Chapter 5
Food Fraud Prevention Overview (Part 3 of 3): The Implementation

Summary
This chapter presents an expanded review of food fraud prevention to consider a systematic approach, the focus on vulnerabilities and then beginning to prepare for decision-making and "how much is enough?" The activities are presented in the Food Fraud Prevention Cycle (FFPC) (Spink 2014; Spink et al. 2019).

The Key Learning Objectives of the chapter are
- (1) **Introduction to the Food Fraud Prevention Cycle (FFPC)—**"a system of systems"
- (2) **The focus on vulnerability before risks or hazards**
- (3) **Then the decision-making criteria for "how much is enough?"**

On the Food Fraud Prevention Cycle (FFPC), this chapter addresses the overall fundamental prevention concepts of "connecting everything to everything" (Fig. 5.1).

Introduction

After understanding the basics and the approach, there is a pragmatic and practical need to actually implement the concepts and get to a point where there can actually be resource-allocation decision-making.

[1] Note: COSO more often uses the term "risk map," but "corporate risk map" is used here and throughout to clarify the intent review the formal and systematic assessment of enterprise-wide risk not a basic risk summary.

J. W. Spink, *Food Fraud Prevention*, Food Microbiology and Food Safety,
https://doi.org/10.1007/978-1-4939-9621-6_5

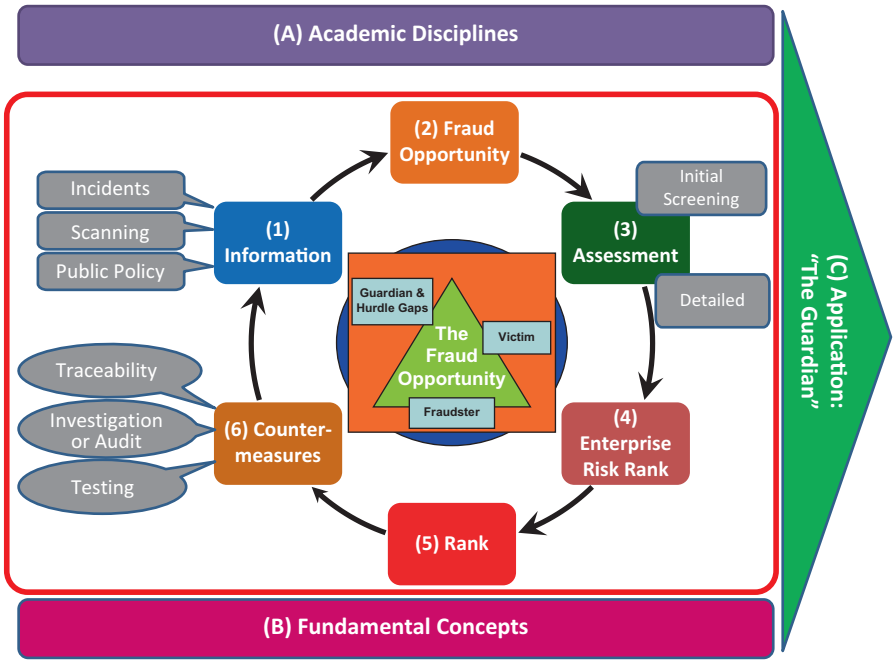

Fig. 5.1 Food fraud prevention cycle: where this chapter applies to the overall concept—the entire cycle 1, 2, 3, 4, 5, and 6 and the fraud opportunity. (Copyright Permission Granted) (Spink 2014; Spink et al. 2019)

Key Learning Objective 1: Systematic Prevention—A "System of Systems"

This section reviews the process for a systematic prevention strategy that is presented in a "system of systems" that is the Food Fraud Prevention Cycle (FFPC) (Spink 2014; Spink et al. 2019). This cycle is comprised of several key components that are presented here.

The Key Learning Objectives of this section are

- (1) Awareness that is comprised of the incident review and fraud opportunity
- (2) Introduction to the fraud opportunity based on the Crime Triangle
- (3) Consideration of how to seek and process new information.

Introduction to the Problem

The Food Fraud Prevention Cycle (FFPC) grew out of the effort to connect each of the separate activities into one complete cycle (Spink 2014). The FFPC is a "system of sub-systems." Each sub-system cycles within the overall system. Everything is

connected. Each assessment feeds the other assessments in a dynamic process. This dynamic process is self-correcting; meaning that as the fraud opportunity fluctuates up and down, the countermeasures and controls systems are calibrated with the changing risk appetite.

Considering assessments, it is important to review that risk is not necessarily a negative. The owners of a company (which includes individual investors who own stocks, mutual funds or have a pension) expect a specific and ratable level of risk that equates to a financial return—some specific activities are too risky for that threshold. A business that is not risky enough will create lower financial returns. The financial security regulations create a standardized process for public companies to report the inherent risk. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) created Enterprise Risk Management (ERM/COSO) accounting practices which were created in response to the US Sarbanes-Oxley Act and later the Frank-Dodd Act (Public Law 107–204 2002; 15 USC 7201 2006; Public Law 111-203 2010; 12 USC 5301 2018) (for more on US securities law, see (SEC 2013)). The Food Fraud Prevention Strategy can be directly integrated into the ERM resource-allocation decision-making system. The terminology used to address food fraud is the same terms that are used in ERM/COSO.

For this section, a simple previous version of the Food Fraud Prevention Cycle is used. The components and linkages are the same but in a less refined form (Fig. 5.2):

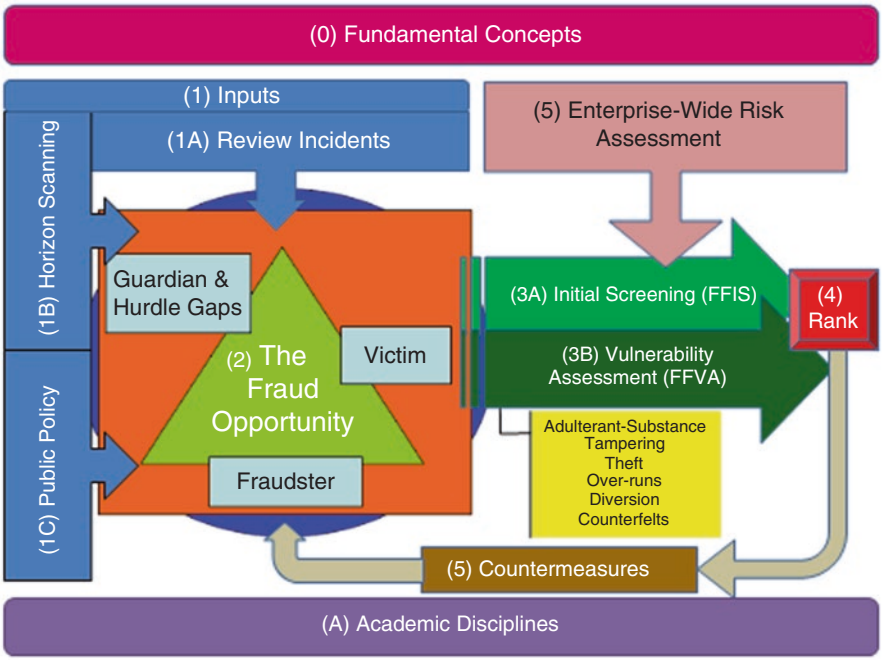

Fig. 5.2 Simple previous version of the food fraud prevention cycle (FFPC). (Copyright Permission Granted)

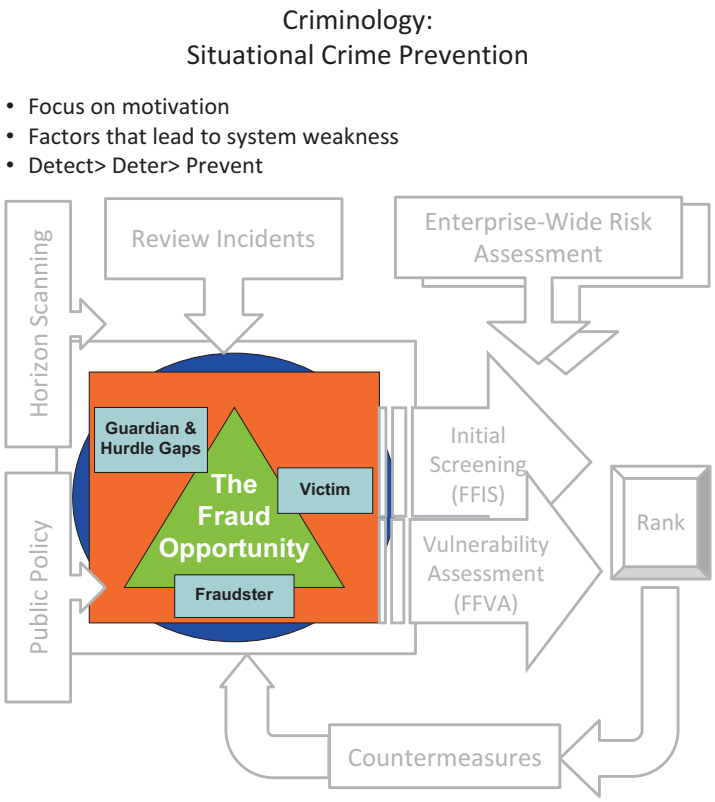

Fig. 5.3 The main influence on the fraud opportunity which is understood by criminology and specifically situational crime prevention. (Copyright Permission Granted) (Spink 2017)

