Chapter 4
Food Fraud Prevention Overview (Part 2 of 3): The Approach

Summary
This chapter presents the application and utility of the overall Food Fraud Prevention Cycle (FFPC). Each component is connected to every other component. The decisions are calibrated and correlated to the formal enterprise-wide decision-making system. Essentially the FFPC "connects everything to everything" in a dynamic and self-correcting cycle. The FFPC components include (1) overall principles (e.g., A, B, and C) and steps that are the activities (e.g., 1, 2, 3, 5, and 5).

The Key Learning Objectives of this chapter are:

- (1) **Food Fraud Prevention Cycle (FFPC):** Presentation of a systematic approach to food fraud prevention
- (2) **Functionality:** The functionality and application of the Food Fraud Prevention Cycle
- (3) **Individuals Steps:** The process steps in the cycle

On the Food Fraud Prevention Cycle (FFPC), this chapter addresses the components and functionality of the entire cycle (Fig. 4.1). The next chapter will address each component of the FFPC.

Introduction

There were stories of that security products suppliers had challenges in getting brand owners to actually make a decision to implement the programs. There was an agreement that counterfeiting was "a problem" and that the brand owner must "do something." There would be months and months of presentations and product reviews but usually a stall just before the final resource-allocation decision-making, the final sign-off from the CFO to purchase the anti-counterfeit component. Early on we saw the rate-limiting step was in the final decision. There was a lack of ability, willingness, confidence, or urgency to make the resource-allocation decision.

J. W. Spink, *Food Fraud Prevention*, Food Microbiology and Food Safety,
https://doi.org/10.1007/978-1-4939-9621-6_4

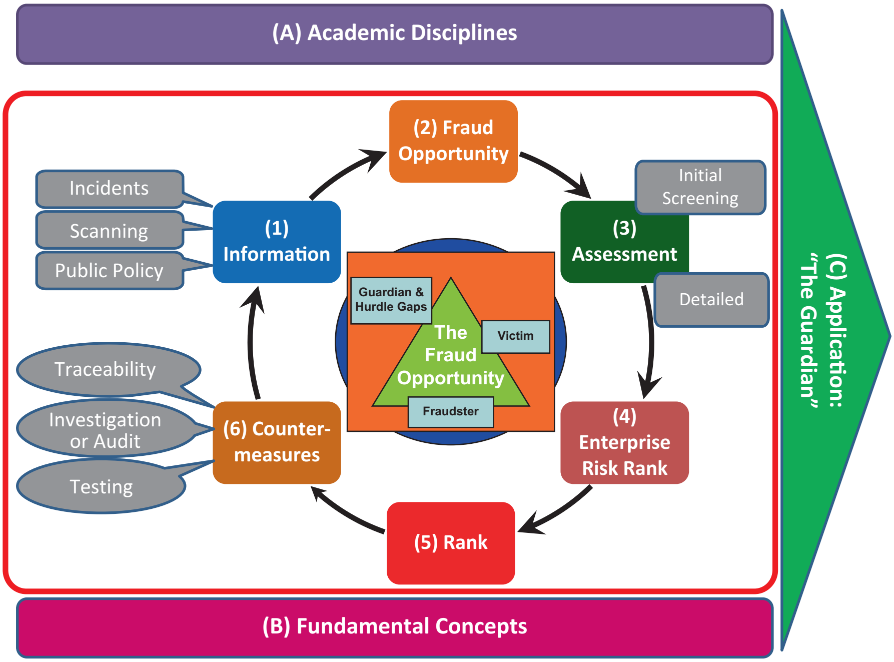


Fig. 4.1 Food Fraud Prevention Cycle: where this chapter applies to the overall concept—the entire cycle 1, 2, 3, 4, 5, 6 and the fraud opportunity (Copyright Permission Granted) (Spink 2014; Spink et al. 2019)

This led to a review of the entire system and then a focus on supporting that final resource-allocation decision-making. The result was the Food Fraud Prevention Cycle—a cycle that "connects everything to everything" including presenting the proposal in terms that the CEO/CFO needed.

