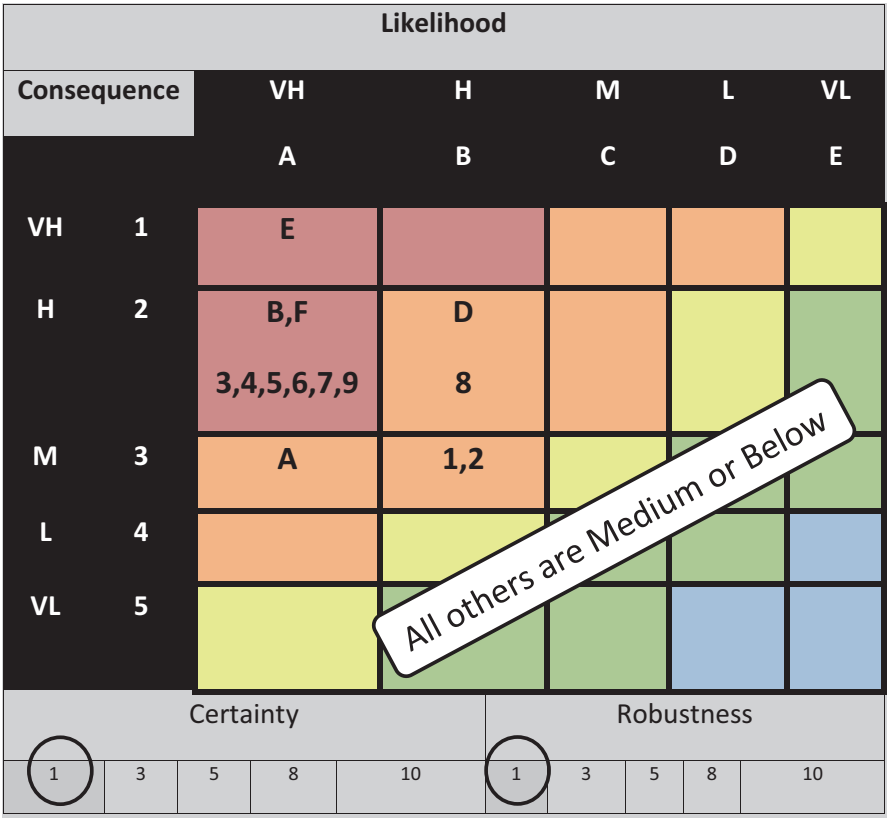

Fig. 17.7 FFIS summary matrix that for this assessment includes only outgoing goods

- Since this is a prefilter, preliminary assessment with low pre-research, the matrix was identified to be very low on "certainty" and very low on "robustness."
- The assessment found 14 items that were a "very high" or "high" food fraud vulnerability based on an estimate of the country-level risk tolerance.
- Of the 14 issues, 11 were in 2 products which were "spirits, alcohol, etc." and "meat, seafood, dairy."
- Also seven of nine "incoming goods/raw materials" were imports from developing countries (Eastern Europe, China, and others).
- The imported product was both at a port and smuggled into the marketplace.
- For "outgoing goods/finished goods," four of six were for "private/kiosk/bazaar/trolley" and "e-commerce/online shipping."

This country-level assessment provided a review of all vulnerabilities. The next step is to conduct further edits to the conclusions. After final agreement

on the rankings, there is now a clear method to identify the focus topic which would be the item highest risk that is item "E." Also, the presentation of the conclusions raises a question about the urgency of addressing the other risks that are above the risk tolerance (in the red and orange zones).

Sidebar: Case Study—European Country, Food, Alcohol, Spirits, Vodka
Included here is an example of a quick but complete FFIS that includes plotting the vulnerabilities on the corporate risk map and then a quick review of possible countermeasures and control systems. Each of the "very high" risks seems to have risk treatments that could be implemented almost immediately—and for all three problems, the equipment or process may already be in place so they could be implemented with only a slight adjustment in the screening target or message. In all three problems, the countermeasures and control systems were not the usual food authenticity tests or anti-counterfeiting components.