The Engine: The Fraud Opportunity

A saying is that "It's all about the fraud opportunity." This means that the root cause of the entire food fraud problem is based on a weakness or vulnerability. The Crime Triangle concept is based on Situational Crime Prevention which includes on a fraudster human adversary identifying a target or victim, in relation to a guardian or hurdle gap (for more, see the chapters on Criminology) (Fig. 5.3). To reduce the fraud opportunity, the goal is to focus on the criminal motivation, identify factors that lead to system weaknesses, and then consider countermeasures to detect, deter, and prevent (Spink 2017).

Sidebar: How the Fraud Opportunity Engine Works—Illicit, The Dark Trade

In 2005, Moises Naim wrote, "Illicit: The Dark Trade" (Naim 2005). This is built upon his previous article "The Five Wars of Globalization" which are illicit trade (1) drugs, (2) arms, (3) intellectual property, (4) people, and (5) money (Naim 2003). Product counterfeiting, product fraud, and food fraud are in the intellectual property category.

Two insights are especially valuable: (1) governments, intragovernmental, and nongovernmental organizations have their hands full with a range of very complex and very bad problems, and (2) for food fraud prevention, there are lessons to be learned from those other problems.

Naim provides some shocking insights on the fraud opportunity including that (Illicit, Naim 2005):

> ***[Product counterfeiting] is… more profitable than trafficking heroin… easier than photocopying… and with penalties like jay-walking.***

A more detailed example is:

- "A batch of 1800 cartons of drugs made in China but labeled as manufactured in India and Pakistan under license from multinational companies…
- Turned out to involve ten copycat manufacturers…
- In five provinces,…
- Using five different suppliers for packaging...
- Manufacturing sites range from small household workshops to legitimate factories: a firm that produces a drug under license need only run an extra shift with substandard inputs.
- Workers on the line may never know they were doing anything wrong."

For all the five wars of globalization, there are reasons he says "Why Governments Can't Win":

- "Technology will continue to spread widely; criminal networks will be able to exploit these technologies more quickly than governments that must cope with tight budgets, bureaucracies, media scrutiny, and electorates."
- "Those criminal networks:
  - They are not bound by geography.
  - They defy traditional notions of sovereignty.
  - They pit governments against market forces.
  - They pit bureaucracies against networks."

Prior to any strategic review of product counterfeiting, it is important to establish some key concepts (Naim 2005):

- "**Illicit trade is driven by high profits, not low morals**
- **Illicit trade is a political phenomenon** – illicit traders cannot prosper without help from governments or accomplices in key public offices.

(continued)

- **Illicit trade is more about transactions than products** – we are so accustomed to parsing the illicit trades into separate product lines
- **Illicit trade cannot exist without licit trade** – all illicit businesses are deeply intertwined with licit ones. Indeed, traffickers have strong incentives to combine their illicit operations with legitimate business ventures.
- **Illicit trade involves everyone** – someone is buying…
- **Governments can't do it alone.**"

Ultimately, the insight from Naim may be disturbing or disgusting, but it is the reality. Once the underlying concepts are clearly understood and embraced, then there can be a rational and pragmatic path forward. The works by Naim were fundamental in the development of the food fraud prevention concepts.

Awareness: Incident Review and Fraud Opportunity

The first function or step in the FFPC is awareness which builds upon the information. Information could be from "incident reviews" which are known events, scanning, or "horizon scanning" that could be a wide range of "signals" such as price changes or commodity shortages and "public policy" which includes increased risk of detection or enforcement due to new priority setting (Fig. 5.4) (Spink 2017). This awareness building is based on the criminology-based science of intelligence analysis. To provide the right type of information or intelligence to assess the fraud opportunity or problem, there is a systematic gathering and analysis of raw data, a process to monitor changes, and then a step to filer and process this into actionable intelligence.

Sidebar: Does a Good Food Defense Program Help Prevent EMA? Maybe (MSU-FFI 2018)

Title: Does a Good Food Defense Program Help Prevent EMA? Maybe.

By John Spink • November 13, 2013 • Blog

This is an excerpt of an email from a food industry leader. If this person has this question, then I'm sure many of you do as well. The original question was: "Would a good food defense program help prevent 'intentional adulteration'?" Answer: Maybe, but probably not yet.

The "maybe" is based on questions of scope and scale of the food defense program. Let me begin by noting that food fraud is beyond an "adulterant-substance" or "economically motivated adulteration" (EMA), for example, you may also have problems or product recalls if you have a country of origin fraud, mislabeling, or even unauthorized repackaging that compromises traceability.

In most cases, food defense is defined as combating intentional attacks to harm another. The harm could be a terror, economic, or public health. The attackers often want to get publicity or want to really hurt people, so we often find out quickly about the act. With food fraud, they definitely do *not* want to get caught…they'll be sneaky, actively try to evade our tests and systems, and they'll be both persistent and keep evolving to stay stealthy.

As for addressing with other types of crime problems, prevention is not only infinitely more cost and time effective, but it is the only thing that often actually works. Using Situational Crime Prevention, we go look for the vulnerabilities…then decide how we can reduce that threat.

At that point, when we understand the vulnerability—e.g., species swapping of animal protein—we know what and where we should test. We know what we should be testing for, that is, to "detect." If the frustrater is operating within in the legitimate supply chain, then the countermeasure can "deter" against that specific attacker. If it is known that the customer does "some" species tests when receiving products, and new bad guys can find out that the company is testing, then the species tests lead to prevention. Also, you're looking for the right test at the right spot at the right frequency. For example, a company was running species tests 24 hours a day for 7 days a week during an incident and then completely stopped testing after the food fraud incident had passed. They said "Why test? The incident is over." Click—that was the door of their fraud opportunity reopening. They don't need to test a lot, but they should be testing at least some product if only to counter an accusation of "willful negligence" for this "reasonably foreseeable hazard."

In a company, there are often two defined concepts of unintentional acts such as food safety and also of intentional acts defined as food defense. If this is the case, it is structurally efficient for a company to put food fraud under food defense but to understand that the countermeasures and control systems and processes are very different. Think of combating shoplifters compared to ferreting out suppliers diluting product. What about combating employee theft versus country of origin labeling fraud? No one—me included—will ever be able to be an expert on all food fraud concepts and threats. We're trying to create an educational foundation of knowledge, moreover, and then a group of colleagues. (I consider myself as a food fraud librarian who is gathering, categorizing, and writing about all the information in the books we find.) We will need to help train and support those people who will take the reins of food fraud prevention. We will need to start by defining the scope and scale of a good food defense plan.

Overall, it is most efficient if food fraud prevention is a separate, standalone, interdisciplinary, enterprise-wide team or task force function. This is similar to anti-counterfeiting and brand protection programs that are coordinated at the corporate level, and then individual responsibilities are distributed into the operations and the business units.

(continued)

I ended my email to the food industry leader by stating "Actually, this would be a great blog post, maybe I'll post it." So I am. Consider if your food defense plan really does address food fraud prevention. Don't wait for FSMA or GFSI; companies have food fraud risks every day (MSU-FFI).