The value of the Food Fraud Prevention Cycle (FFPC) is that all work functions or activities are included with methods to convert information into a useable form. If new functions or activities are identified, they will be added to the cycle or within current activities. The corporate-level risk assessor considers "I understand that there might be two deaths. I'm really concerned. I have no idea how I would assess this in relation to all other risks." The resource allocation judgment was apart from other proposals. Unless there was a regulatory requirement (mandatory where inaction would be illegal)—or the influence of the General Counsel to "do something"—the other proposals were implemented.

The final, and transformational, step in the development of the FFPC was incorporating the food fraud vulnerability or risk into Enterprise Risk Management on a corporate risk map.[1] This is important because when the Board of Directors or the

[1] Note: COSO more often uses the term "risk map" or "heat 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.

C-suite reviews a new risk, at first they are seeking just a broad and quick estimate of the issue. “How big is this problem?” “Will there be a big investment or many new resources needed?” “Should the CEO/CFO alert the Board of Directors immediately or is this really just another general risk?”

Beyond connecting every step or activity to each other, conceptually this is a cycle that is dynamic and self-correcting. The “fraud opportunity” and “risk appetite” fluctuate, and this cycle will provide a guide to increasing—or, key, decreasing—the ongoing investment in countermeasures and control systems. The value is that this is (1) a complete system that addresses all types of activities, (2) communicated in a format that supports decision-making, and that it is (3) self-correcting by encouraging a calibrated increase or decrease in countermeasures and control systems.

Key Learning Objective 1: Functionality and Application of the FFPC

This section reviews the functionality and application of the Food Fraud Prevention Cycle (FFPC). There are work processes for each function or steps that contribute to the bigger risk control strategy. The key is the overarching strategy that starts with a focus and understanding of the “fraud opportunity” rather than building upon or expanding other programs. 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).

The Key Learning Objectives of this section are:

- (1) Understand the process to coordinate and optimize countermeasures.
- (2) Continuous monitoring of the fraud opportunity and vulnerability assessment to optimize the risk treatment.
- (3) Consider the specific process steps in the Food Fraud Prevention Cycle.

Coordinating Countermeasures: Scouting Internally for Other Current Programs

It may seem either commonsense or utterly simplistic, but after the first review of the fraud opportunity, there is an efficiency of scouting across the enterprise for other countermeasures and control systems that could apply. Often, when there is a crisis, new programs or systems are implemented without extensive planning, coordination, or research. The work groups make the best decision they can under the time constraint and with the resources provided. There is usually a focus on one specific problem and with resources or insight from within one or a small group of experts. The urgency of the crisis does not lend itself to taking time to reflect too much on the enterprise-wide perspective or to conduct a lot of additional data gathering. Also, there is often a “Crisis Management” or “Business Continuity” team who does not have a responsibility to review the incident over time or to conduct a more prevention-based assessment. Often there is a series of crises…often there is “fire after fire.”

Thus, when developing a Food Fraud Prevention Strategy, it is efficient to take the time to identify related programs or projects that could be helpful to reduce or control the fraud opportunity (Fig. 4.2).

Often holistic reviews of the programs or projects identify ways they could be connected for a more significant impact. In other instances, the food fraud prevention countermeasures and controls systems may already be in place (during the search, the mindset should be that there *are* other programs already addressing part of the problem, so keep searching). Those other projects, activities, or processes may be implemented but not *yet* considered in the Food Fraud Prevention Strategy.

Considering food fraud in the continuum of all food control programs, it is entirely possible that 99% of all audits, testing, oversight, inspections, traceability, transparency, and data collection are already implemented (Fig. 4.3). Those programs just need to be identified and coordinated within the Food Fraud Prevention Strategy. For example, the separate activities to address food quality, food safety, and food defense contribute insight to address food fraud. When utilizing the visibility to risks from those other areas, it is possible that only minor extra effort is needed to completely address food fraud.