From the report:

Title: Prefilter Food Fraud Initial Screening (FFIS) Using Open-Source Information

For: *Country*/Vodka

Date: October 6, 2017

Summary: An open-source search was conducted to review the food fraud vulnerability for ***Country/Vodka***. The goal was to provide an example of the FFIS tool for a specific problem. The review assessment is ranked as certainty 1/10 and robustness 1/10, and the team was the MSU Food Fraud Initiative members. The assessment identified three specific "very high" and four specific "high" vulnerabilities. The likelihood was an estimate based on base awareness and local discussions. The consequence was a combination of the health hazard incidents, the loss of economic contribution from lost sales, and then a social factor of concern raised by an incident/illness/death by the specific retail location. For example, it is more concerning for consumers if there is a slight problem at a trusted supplier rather than an incident at an informal or illicit market. The "market" main concerns appeared to be (1) online marketplaces and (2) "white van" deliveries (e.g., an unofficial seller of product "out of the back of a 'white van.'" The "product" for an online sale is the delivery, and the main concerns were (1) local courier or person-to-person delivery and (2) private or contract couriers. Together, three "very high" problems were identified. Possible countermeasures and control systems were suggested for each:

1. For high incident geographic areas (such as a specific postal code), possibly utilize an X-ray/computer system to identify >0.5 L glass or plastic bottles.

(continued)

Markets/ Products		Major retailer/ Specialty	Minor retailer/ Independent	Bazaar/ Kiosk/ Flea Market	Online	"White Van" – individual & Other
		A	B	C	D	E
Pick-up	1	VL	VL	M	NA	NA
Local Inventory – Direct Delivery	2	VL	VL	M	H	H
Domestic Ship – Mail	3	L	L	NA	VH	NA
International Ship – Mail	4	NA	NA	NA	VH	NA
Local Inventory – "Courier" Delivery, P2P Handoff & Other	5	VL	M	H	VH	H

Fig. 17.8 FFIS assessment detail of the specific fraud opportunity problems. (Copyright Permission Granted) (Spink 2017)

2. Add or adapt current mail X-ray/computer scanner for >0.5 L liquid in glass or plastic.
3. Review warning communication to this target group of consumers (e.g., social media of Snapchat, Instagram, specific information brokers).
4. Note: All three countermeasures and control systems may already be implemented by other agencies.

The next step would be to review if the resource-allocation decision-maker requires an increase in the certainty and robustness to a level necessary to decide on countermeasures and control systems.

Method: The prefilter Food Fraud Initial Screening Tool (FFIS) is the first of the two-stage process for Enterprise Risk Management (ERM). The initial screening is conducted both as a Food Fraud Vulnerability Assessment starting point and to understand public information that could lead to litigation. The limits for likelihood, consequence, and corporate risk appetite were estimated.

Assessment Detail: This conclusion was based on an assessment. The nature of the product and specific research question enabled one matrix to be used (Fig. 17.8).

Next, although it was very easy to see the cluster of "very high" concerns, the results were plotted on a risk map (Fig. 17.9).

Process Check—These "very high" food fraud problems versus all countrywide "very high" problems: Plotting the problems on this corporate risk map is helpful for the resource-allocation decision-maker since these findings can be calibrated against all of the enterprise-wide risks. For example, while it may be clear, these are by far the most concerning three problems; they may actually be lower compared to enterprise-wide problems. For example, a countrywide *Salmonella* outbreak would seem to be higher than all three of these food fraud problems. This brings up a question of whether the likelihood and consequence were properly calibrated.

Process Check—Recalibration: The corporate risk map and enterprise-wide ranking include a built-in recalibration feature. The original likelihood

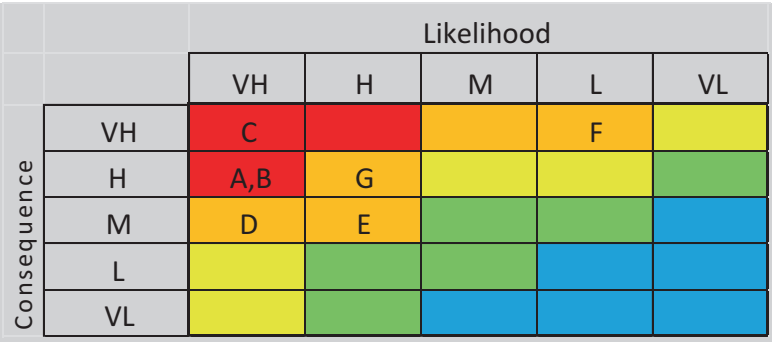

Fig. 17.9 FFIS heat map summary of the fraud opportunity problems. (Copyright Permission Granted) (Spink 2017)