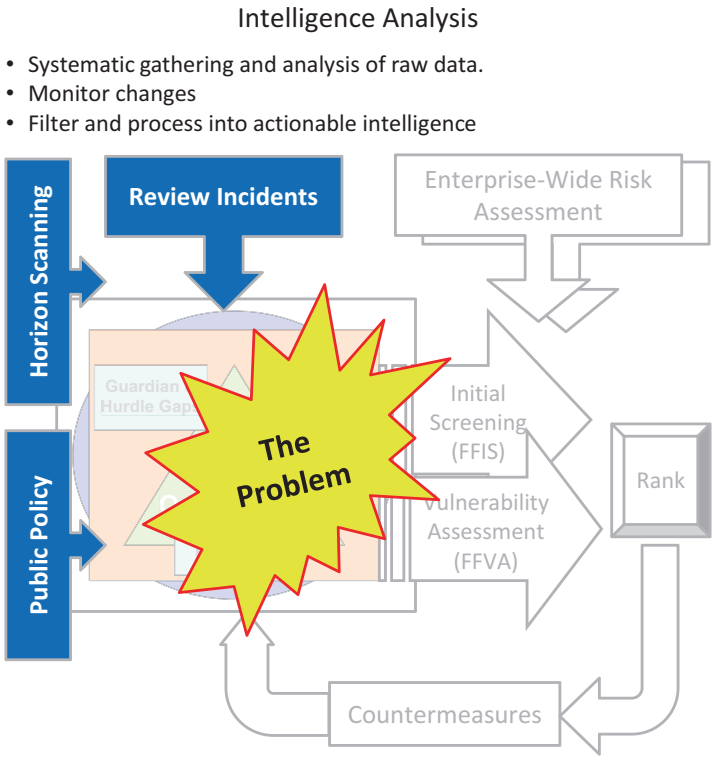

Fig. 5.4 The intelligence analysis that provides information and data to understand the food fraud problem. (Copyright Permission Granted) (Spink 2017)

Key Learning Objective 2: The Vulnerabilities and Countermeasures

This section reviews the next steps which are assessing the vulnerabilities and the final actions of judging or selecting countermeasures and control systems. These two steps are between other key activities such as understanding the fraud opportunity and conducting the risk rank which supports resource-allocation decision-making. Building on theories such as criminology, total quality management, and enterprise risk management, it is most efficient and effective to start by understanding the system weaknesses and the root cause of the problem.

The Key Learning Objectives of this section are

- (1) Review the process of vulnerability assessment: initial screen and detailed assessment
- (2) Consideration of what assessment or predictive models are even possible
- (3) Then the system to review and select optimal countermeasures and control systems

Vulnerabilities: Understood by Risk Assessment and Decision Sciences

Another function or step is the focus on vulnerabilities rather than risks. The core concepts of risk and vulnerability will be covered in more detail in the Business Risk chapter and the Vulnerability Assessment chapter. The key components are building upon an understanding of the fraud opportunity to then conduct assessments which would start with an initial screen before determining if there is a need for a more detailed assessment. The Food Fraud Prevention Cycle sub-system of vulnerability assessment is a two-stage process that includes an initial screen and then a detailed assessment that is conducted as required (Fig. 5.5). To support decision-making to reduce the fraud opportunity, the assessment should consider the following: is the issue an actual problem, how much of a problem, and then how to provide first a quick review before a more detailed assessment.

The Food Fraud Prevention Cycle (FFPC) is based on an objective to focus on the cause *and* effect—both. The food safety systems address the effect or result. Once a hazard is found in the food supply chain, it is usually classified as either a traditional hazard (e.g., food safety, an unintentional act with naturally occurring problems) or nontraditional (e.g., food defense, intentional act with non-naturally occurring food safety hazards). The traditional food safety management systems are refined to evaluate an acceptable or unacceptable hazard threshold clearly (e.g., product recalls are defined as Class I, II, or III (for more see (Fortin 2009)) and the industry and regulatory product recall procedures are refined and honed. These hazards are usually well known, researched, addressed by regulations with defined thresholds, and defined as biological, chemical, and physical.

On the other hand, the nontraditional hazards – if they don't fit into the more traditional food safety product recall activity – are often addressed by an ad hoc process by necessity. There occasionally incidents that don't seem to fit into general categories or response plans, so the responders do the best they can to figure some way to address the crisis. An intentional act to harm could be a single disgruntled employee or a coordinated, global terrorist network, or anything in between. When conducting a suspicious activity review "intervention," the worst case should be assumed in for every incident.

These unknowns related to intentional acts to harm define the efficiency of creating a separate Food Fraud Vulnerability Assessment and Prevention Strategy. Also, the variability of the nontraditional hazards emphasizes the importance of focusing

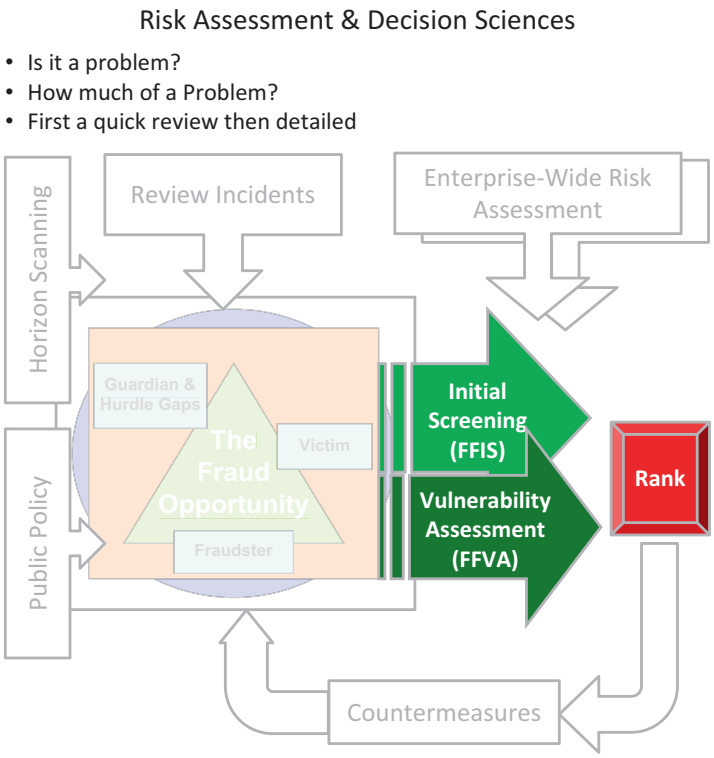

Fig. 5.5 The decisions sciences that provide a structured method to conduct the assessment and support the selection and implementation of countermeasures and control systems. (Copyright Permission Granted) (Spink 2017)

on prevention and thus vulnerabilities. When focusing on reducing the vulnerabilities—and reducing the fraud opportunity—it is most efficient to remove consideration of the human fraudster from the equation. It is easier to respond to the physical components of the vulnerability rather than to try to confront a specific fraudster or type of fraud act.

These concepts are included in the Food Fraud Vulnerability Assessment. These methods and processes are in their infancy and continue to evolve and mature as they are used. The GFSI Food Fraud Position paper was published in July 2014, the SSAFE/PWC Food Fraud Vulnerability Assessment was published in January 2015, and the Food Fraud Initial Screening Tool (FFIS) was published in November 2016 (GFSI 2014; SSAFE 2015; PWC 2016; Spink et al. 2016).

Essentially "if there is a fraud opportunity then there is a fraud opportunity." If you did purchase from criminals, they might not commit a crime because they don't perceive an opportunity…though you'd prefer not to purchase from criminals. "Where there is fraud opportunity there is a fraud opportunity; regardless of the morals, ethics, or honesty of the supplier."

Sidebar: "It Is Simply Not Possible to Validate Predictive Models of Rare Events That Have Not Occurred"

At the 2008 Society for Risk Analysis annual meeting, Robert G Ross of the US Department of Homeland Security presented "Observations on the Importance of Risk Communication in Managing Homeland Security Risk"((Ross 2009) also (Ross 2006a, b, 2007)). He discussed "models for insight versus models to predict." He recommended using a range of risk models to provide a wide range of insight on these unique vulnerabilities. Regarding probabilistic risk assessment and more advanced quantitative risk assessments, he made several important key points that apply to food fraud prevention (JASON 2009):

- "[It] is simply not possible to validate (evaluate) predictive models of rare events that have not occurred, and unvalidated models cannot be relied upon."
- There is a "…distinction between models for probabilistic risk assessment on long timescales… versus specific point production of individual rare events."
- "It is not a realistic goal to anticipate and prevent all rare events, but it may be possible to make rare events rarer, and to reduce their effect."
- "A rare event is preceded by a chain of individually more likely developments that create intent, capability, and opportunity. Intervention may be possible at many points in that chain."
- "There are two principal problems in applying quantitative models to the anticipation of rare events. One problem is that rare events are rare. There will necessarily be little or no previous data from which to extrapolate future expectations in any quantitatively reliable sense, or to evaluate any model."
- "In the extreme, how can the probability of an event that has never been seen or may never even have been imagined be predicted?"
- "An additional difficulty is that rare event assessment is largely a question of human behavior, in the domain of the social sciences, and predictive social sciences models pose even greater challenges than predictive models in the physical sciences. Reliable models for ameliorating rare events will need to address smaller, well-defined, testable pieces of the larger problem."