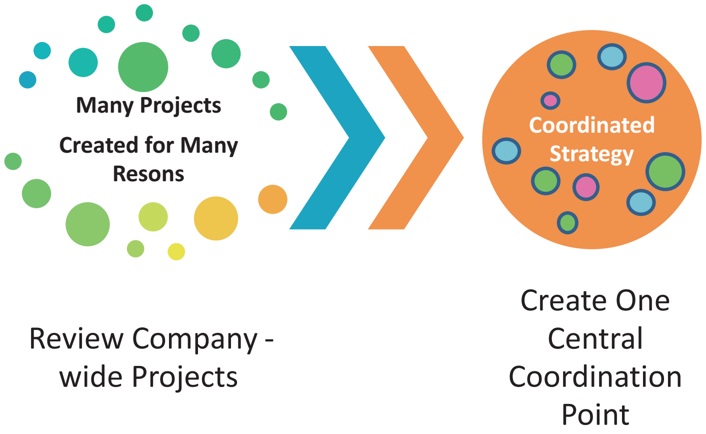
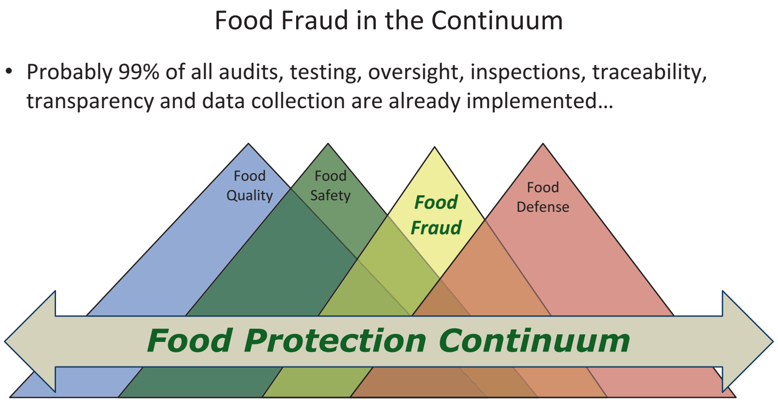


Fig. 4.2 Creating a coordinated plan that organizes and calibrates a seemingly unaffiliated set of activities (often projects are created as a response to one specific incident or required compliance requirements—the new project is not necessarily connected or calibrated with all other related projects)



Food Fraud in the Continuum

- Probably 99% of all audits, testing, oversight, inspections, traceability, transparency and data collection are already implemented…

Fig. 4.3 Food fraud in the continuum—considering all food protection programs or projects and how they contribute to food fraud prevention (Copyright Permission Granted) (Spink 2015a, b)

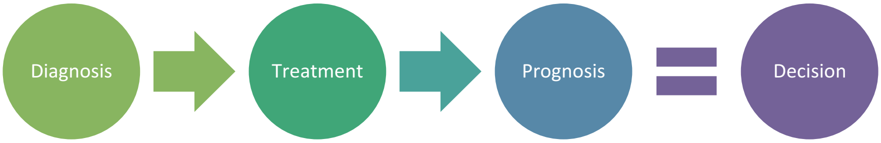


Fig. 4.4 Continuum of diagnosis, treatment, prognosis, and the decision (Copyright Permission Granted) (Spink 2019a, b)

Selecting Countermeasures and Control Systems

The component "(6) Countermeasures" includes the consideration of countermeasures and control systems. A **countermeasure** is an activity such as authenticity testing or including anti-counterfeit authentication features such as a serial number. A **control system** would be monitoring such as traceability or other supply chain transparency. The review of countermeasures is similar to a medical response of "diagnosis-treatment-prognosis = decision" (DTP).

> Think about a sick person visiting a medical doctor. Overall there is a process for 'diagnosis,' then consider a series of possible 'treatments,' and each treatment considers a 'prognosis' (Fig. 4.4). The diagnosis is similar to considering vulnerabilities. The treatments are the countermeasures or control systems which do include 'do nothing.' Finally, each diagnosis-treatment option should consider a prognosis or result of the effort. For example, if fraud is occurring at 1 to 5% of the finished good, then there is no need for a treatment that reduces the sensitivity from 1 part per thousand to one part per million.