#	Total (Likelihood * Consequence)	Group/ Product
	Incoming Goods-TOTAL (Econoimc + Hazard + Social)	
1		<<NOT REVIEWED
2		
3		
	Outgoing Goods-TOTAL (Econoimc + Hazard + Social)	
A	VH = VH * H	Online company, domestic mail delivery
B	VH = VH* H	Online company, international mail delivery
C	VH = VH * VH	Online company, courier or P2P handoff delivery
D	H = VH * M	Online company, local inventory direct delivery
E	H = H * M	Online company, courier or P2P handoff delivery
F	H = L * VH	White Van, direct delivery
G	H = H * H	White Van, courier or P2P handoff

Fig. 17.10 FFIS detail of the heat map fraud opportunity problems including the total, likelihood, consequence as well as the details of each problem. (Note: the incoming and outgoing goods detail is included to clarify that only the local impacts were assessed) (Copyright Permission Granted) (Spink 2017)

and consequence estimates can be recalibrated. Each of the 25 cells can be reassessed based on the newly defined likelihood and consequence factors. The recalibration is not bad—it is actually good or even *great*. If there is a need for a recalibration, then it indicates that the resource-allocation decision-maker has reviewed the process in detail and provided more refinement. The next FFIS/FFVA will be more finely tuned.

A legend for the risk map was created (Fig. 17.10). This allows a quick presentation of the findings.

(continued)

Table 17.6 FFIS detail of each cell with reference number, rank, problem, and countermeasures (Spink 2017)

Ref #	Rank	Problem	Countermeasure
D3	VH	Vodka bottles shipped through the domestic mail	For high incident, areas utilize X-ray/computer scanner to identify >0.5 L glass or plastic bottles (Q: are these already in use?)
D4	VH	Vodka bottles shipped through the international mail	Add or adapt current mail X-ray/computer scanner for >0.5 L liquid in glass or plastic (Q: are they already in place?)
D5	VH	Late night young people buying vodka from pedestrians	Review warning communication to this target group (social media of snapchat, Instagram, specific information brokers) (Q: what other public health information distribution or programs exist?)

Next, since there was such a tight cluster of "very high" incidents in terms of the markets and products, there could be a simple consideration of countermeasures and control systems (Table 17.6).

While this is a quick assessment that is low in certainty and low in robustness, it does add value to provide a case study but also for the country to begin to address this specific research question.

Conclusion

Before conducting assessments, it is important to thoroughly review the theoretical foundation and then adapt the use case to the specific application. The previous chapter covered risk analysis and basic assessment which provide a foundation that was built upon here to provide an expanded review of the application and assessment. This chapter provided a series of examples and reviews that led to key conclusions. ***The first conclusion is*** to clearly define the research question and the specification of the resource-allocation decision-making. The research question is exactly what problem you are addressing such as reducing the fraud opportunity and not a tactical middle step such as which test to choose. This effort to not just review the incidents but consider the decisions that will be made will help refine the specification of "how much is enough" for an assessment. ***The second conclusion is*** to conduct a case study or a use case (description of the method of how a goal is achieved) to be able to refine the assessment to meet the specific need. Since this is often the first time a food fraud assessment is conducted, a quick exercise will help both to provide insight but also to refine the process. This preliminary step seems contrary to the "do it right the first time" mantra. In this situation, it is probably impossible or at least impractical to try to decide on the method that would be used forever. For the first time addressing food fraud prevention the "do it right the first time," the "it" is a pilot or preliminary study. The key outcome is the lessons learned

Sidebar: Bell-Shaped Distribution of Your Risks Versus an ERM Heat Map

The presentation of an assessment has several forms. There is no right or wrong method.

That said, be *very clear* about your goal *before* plotting the data or even before gathering any data. If the goal is to review food fraud in relation to all other enterprise-wide risks (the most applicable goal), then the method would *not* be to create a bell-shaped, even distribution of all food fraud incidents.