This insight provides a foundation regarding rare events for what *cannot* be expected from traditional probabilistic risk assessment. This insight encourages a shift in focus from predicting the exact incident that will occur to consider the wide range of factors, variables, or vulnerabilities that are known. Ross's presentation encouraged the use of many different types of assessments and to focus on "models for insight" rather than "models for prediction"—risk-informed versus risk-based decision-making.

Recalls: Background and Definitions

The FDA website explains the "Types of FDA Enforcement Actions." Overall, the FDA regulatory goal is to "assure compliance with the Federal Food, Drug, and Cosmetic Act (the Act)." While the Act covers a wide range of issues, efficient resource allocation is directed by a risk-based approach for a priority on the worst public health harms.

The first goal of the logical risk-based approach is to do whatever it takes to reduce the current or immediate public health harms. Sometimes this leads to a priority for a product recall over a possible extended criminal investigation. An immediate product recall reduces the success of a criminal investigation because the perpetrators are alerted that the officials know of the problem. It is important to take immediate activity since a perpetrator can destroy evidence, modify records, or even flee the country (Spink 2011).

> "Specific enforcement activities include actions to correct and prevent violations, remove violative products or goods from the market, and punish offenders. The type of enforcement activity FDA uses will depend on the nature of the violation. The range of enforcement activities includes issuing a letter notifying the individual or firm of a violation and requesting correction, to criminal prosecution of the individual or firm."

There are a range of actions or responses available for a regulator such as the US Food and Drug Administration (FDA). Recalls are actions taken by a firm to remove a product from the market. Recalls may be conducted on a firm's own initiative, by FDA request or by FDA order under 21CFR7.3 statutory authority (21CFR7.3 2014).

There are three types of product recalls:

- **"Class I recall**: a situation in which there is a reasonable probability that the use of or exposure to a violative product will cause serious adverse health consequences or death.
- **Class II recall**: a situation in which use of or exposure to a violative product may cause temporary or medically reversible adverse health consequences or where the probability of serious adverse health consequences is remote.
- **Class III recall**: a situation in which use of or exposure to a violative product is not likely to cause adverse health consequences."

There are other potential actions including:

- "**Warning Letters** – are sent to the individuals or firms, advising them of specific noted violations; These letters request a written response as to the steps which will be taken to correct the violation. These letters constitute one form of warning that can be issued under current Agency policy."
- "**Seizure** – An action brought against an FDA-regulated product because it is adulterated and/or misbranded within the meaning of the Act. The purpose of such an action is to remove specific violative goods from commerce."
- "**Injunction** – An order by a court that requires an individual or corporation to do or refrain from doing a specific act. FDA may seek injunctions against individuals and/or corporations to prevent them from violating or causing violations of the Act."

- "**Criminal prosecution** – may be recommended in appropriate cases for violation of Section 301 of the Act; Misdemeanor convictions, which do not require proof of intent to violate the Act, can result in fines and/or imprisonment up to 1 year. Felony convictions, which apply in the case of a second violation or intent to defraud or mislead, can result in fines and/or imprisonment up to 3 years."
- "**Criminal Fines** for Food Drug and Cosmetic Act Violations – Misdemeanor fines under the Act may reach $500,000 under some circumstances. The Criminal Fine Enforcement Act of 1994 (Public Law 98-596) provides for fines for violations of Federal law. Although it is not part of the Act, the Criminal Fine Enforcement Act of 1994 applies to all fines levied under the Act, as well as other statutes that contain provisions enforced by FDA."

When responding to a regulatory or enforcement action, it is important to clearly understand the exact scope of each term. Several key terms are provided here (emphasis added):

- "(b) **Citation or cite** means a document and any attachments thereto that provide notice to a person against whom ***criminal prosecution*** is contemplated of the opportunity to present views to the agency regarding an alleged violation."
- "(c) **Respondent** means a person named in a notice who presents views concerning an alleged violation either in person, by designated representative, or in writing."
- "(d) **Responsible individual** includes those in positions of power or authority to detect, prevent, or correct violations of the Federal Food, Drug, and Cosmetic Act."
- "(g) **Recall** means a firm's removal or correction of a marketed product that the Food and Drug Administration considers to be in violation of the laws it administers and against which the agency would initiate legal action, e.g., seizure. Recall does not include a market withdrawal or a stock recovery."
- "(h) **Correction** means repair, modification, adjustment, relabeling, destruction, or inspection (including patient monitoring) of a product without its physical removal to some other location."

Countermeasures and Decision-Making

Once the vulnerability assessment is in place and operating, this next component includes a review of countermeasures and decision-making in the corporate risk map (Fig. 5.6) (Spink 2017). The consideration of countermeasures is a vital separate sub-system, so there is a formal way to seek, consider, and reinforce resource-allocation decision-making. To connect the functions or steps, this sub-system would support the detect-deter-prevent steps and consider currently implemented and possibly new technologies which include the popular interoperable enhanced traceability innovations and also more tactical responses such as enforcement and prosecution. Countermeasures and control systems are the risk treatments that should be selected based first on the confirmation of a need to address this vulnerability and then the direct contribution to reducing the fraud opportunity.

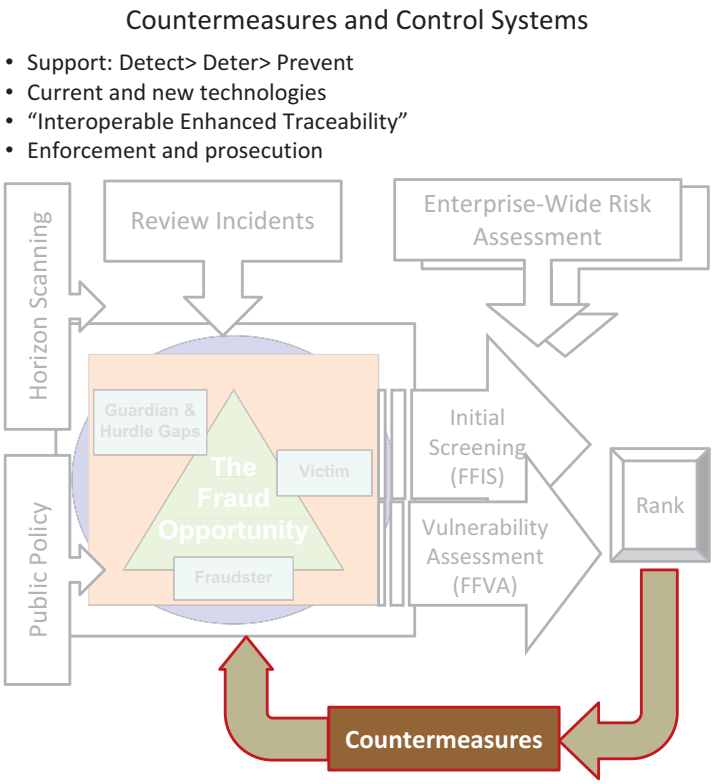

Fig. 5.6 The countermeasures and control system linkage that supports the reduction of the fraud opportunity. (Copyright Permission Granted) (Spink 2017)

The Determination of "How Much Is Enough" by Enterprise Risk Management (ERM/COSO)

At this point, there is a realization that there is usually no structured, analytical, methodical decision-making process for "how much is enough?" There are two critical benefits of applying ERM into the operations (covered in more detail in the Business Decisions chapter) which include that holistic countermeasures and control systems are considered efficiently when vulnerabilities are being assessed, and the frontline decision-making includes those overarching, corporate decision-making insights (Fig. 5.7) (Spink 2017). At first, the proposals will need to be evaluated on a case-by-case basis, but over time the risk assessors will become more familiar with what types of hazard levels and countermeasure are (or are not)