Sidebar: Review of the GMA Brand Protection and Supply Chain Integrity Report (MSU-FFI 2018):

Title: GMA Brand Protection and Supply Chain Integrity Report

By John Spink • March 13, 2014 • Blog

On February 20, 2014, the Grocery Manufacturers Association (GMA) released their new report on "Brand Protection and Supply Chain Integrity" (GMA 2014). With my MSU colleague Dr. Doug Moyer, we participated in the Brand Protection Working Group that provided guidance for the project. This report was commissioned by GMA and the Food Marketing Institute (FMI) based on a direct request from their 2012 CEO Leadership Forum—addressing counterfeit product was "among the highest priorities of the members." The research was conducted pro bono—as are most GMA reports—by information technology/transaction management supplier Inmar and product authentication supplier Authentix. The report included expert insight by those authors, the best practices survey of GMA/FMI members, and was supplemented by a consumer survey previously conducted by Inmar.

The project was scoped to only include products with a human or animal public health threat (it did not seem to be the intent, but these were all FDA-regulated products.)

- "The scope of products covered in this guide includes CPG [consumer packaged goods] – food, over-the-counter medicines, pet and health, and beauty care products. The guide does not cover coupons, apparel, sporting goods, automotive, electronics or other non-food items found in mass merchandisers and specialty retail."

The report used a broad—or macro—definition of counterfeiting, which expanded the focus beyond trademark, patent, or copyright infringement. It did zoom in on illegally manufactured or adulterated goods—specifically not including stolen goods or actions that do not violate the IP rights. In the USA, the "counterfeiting" laws focus on the intellectual property rights.

- "For the purposes of this guide, **counterfeit goods** are defined as illegitimately manufactured or adulterated goods. This guide does not address stolen goods or products such as 'replica' or 'genuine imitation' items that do not otherwise violate a brand owner's rights."

There was a focus—consistent with our previous MSU-FFI publications and research direction—on "detection, prevention, and deterrence."

There was a broad range of best practices noted but few direct recommendations for countermeasures in the case study section of the report, except for the following regarding packaging:

- "[To address packaging anti-counterfeiting countermeasures] the manufacturer enlisted a third-party security company to develop a program that was compatible with already existing programs. Four important steps were taken to combat the unauthorized product:

- Late stage customization to add security post-production
- Tamper-evident security labels with covert and forensic features
- Labels supplied from a secure, third-party print facility
- Labels printed with region-specific information to meet local regulations."

Also, packaging technology expertise was identified as one of the key expert areas:

- "Create a dedicated group that has expertise in 4 key areas: law enforcement, supply chain, packaging technology and legal."

A best practice directly addressed packaging countermeasures:

- "Build anti-counterfeit and brand protection elements into the product design process with the goal to employ in-product and on-package authentication technology."

In summary, this report provides some interesting best practices and a base from which companies can start building a Brand Protection response. While our MSU-FFI is focused on food, none of us can ignore that the bad guys focus on all products. Expanding our perspective to understand the insights in reports like this is essential. There are best practices we can learn from by many adjacent industries.

Defining Food Fraud Prevention to Align Food Science and Technology Resources

Previously published blog post:

Title: Defining Food Fraud Prevention to Align Food Science and Technology Resources

By John Spink • December 16, 2013 • Blog (MSU-FFI 2018)

The EU food fraud resolution just advanced from task force committee to a full European Parliament vote in early 2014. Defining food fraud and a focus on preventative actions are no longer just academic exercises. That said, our new "Defining food fraud prevention to align food science and technology resources" is perfect timing, with very important insight for implementing regulations and industry best practices (Spink et al. 2013a).

Focus Research on Prevention

There have been incredible advances in food science and food integrity testing. A key to our success in preventing food fraud will be the balancing what we "can" do with what we "need" to do (e.g., "do I need to act?". The effort to focus research on prevention will be critical to protecting the food

(continued)

supply – our goal is not to just find adulterant-substances. Our goal is to create a system where they don't get in the food in the first place! From our article, "Whilst better means of detecting food fraud are required, 'successes must be measured in terms of how the activities support prevention. We need a systems approach to optimize the roles of all food supply chain and research partners."