- First, there may be a need for an even distribution of the findings.
  - This spreads the results evenly across a spectrum such as very low to very high.
  - The calibration is the specific data set against itself.
  - This spreads the results evenly across the scale. This is similar to grading students on a bell-shaped curve. Even if all the students were brilliant, the bell-shaped curve would require the top 10% of students to be categorized as "excellent" and the bottom 10% to be categorized as "failing."
  - As risk treatments are applied, and as individual vulnerabilities are reduced, the plot is recalibrated to spread the data over that span.
- Second, there may be the use of a standardized heat map that plots the assessment on a matrix such as bound by likelihood and consequence predefined in a method or standard.
  - This spreads the results as determined by the definition of very low to very high.
  - The calibration is the assessment of the general definition of very low to very high.
  - This spreads the results as determined by the general definition of likelihood and consequence.
  - As risk treatments are applied, and the individual vulnerabilities are applied, the entire data set could shift below the risk tolerance—actually, that is the goal. The risk threshold is set by the method.
- Finally, a variation of the standardized heat map is a corporate risk map that plots the likelihood and consequence determined by the entity's unique and specific risk tolerance.
  - This spreads the results as determined by the definition of very low to very high.
  - The calibration is the assessment of the entity's unique and specific definition of very low to very high.

(continued)

- This spreads the results as determined by the entity's definition of likelihood and consequence.
- The risk threshold is set by your own company's risk managers based on a formal system such as ERM/COSO (which is actually set by your owners through their proxies, the Board of Directors).

As discussed elsewhere, the likelihood and consequence are presented in qualitative terms (e.g., words: very high, high, medium, low, very low) or quantitative terms (e.g., numbers: 5, 4, 3, 2, 1). The plot can include only the points or include a statement of the standard of deviation or confidence intervals. Presenting two dimension figures with the point estimate and confidence intervals is very complex, and the charts are often confusing. Thus, just the point plot is usually used.

It is important to note here that the use of numbers may imply precision where a "3" is presented as defined by an analytical method to be significantly different than "2". Further, a "3.7" versus a "3.8" implies accuracy and precision to two significant digits. For initial screening, prefilter, or early stage assessments, it is strongly recommended to use words not numbers.

Appendix: WIIFM Chapter on Risk Implementation

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 provided insight and methods for the overall starting point of vulnerability assessments which is the Food Fraud Initial Screening (FFIS) within the Food Fraud Prevention Cycle (FFPC)
Quality team	This chapter presented the prefilter and Food Fraud Initial Screening (FFIS) method—with case studies
Auditors	This chapter will provide insight on the type of assessments you might recognize that are effective risk communication and that it is based on sound methods
Management	The output should be a very simple one-page summary that presents *all* enterprise-wide risks under your control—with as much background detail as *you* need
Corp. decision-makers	The process will provide *you* with a high-level, one-page summary which the Food Fraud Prevention Strategy will seamlessly integrate into your COSO/ERM type system with just with as much detail as *you* need

Appendix: Study Questions

This section includes study questions based on the Key Learning Objectives in this chapter:

1. Discussion question
   (a) What is the COSO/ERM source of credibility or authority?
   (b) Why is it so difficult to obtain even a simple estimate of the economic impact of food fraud or product counterfeiting?
   (c) What are the biggest hindrances of conducting a countrywide or company-wide assessment?
2. Key learning objective 1
   (a) What is a COSO defined "initial screen"?
   (b) What is the first step in a COSO assessment?
   (c) What is the "risk of conducting a risk assessment"?
3. Key learning objective 2
   (a) What is an FFIS?
   (b) What is an enterprise-wide assessment per COSO/ERM?
   (c) What are the COSO defined strengths and weaknesses of a qualitative vs. quantitative assessment?
4. Key learning objective 3
   (a) What is "seizure data"?
   (b) What are the "challenges of using seizure data" in a FF assessment?
   (c) Why does FF prevention—and many types of crime such as IPR counterfeiting—inherently include "inconsistent sources of data"?