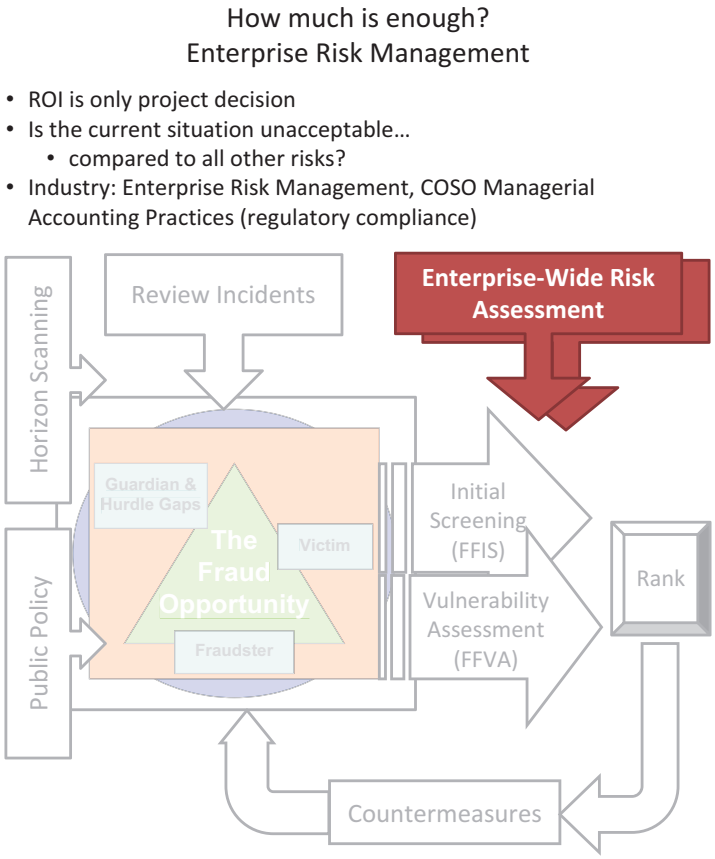

Fig. 5.7 The linkage to an enterprise-wide risk assessment that provides guidance resource-allocation decision-making and "how much is enough?". (Copyright Permission Granted) (Spink 2017)

implemented. This sub-system is the resource-allocation decision-making step. By calibrating the FFPC to the ERM system, return on investment is only a project decision and not a consideration against all other possible allocations; this provides a way to review if the current situation is unacceptable as compared to all other risks across the enterprise and also correlate with the implemented ERM systems based on COSO managerial accounting practices. These sub-systems create a holistic and all-encompassing system to manage the Food Fraud Prevention Strategy.

Sidebar: Understanding a Generic or Specific Risk Tolerance

The calibration of the vulnerability assessment to the corporate risk tolerance is a separate and unique function in the Food Fraud Prevention Cycle. Without this calibration, the use of a generic assessment tool creates a generic risk rank. What is "high" for one industry, company, or product may not be "high" for your company—this could be for many reasons include some countermeasure or control system that is not considered in the vulnerability assessment or the general nature of your operations or supply chain.

The food fraud assessments and strategies build upon ERM/COSO which, itself, builds upon risk appetite or risk tolerance. These are terms that are defined in other total quality management systems and specifically in Six Sigma and also in a range of ISO standards from ISO 22000 Food Management and most importantly in ISO 31000 Risk Management.

- **Six Sigma:** this principle is based on a cycle of plan-do-check-act (PDCA) with a "specification limit." A limit could be a type of variation or a resulting flaw. By design, the limit is "Six Sigma" or six times the standard of deviation. The method to determine the limit—or here, the variation or flaw—is undefined and refers to another decision-making system.
- **ISO 22000 Food Management Systems:** this standard is based on a "critical limit" that is a "measurable value which separates acceptability from unacceptability." The method to determine of the limit—or here, critical limit—is undefined and refers to another decision-making system.
- **ISO 31000 Risk Management:** this standard has a process step to "establishing the context" which is "defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy." The method to determine the maximum limit of tolerable risk—or here, the parameters—is undefined and refers to another decision-making system.
- **ERM/COSO:** this process is specifically focused on evaluating the maximum acceptable level of risk or uncertainty for an enterprise. An enterprise could be a company, a country, or any organization. Specifically, ERM is "designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." Also, "an organization's risk appetite should be articulated and communicated so that personnel understands that they need to pursue objectives within acceptable limits." And, "ultimately, management and the board need an understanding of the entity's portfolio of top risk exposures affecting entity objectives so that they can determine whether it is in line with the stakeholder's appetite for risk."

Sidebar: Chase the Problem or Try to Eliminate the Root Cause and Motivation?

To optimize the efforts, there is a need to shift the paradigm from addressing the problem to reducing the root cause of the anomaly. Henry David Thoreau was credited with saying "There are a thousand hacking at the branches of evil to one who is striking at the root." Also, there is a question of "how fast do you need to run not to get caught by a bear?" The answer is "faster than the person you're running with" (since it assumed that your colleague gets caught and eaten). Both of these analogies are considered when shifting the food fraud countermeasure and control system focus to prevention.

Continuing the analogy of the home burglary, if there start to be more home break-ins around your neighborhood what is the ***first*** thing you do? Call your politician to ask for more strict laws? Demand more investigation and prosecution by the county court? Do you ask for more police to patrol the neighborhood and investigate all suspicious characters? If you are concerned about those burglaries, maybe the first thing is to make sure you lock your doors and windows.

To think about this another way, to protect your house from a burglar: if you lock your doors, the criminal may climb in the window; if you lock your window, they might just break the glass; if you put bars on your windows, they may try to kick in your back door, on and on until the effort to break into your house is just too much of a hassle**.**

To review the selection of a food fraud prevention countermeasure, consider the cost of applying a unique serial code (a significant technological feat compared to lot number or manufacturing dates on a long production run) includes information technology infrastructure and management to control and confirm the application as well as the management through to the consumer. Depending on how much the system relies on the code to confirm authenticity, there is also a potentially high legal liability. For example, consider a medicine that is used to restart a heart after open-heart surgery. The legal liability for the manufacturer could be literally catastrophic if that "authenticated" product is really a counterfeit or substandard. The interoperable-enhanced traceability system value must be weighed against the loss.

These are examples of the "problem." A more efficient focus is to consider reducing the "motivation" for the fraudsters to commit an act.

For any new countermeasure or control system, the question must be asked "how *will* the counterfeiter circumvent the system" or even "how *will* the counterfeiters *benefit* from the system." This takes into consideration the counterfeiters will respond. This takes into consideration that counterfeiters research how to avoid detection both now and in response to future countermeasures and control systems. If these are all considered, then an efficient and effective countermeasure or control system can be selected and implemented. If not then the likelihood of success is a guess.

(continued)

The countermeasures and control systems don't have to be perfect or completely eliminate the "fraud opportunity." The response is calibrated to your unique fraud opportunity and reduces the vulnerability to within your specific risk tolerance. Often burglars are looking for a soft target. They are not trying specifically to break into your home. Usually, if your doors are locked, windows shut, lights on, no tempting bags of money in plain sight, dog barking, and the alarm is on, they will probably look for a softer target. That is the goal of food fraud prevention: run faster than the person you're running with and move on from raking leaves to hack at the roots of the tree.

Key Learning Objective 3: A Systemic Approach to Food Fraud Prevention

This section reviews the Food Fraud Prevention Cycle functionality—"how it actually works." The foundation is based first on the detailed framework of all industry or regulatory, domestic or international, compliance requirements and then integrates with other current systems. As is taught when addressing a geometry problem, first lay out all the "knowns" and "givens" and consider applicable "tools" *before* starting to gather more data or solving the problem. There is a need for a process or function that coordinates all the activities.

The Key Learning Objectives of this section are

- (1) Focus on the root cause which is the "fraud opportunity."
- (2) Conduct vulnerability assessments including a way to methodically seek and utilize new information. This should also consider this risk compared to all other enterprise-wide risks before determining a "rank."
- (3) Define a way to consider and select countermeasures and control systems including a feedback loop to dynamically monitor and recalibrate the entire cycle.

The Fraud Opportunity: The Root Cause

A fundamental idea is "It's all about the fraud opportunity"—every assessment or decision is defined in terms of how it contributes to the prevention and reduces the fraud opportunity. The engine of the cycle—the center of everything—is the "fraud opportunity." Everything revolves around understanding the characteristics and influencers of this Crime Triangle. When the fraud opportunity is understood, then there can be a more efficient selection of countermeasures and control systems as well as an explanation of how and why the interventions reduce the vulnerability. Without an understanding of the fraud opportunity, the risk treatments are guesses—granted they are educated guesses but still without a methodical approach.

Another fundamental idea is: "If one aspirin is good, then ten is better. Right?" "Traceability is good, so more is better. Right?" Then RFID, the blockchain, DNA, mass serialization, whole genome sequencing, and other things must be better, right? Maybe. The critical question is how these countermeasures and control systems contribute to the prevention and reducing the vulnerability. The Food Fraud Prevention Cycle (FFPC) is used to create and help decision-making in the strategy. The strategy is the action plan. The Food Fraud Prevention Cycle is a dynamic process since there is a constant fluctuation of the specific fraud opportunity and the unique risk appetite. The cycle is used to ramp up—or down—the countermeasure and controls systems.

The strength of the FFPC is that it covers all the activities including the resource-allocation decision-making and "connects everything to everything" *and* it is self-correcting to optimize the countermeasures and control systems. Without the feedback and recalibration step, the countermeasures and control systems usually keep adding up and up. With the calibration and review of all implemented programs, there is now a methodical approach to evaluate what countermeasures and controls systems should be scaled down or removed. This would include a corresponding addition or reduction in staffing.

The Components of the Food Fraud Prevention Cycle: How They Fit Together

At this point in the book, the Food Fraud Prevention Cycle (FFPC) is becoming familiar since it is the map for all the content. Once the overall Food Fraud Prevention Strategy (FFPS) is in place, it includes a dynamic Food Fraud Prevention Cycle (FFPC). Several vital systems help build awareness of the vulnerabilities and also for the entire cycle (see above in Fig. 5.1 from this chapter) (Spink 2014; Spink et al. 2019). The FFPC components include (1) overall principles (e.g., A, B, and C) and steps that are the activities (e.g., 1, 2, 3, 4, and 5).

Key components of the FFPC include these (the FFPC figure is included again here for convenience, Fig. 5.8):

- (A) Academic Disciplines: There is a range of academic disciplines that contribute to the understanding and management of the "fraud opportunity." These are not specific systems in the FFPC but are important to provide insight on each factor.
- (B) Fundamentals: Some basic principles or fundamentals enable the actions and provide insight into the working of the cycle and the specific functions.
- (1) Inputs: This function considers new information to add to the review of the fraud opportunity.
  - (1A) Incident reviews and review of changing marketplace conditions such as commodity price changes.

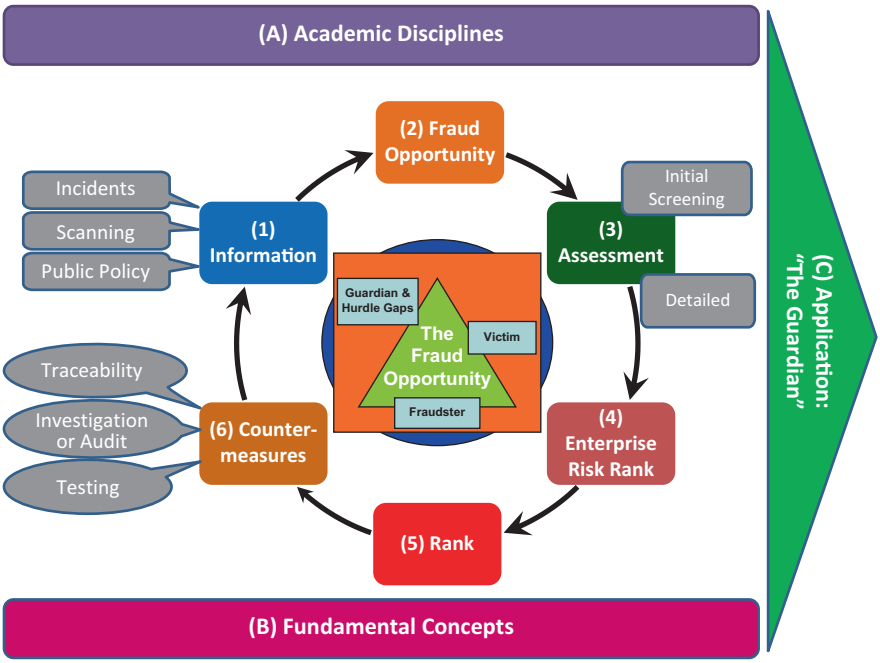

Fig. 5.8 This is the entire food fraud prevention cycle (FFPC). (Copyright Permission Granted) (Spink 2014; Spink et al. 2019)

  - (1B) Scanning: this is an active review of what is happening externally such as market price changes, supply shortages, and other general intelligence about vulnerabilities or incidents.
  - (1C) Public policy: changing public policy or regulatory focus.

- (2) Fraud Opportunity: This is based on the Criminology theory of Situational Crime Prevention. It is a separate assessment that feeds into the vulnerability assessment.
- (3) Vulnerability Assessment: The Enterprise Risk Management/COSO vulnerability assessment is a two-stage process starting with an "initial screening" and extends to a "detailed screening." For food fraud prevention, this is demonstrated by the Food Fraud Initial Screening Tool (FFIS), the SSAFE/PWC Food Fraud Vulnerability Assessment Tool (FFVAT), and others (SSAFE 2015; Spink et al. 2016).

  - (3A) Initial screening or prefilter: Food Fraud Initial Screening (FFIS)
  - (3B) Detailed assessment or full review: Food Fraud Vulnerability Assessment (FFVA)

- (4) Risk Appetite: The ERM/COSO process extends to applying the vulnerabilities to the Corporate Risk Map. This map helps the corporation determine what

risks are within the risk appetite. Every new vulnerability or changing assessment does not lead to a risk that is an unacceptable hazard.

- (5) Enterprise-Wide Risk Assessment: Connection to the resource-allocation decision-making defined by the "risk tolerance."
- (6) Countermeasures and Control Systems: These are a wide range of activities that either directly confronts specific types of attacks or that provide insight on when a product may be "out of control."
- (C) Application—"The Guardians": This includes combined external controls or programs that investigate, enforce, and prosecute the fraudulent activity.

This *system of systems* creates awareness that there is a cycle, and within that, there is an awareness of how all the emerging and current factors fit together.

Sidebar: Who in Their Right Mind Would Decommission an Anti-counterfeit Countermeasure?

Without a rigorous risk assessment system, no one in their right mind would reduce a redundant anti-counterfeit countermeasure. For example, a new packaging group manager could inherit a product with ten of the same anti-counterfeit features (e.g., holograms, micro-taggants, color shifting ink, etc.). If the decision is without a methodical approach or demand, and if there is a new counterfeit incident, the manager may be blamed. This would be like deciding that the lease on a second battery backup sump pump for your basement was not cost effective. That might be a logical decision, but if the basement floods, there will be huge consequences for the manager—possibly a career limiting move. Without a clear analytical assessment—not just the logic or common sense—the risk assessor could get fired. If a customer dies, this could lead to criminal prosecution! Thus, no one in their right mind would remove a legacy countermeasure or control system without a very thorough and analytical decision-making process.

By using the Food Fraud Prevention Cycle, including plotting the vulnerabilities on the Corporate Risk Map,[1] there is a clear, logical, methodical, and analytical assessment that the lease on the second sump pump is illogical. The FFPS and FFPC clearly define that removing the second sump pump is a wise and logical business decision. If there is an adverse event (e.g., the basement floods), the risk assessor can defend the decision to remove the second backup sump pump.

Sidebar: Food Fraud Criminal Cases – How to Keep your Boss Out of Handcuffs

While food industry managers are not thinking about criminal prosecution—at least not yet for food fraud prevention—one of the strongest motivators for action is a legal liability and the "court of public opinion." Whether based on the EU-type food integrity laws or the US-type public health laws, a

(continued)

suspicious product can be determined to be "unfit for commerce." A product recall is quick and very economically harmful for a company. While additional liability for gross incompetence or willful blindness is impactful, a product recall achieves the most fundamental goal of removing the suspicious or dangerous product from commerce.

As for the "court of public opinion," the impact of social media can be catastrophic for a brand or company. Often the risk of a possible product recall—or bad press about product integrity—has driven companies to change their operations. (MSU-FFI 2018):

Title: How to Keep your Boss Out of Handcuffs

By John Spink • May 22, 2013 • Blog

Are food fraud incidents being treated as criminal cases? In the first MSU-FFI Food Fraud Overview MOOC earlier this month, I briefly discussed this, and I want to follow up with examples and details here. It takes quite a bit for a US agency to pursue criminal charges when there are civil law options (Goldstone 2001). The burden of proof for a criminal case is much higher than for civil charges—and in many situations, even state-level civil cases can shut down a business and seize all assets, even when the business is not aware of the dangerous public health threat. For example, see the State of Alabama's Deceptive Trade Practices Act (AL Code 8-19-1 2017). This Alabama act is focused on protecting public health and welfare but also on protecting the legitimate innovative businesses that are trying to provide healthy lifestyle products: "Legislative intent – The public health, welfare, and interest require a strong and effective consumer protection program to protect the interest of both the consuming public and the legitimate businessperson." Several key definitions from the Alabama law include (emphasis added):

- "**GOODS:** Includes but is not limited to any property, tangible or intangible, real, personal, or any combination thereof, and any franchise, license, distributorship, or other similar right, privilege, or interest."
- "**KNOW, KNOWING, KNOWINGLY, KNOWLEDGE, and KNEW**: Either actual awareness or such awareness as a reasonable person should have considering all the surrounding circumstances."
- "**PERSON:** Includes but is not limited to natural persons, corporations, trusts, partnerships, incorporated or unincorporated associations and any other legal entity."
- "**SALE, BUYING, and DISTRIBUTION:** In addition to their ordinary meanings, include but are not limited to the act of leasing, renting, or consigning."
- "**SERVICES:** Work, labor, and other services, including but not limited to services furnished in connection with the sale or repair of goods."
- "**TRADE** or **COMMERCE:** Includes but is not limited to the advertising, buying, offering for sale, sale or distribution or performance of any service or goods, and any other article, commodity or thing of value wherever situated and shall include any trade or commerce affecting the people of this state."