References

CIB, Counterfeiting Intelligence Bureau. (1997). *Countering Counterfeiting. A guide to protecting & enforcing intellectual property rights*. Counterfeiting Intelligence Bureau (CIB), International Chamber of Commerce (ICC).

COSO, Committee of Sponsoring Organizations of the Treadway Commission. (2011). *Embracing enterprise risk management.* By Mark L Frigo and Richard J Anderson. URL: https://www.coso.org/Documents/Embracing-ERM-Getting-Started.pdf.

COSO, Committee of Sponsoring Organizations of the Treadway Commission. (2012). *Risk assessment in practice - Enterprise risk management.* Committee of Sponsoring Organizations of the Treadway commission, COSO.

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

ISO, International Organization for Standardization. (2018). *ISO 22380:2018 Security and resilience -- Authenticity, integrity and trust for products and documents -- General principles for*

product fraud risk and countermeasures. Status: Published, Publication date: 2018-08-22. URL: https://www.iso.org/standard/73857.html.

MSU-FFI, Food Fraud Initiaive. (2018). *Blog series, food fraud initiative*. Michigan State University, developed and presented by John Spink. URL: www.FoodFraud.msu.edu/Blog/.

OECD, Organisation for Economic Co-operation and Development. (2007). *Estimating the magnitude of counterfeiting and piracy, in OECD*. The Economic Impact of Counterfeiting and Piracy, OECD Publishing, Paris. URL (full text): http://dx.doi.org.proxy2.cl.msu.edu/10.1787/9789264045521-5-en, OECD Publishing.

Public Law 113-54. (2011). *113th Congress, An Act to amend the Federal Food, Drug, and Cosmetic Act with respect to human drug compounding and drug supply chain security, and for other purposes*. <<NOTE: Nov. 27, 2013 - [H.R. 3204], Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, <<NOTE: Drug Quality and Security Act. 21 USC 301 note.>> SECTION 1. SHORT TITLE - This Act may be cited as the "Drug Quality and Security Act". URL: https://www.govinfo.gov/content/pkg/PLAW-113publ54/html/PLAW-113publ54.htm.

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. (2017). *Unique food fraud prevention challenges in E-commerce*. Food Safety Authority of Ireland (FSAI), Safeguarding the food chain - protecting authenticity and integrity, October 5, 2017 – Dublin. URL: https://youtu.be/uhrkoUuOhEk.

Spink, J. (In press, 2019). The current state of food fraud prevention: Overview and requirements to address "how to start?" and "how much is enough? *Current Opinions in Food Science*.

Spink, J., Elliott, C. T., Dean, M., & Speier-Pero, C. (2019). Food fraud data collection needs survey. *npj Science of Food, 3*(1), 1–8.

Spink, J., & Levente Fejes, Z. (2012). A review of the economic impact of counterfeiting and piracy methodologies and assessment of currently utilized estimates. *International Journal of Comparative and Applied Criminal Justice, 36*(4), 249–271.

Spink, J., Moyer, D. C., Park, H., & Heinonen, J. A. (2013). Defining the types of counterfeiting, counterfeiters, and offender organizations. *Crime Science, 2*(8), 1–9.

Spink, J., Moyer, D. C., & Speier-Pero, C. (2016). Introducing the food fraud initial screening model (FFIS). *Food Control, 69*, 306–314.

Spink, J., Moyer, D. C., Park, H., & Heinonen, J. A. (2014). Development of a counterfeit incident clustering tool (PCICT). *Crime Science, 3*(3), 1–8.

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.

USITC, US International Trade Commission. (2011a). *China: Effects of intellectual property infringement and indigenous innovation policies on the U.S. economy*. United States International Trade Commission, Investigation No. 332-519, USITC Publication 4226, May 2011.

USITC, US International Trade Commission. (2011b). *China: Intellectual property infringement, indigenous innovation policies, and frameworks for measuring the effects on the U.S. Economy*. United States International Trade Commission, Investigation No. 332-514, USITC Publication 4199 (amended), November 2010.

WCO, world Customs Organization. (2007). *WCO trends and patterns report - A capacity building estimate*. ISSUE 2 - December 2007. URL: http://publications.wcoomd.org/images/upload/pdf/TrendsAndPatternsReport2.pdf.