In a Packaging World Magazine article, legal guru Eric Greenberg discussed the criminal charges levied against the Peanut Corporation of America (PCA). The criminal charges are outlined in an indictment that is based on intent to defraud. One of those people charged already pleaded guilty, so the prosecution will probably have a willing witness. One broader law, the US Park Doctrine, states that charges can be brought against corporate leaders even if they didn't know of the dangerous acts. In the PCA case, there is evidence that the leaders did know of the salmonella contamination, so other, more direct charges could be levied.

The PCA case highlights a concerning issue for food manufacturers and retailers where the fraudster actively seeks to avoid detection. Even in facilities that are audited by competent auditors—even in unannounced inspections—the bad guys can find ways to hide their fraudulent operations, which is what happened when PCA intentionally transferred product from a noncertified manufacturing plant to a certified one after inspections and then presented the goods as manufactured in a certified manufacturing plant.

Various types of criminal charges can apply. During the MOOC I mentioned what the US Customs has called "honey laundering." This is where honey is transshipped from a country with a high tariff through a country with a lower tariff and labeled as coming from that low tariff country. The "origin laundering"—or "neutralization"—is the fraudulent and deceptive change of the country of origin on the label. The fraud opportunity for tax avoidance smuggling can be substantial. One honey case led to $180 million in profit from the avoided taxes (DOJ 2009; ICE 2010).

There is a public health vulnerability in smuggling for two reasons. First, in a product recall, it is not possible to trace the fraudulent honey…or, worse, if the traceability codes are incorrect, the wrong product might be recalled while the dangerous product remains in the marketplace (CACP 2006; Liang 2006). Second, we lose transparency on the product itself (Roth et al. 2008). With the lack of transparency, there is an increased fraud opportunity to use unapproved or dangerous ingredients. At a minimum, the bad guys often get greedy and start adulterating the product to further increase their profits.

As was stated in the indictments, several of the food fraudsters did start adulterating the honey with sugar. In this instance, the perpetrators all knew they were committing a crime, so criminal charges were not a surprise—though criminals don't think they'll get caught.

Regarding food fraud prevention, the takeaway is that we need to reduce the fraud opportunity regardless of whether we trust our suppliers or don't think there is any logical reason for anyone to commit fraud. Regarding protecting your corporate leaders from being led out of your facility in handcuffs, be diligent in developing and supporting a Food Fraud Prevention Strategy. Address "reasonably foreseeable hazards," and your actions will reduce the potential charge of "willful blindness."

Risk Analysis of the FFIS and FFVA: "The Assessment"

There is a need to further expand on how and why "risk analysis" is incorporated in the Food Fraud Prevention Cycle. The fraud opportunity is covered in detail in the Criminology chapter, and risk analysis and vulnerability assessments were covered in other chapters. The application and use within the cycle are not really two distinct steps as indicated but a continuum. When starting to review food fraud for the first time, a CEO/CFO/CRO may ask "generally, what are we looking at here? Not so bad or really bad?" Considering an analogy of checking the weather outside, the scale needed could be as broad as "will tomorrow be deathly hot or deathly cold?" Their question is not about resource-allocation decision-making yet but more of a mental set on what is to come. Also, if this is perceived as a potentially very impactful activity, the C-suite may feel it is crucial to immediately update or warn the Board of Directors.

The most basic step is a very high-level prefilter or what Enterprise Risk Management refers to as an "initial screen"—for example, a Food Fraud Initial Screen (FFIS) (Spink et al. 2016). This is a review of all types of fraud and all products but at a very high level and with very quick assessments such as a small group of subject matter experts. At this point early in the process of reviewing the new risk, it is important to present a full and complete assessment—although possibly casual, uncertain, and un-robust—because the resource allocation decision-maker can define how much (if any) more detail is needed. There are examples where countermeasures and control systems were approved after just a broad discussion of the fraud opportunity and brainstorming of some countermeasures and control systems.

Through the use of the cycle and the continuous review, there can be an assessment of how much information—as well as the necessary level of accuracy, precision, and certainty—is needed. If the resource-allocation decision-maker has enough information, then that is the final specification. The resource-allocation decision-maker has the final say for how much information is enough to make a yes or no decision.

Countermeasures: The Risk Treatment

Consideration of countermeasures and control systems should be reviewed each and every time a vulnerability assessment is conducted. The best time for innovative and effective brainstorming is at that first point of awareness, but also it is the most dangerous time because an inefficient path and vision could be set. This also provides a great service to not only provide an updated vulnerability assessment but to already include ideas for countermeasures and control systems. When communicating problems to management, it is always best to present problems or a crisis alert accompanied by some possible responses. After a new incident, the updated

vulnerability can be presented as well as possible countermeasures and control systems that could get the situation within the risk tolerance.

To support this resource-allocation decision, the FFPC creates a method to review and explain countermeasures and control systems as well as utilizes the ERM and corporate risk map to explain "how much is enough?"

Case Study: Peanut Allergen Adulterant—Substances in Ground Cumin

This example uses the peanut in cumin food fraud incident of a company who does *not* have an immediate food safety incident. If a food fraud team did find a health hazard from the peanut allergen in cumin, the immediate response would be to contact the food safety or crisis management team. After confirming there is *no* immediate health hazard for this product, an effective food fraud prevention team use of the Food Fraud Prevention Cycle could include:

- The **information gathering** step of **scanning** identifies a new issue of "peanut in Cumin." Specifically, the employee who is responsible for scanning receives an alert that identifies the new information. The responsible employee considers whether they should alert the "food fraud team leader" or wait to present this new information at the next regular team meeting. (The team will need to calibrate what leads to an emergency meeting or what can wait.)
- The **fraud opportunity** step considers the new information. The new incident is reviewed in terms of the impact on the three components of victim, fraudster, and guardian and hurdle gaps.
- Then the **vulnerability assessment** is updated to include the refined fraud opportunity details.
- The **Enterprise Risk Management** developed a **corporate risk map** that is updated including a consideration of the updated **risk rank**.
  - If the new incident is plotted in the "unacceptable" range of the corporate risk map, then countermeasures and control system responses are developed. At this point, only possible projects are researched, and they will be reviewed later for a final decision.
- It is always good to consider **countermeasures and control systems** so, if anything, the boss knows you're already working on it and second to provide a very general idea of the effort for applying the risk treatment.
- The **risk communication** would be to review the new information that is provided to the resource-allocation decision-maker such as "A new food fraud incident of peanut in Cumin was identified. The [ways this could] impact on our company is":
  - 1. "The incident does *not* fundamentally change how we understand our fraud opportunity, and the vulnerability is still in the "acceptable" range."
  - 2. "The incident *does* fundamentally change the way we understand our fraud opportunity and the vulnerability is now in the "unacceptable range."

Hopefully, to calm senior leaders, this should be followed with "the food fraud prevention team that is already meeting to consider and implement countermeasures and/or control systems within the policy and strategy that you have already approved. We will present more details as you require.""

Conclusion

The previous Food Fraud Prevention Overview chapters established the foundation and need for the proactive, holistic, and all-encompassing approach. This chapter built upon that and presented how the prevention strategy is managed in a cycle that "connects everything to everything." The Food Fraud Prevention Cycle (FFPC) builds upon that prevention concept to demonstrate a systematic approach that builds upon the fraud opportunity and connects to a resource-allocation decision-making function that is Enterprise Risk Management (ERM/COSO). The emphasis is that "It's all about the 'fraud opportunity.'" ***The first conclusion is*** that there is a need for a system that connects all the essential components together with a focus on prevention. The basic workings of the cycle include broad concepts from the gathering of information, assessing the root cause (the fraud opportunity), conducting assessments that address all types of fraud for all products that then calibrate those assessments with all other enterprise-wide risks, and finally enabling decision-making for the selection of countermeasures and control systems *before* cycling deeper through the process again. ***The second conclusion is*** that it is possible to create a systematic way of assessing and managing the Food Fraud Prevention Strategy. A complex system cannot be efficiently or quickly implemented. There is a need to *not* build from the bottom up but to start with an approach that considers risks across the *entire* enterprise—all hazards approach for all types of fraud, all products, and all enterprise. The Food Fraud Prevention Strategy will then define—based on the specific fraud opportunity and the unique risk tolerance of the enterprise—"how much is enough." This was referred to as the "corkscrew approach." ***The final conclusion is*** that the Food Fraud Prevention Strategy is first implemented broadly but not deeply to then defines where to go deeper. The countermeasures and control systems will be drilled down such as the turning of a corkscrew. There is a saying:

> ***Combating fraudsters is like a never-ending chess match of strategic moves and countermoves.***
>
> ***You can only trust as far back as you can trust (you may need to have the countermeasures and controls only focused on testing incoming good… but try to figure out how you can reduce the fraud opportunity by trying to dissuade the fraudster from actually attacking you).***

Appendix: WIIFM Chapter on Prevention 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	While it may seem overly complex at first, after review, the FFPC is a very simple "plan-do-check-act"-type method that "connects everything to everything"—and this starts at a high level and only goes as deep as you require.
Quality team	This presented the Food Fraud Prevention Cycle (FFPC) and provided methods and case studies.
Auditors	This provides more insight into the inner workings of the overall Food Fraud Prevention Strategy.
Management	This is a presentation of the FFPC which is a very thorough and methodical approach.
Corp. decision-makers	The FFPC is an information management and business process coordination that could actually be used for any decision—but for now fully implement for food fraud so you have a working example.

Appendix: Study Questions

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

1. Discussion Question:
   (a) What is a "system of systems"?
   (b) How is a "vulnerability" different from a "risk"?
   (c) Why is the focus on "prevention" versus "mitigation" important?
2. Key Learning Objective 1
   (a) What is the "fraud opportunity"?
   (b) Must the FFPC be following in the specific sequence?
   (c) Who—or what group—decides whether a Food Fraud Prevention Strategy (FFPS) is complete or compliant?
3. Key Learning Objective 2
   (a) Define "vulnerability"?
   (b) Is the goal to completely eliminate vulnerabilities?
   (c) How is a vulnerability assessed or defined?

4. Key Learning Objective 3
   (a) What are "risk tolerance" and "risk appetite"?
   (b) On the FFPC, where is the "risk treatment" applied?
   (c) What is the relationship between an initial screen/prefilter and a detailed assessment?

References

12 USC 5301 (2018). United States Code, 2012 Edition, Supplement 5, Title 12 – Banks and Banking; Chapter 53 – Wall Street Reform and Consumer Protection; Sec. 5301 – Definitions; 'Dodd-Frank Wall Street Reform and Consumer Protection Act'. Accessed: January 12, 2018, URL: https://www.govinfo.gov/content/pkg/USCODE-2017-title12/pdf/USCODE-2017-title12-chap53-front.pdf.

15 USC 7201 (2006). United States Code, 2006 Edition, Supplement 5, Chapter 98 – Public Company Accounting Reform and Corporate Responsibility, this Act may be cited as the "Sarbanes Oxley Act of 2002"URL: https://www.govinfo.gov/content/pkg/USCODE-2011-title15/pdf/USCODE-2011-title15-chap98-sec7201.pdf.

21CFR7.3 (2014). Defined in the US Code of Federal Regulations, Title 21 Food and drugs, Subchapter A General and Part 7 Enforcement policy, section 7.3 definitions URL: https://www.fda.gov/Safety/Recalls/IndustryGuidance/ucm129337.htm.

AL Code 8-19-1 (2017). 2017 Code of Alabama, Title 8 - Commercial Law and Consumer Protection, Chapter 19 - Deceptive Trade Practices, Section 8-19-1 - Short title Universal Citation: AL Code § 8-19-1 (2017),This chapter shall be known and may be cited as the "Deceptive Trade Practices Act." URL: https://law.justia.com/codes/alabama/2017/title-8/chapter-19/.

CACP, Coalition Against Counterfeit and Piracy (2006). No Trade in Fakes, Brand Integrity Tool Kit US Chamber of Commerce, Coalition Against Counterfeit and Piracy (CACP).

DOJ, U.S. Department of Justice (2009). Chinese Honey Supplier Arrested on U.S. Charges for Allegedly Conspiring to Evade U.S. Restrictions on Imported Honey, for Chicago Office of German Food Distributor, U. S. Department of Justice, United States Attorney Northern District of Illinois, For Immediate Release, Wednesday, May 6, 2009.

Fortin, N. D. (2009). *Food regulation: Law, science, policy, and practice*. Hoboken: Wiley.

GFSI, Global Food Safety Initiative. (2014). GFSI Position on Mitigating the Public Health Risk of Food Fraud, Global Food Safety Initiative, Consumer Goods Forum.

Goldstone, D. (2001). Deciding whether to prosecute an intellectual property case. U.S. Department of Justice, U.S. Department of Justice,. 49.

ICE, US Immigration and Customs Enforcement (2010). Honey importer sentenced to 30 months for conspiring to evade US import duties, News Releases. US Department of Homeland Security.

JASON, Defense Advisory Panel (2009). Rare Events, October 2009, Approved for Public Release, JSR-09-108 (an evaluation of the nation's ability to anticipate and assess the risk of rare events. "Rare events" specifically refers to catastrophic terrorist events, including the use of a weapon of mass destruction or other high-profile attacks, where there is sparse (or no) historical record from which to develop predictive models based on past statistics.), URL: https://fas.org/irp/agency/dod/jason/rare.pdf.

Liang, B. A. (2006). Fade to black: Importation and counterfeit drugs. *American Journal of Law & Medicine, 32*(2–3), 279–323.

MSU-FFI, Food Fraud Initiative (2018). Blog Series, Food Fraud Initiative, Michigan State University, developed and presented by John Spink, URL: www.FoodFraud.msu.edu/Blog/.

Naim, M. (2003). The five wars of globalization. *Foreign Policy, 134*, 28.

Naim, M. (2005). *Illicit: How smugglers, traffickers, and copycats are hijacking the global economy*. New York: Doubleday.

Public Law 107–204 (2002). Public Law 107–204, 107th Congress, An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes; this Act may be cited as the "SarbanesOxley Act of 2002" (SOX or Sarbox); 15USC7201; (Public Law 107–204, Public Law 111–203); URL: https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf.

Public Law 111-203 (2010). 111th Congress, An Act to promote the financial stability of the United States by improving accountability and transparency in the financial system, to end "too big to fail", to protect the American taxpayer by ending bailouts, to protect consumers from abusive financial services practices, and for other purposes; July 21, 2010 - [H.R. 4173]; 12USC 5301; This Act may be cited as the "Dodd-Frank Wall Street Reform and Consumer Protection Act", URL: https://www.congress.gov/111/plaws/publ203/PLAW-111publ203.pdf.

PWC, PriceWaterhouseCooper (2016). Food fraud vulnerability assessment, Online Tool, Produced with SSAFE Organization, http://www.pwc.com/gx/en/food-supply-integrity-services/publications/food-fraud-vulnerability-assessment.pdf.

Ross, R. G. (2006a). *Measuring effectiveness of anti-terrorism programs using performance logic models* (pp. 355–366). Springer.

Ross, R. G. (2006b). *Part I-long papers-terrorism informatics and countermeasures-measuring effectiveness of anti-terrorism programs using performance logic models* (Vol. 3975, pp. 355–366). Berlin: Springer.

Ross, R. G. (2007). *Collaborative public-private risk assessment in vessel traffic safety* (pp. 353–367). Springer.

Ross, R. G. (2009). *PRA vs. game theory vs. (fill in the blank) in terrorism threat assessment. Society for Risk Analysis Annual Meeting*. Baltimore: Society for Risk Analysis.

Roth, A. V., Tsay, A. A., Pullman, M. E., & Gray, J. V. (2008). Unraveling the food supply chain: Strategic insights from China and the 2007 recalls. *Journal of Supply Chain Management, 44*(1), 22–40.

SEC, US Securities and Exchange Commission (2013). The Laws That Govern the Securities Industry, URL: https://www.sec.gov/about/laws.shtml.

Spink, J. (2011). The challenge of intellectual property enforcement for agriculture technology transfers, additives, raw materials, and finished goods against product fraud and counterfeiters. *Journal of Intellectual Property Rights (JIPR), 16*(2), 183–193.

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). Academia: Food Fraud Prevention Research, INTERPOL-EUROPOL, Debriefing OPSON VI - Launch OPSON VII, October 2, 2017, Dublin.

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

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.

SSAFE, SSAFE Organization (2015). Food Fraud Vulnerability Assessment Tool - FFVAT, (formerly: Safe Secure and Affordable Food For Everyone organization), December 16 2015, URL: http://www.ssafe-food.org/.