Food Industry Leads the Efforts

In the article, a concept we emphasize and explain is that it is critical to have food experts leading—or at least involved in—every aspect of food fraud prevention efforts. "There are very unique aspects of the complex food production systems that are baffling to outsiders. There are complexities to authenticating food that are unlike any other sciences – the complexity of profiling a multi-component food product requires methodologies that are still far from routine or easy to use and interpret. There is an incredible amount of inherent variation in the same food product produced over the course of a year."

Harmonization of Terms

We emphasize in the article that harmonization of terms and prevention efforts are both critical to a global, efficient, and effective effort. As I've published on and presented for years, Situational Crime Prevention and the use of the Crime Triangle are great way to deconstruct the fraud opportunity and really focus on prevention (we thank you Dr. Robyn Mace, MSU School of Criminal Justice, for introducing our food fraud prevention team to the topic back in 2006 and then Assistant Professor Justin Heinonen on the SARA model and victimology).

The Role of Science and Technology

Of course, traditional food science and the more recent focus area of food integrity (Food Authentication) both have critical roles in food fraud prevention. That said, there cannot be just a technology solution. Food fraud prevention requires a systems approach that includes Supply Chain management, criminology, and other fields, such as quality management. "For food fraud, the straightforward measure of the presence or absence of a contaminant is only part of 'the puzzle,' and in contrast to food safety hazards, there are a seemingly near an infinite number of adulterants. In the case of diversion, stolen goods, or production overruns, the fraud does not include an adulterant at all. Actually, the food fraud is conducted with genuine products."

Acknowledging My Coauthors: Christopher Elliott and Kevin Swoffer

I'm very proud and honored to have worked with coauthors Professor Christopher Elliott and Kevin Swoffer on this article (Spink et al. 2013a). Chris is a world-renowned expert on foods and has conducted some incredible innovative research in food integrity and authenticity. He is the Director of the Institute for Global Food Security at Queen's University (Belfast, Northern Ireland, UK). He also is leading an independent UK review of the food supplies network following the horsemeat scandal. Kevin Swoffer has been a constant colleague and supporter since we met at MSU back in 2007. He is the Director of KPS Resources. He has over 30 years of experience in the food manufacture and retail sectors. He was involved at the founding of the GFSI in 2000 and has been actively involved in its development. More recently, Kevin and I have been interacting with and discussing the Food Fraud Think Tank for the Global Food Safety Initiative. Collaborating on this article was a great opportunity to really harmonize our thinking.

Food fraud is not new, but the science is providing a framework within which we all work. By coordinating our activities—as theorists and scholars first—we can be much more efficient. Play your part and stay up on the latest thinking; link to the article to see the full discussion (MSU-FFI).

Key Learning Objective 2: Integrated Framework for "How Much Is Enough?"

This section reviews an integrated framework based on COSO Enterprise Risk Management to get to the most basic question resource-allocation decision of "how much is enough?" There are many methods and tools the address one part of the system, and the connection to the enterprise-wide management is a final integration step.

The Key Learning Objectives of this section are:

- (1) The most important and most overlooked step is to define the resource-allocation decision-making process.
- (2) The COSO Enterprise Risk Management compliance requirements are the overall system.
- (3) Then, these concepts are applied to the other food fraud prevention methods and tools into the internal controls and integrated frame to help determine "how much is enough?

Monitoring for Efficiency: Review the Current Decision-Making Process

It seems redundant for a risk analysis process to include a review of the risk assessment, but this is the strength and value of the overall controls and provides more transparency and accountability. The process includes different levels of the organization reviewing the risk assessments of other levels. For example, the C-suite reviews the operation and vice versa (Fig. 4.5). Both have their risk assessments reviewed by the board. The Food Fraud Prevention Cycle incorporates these

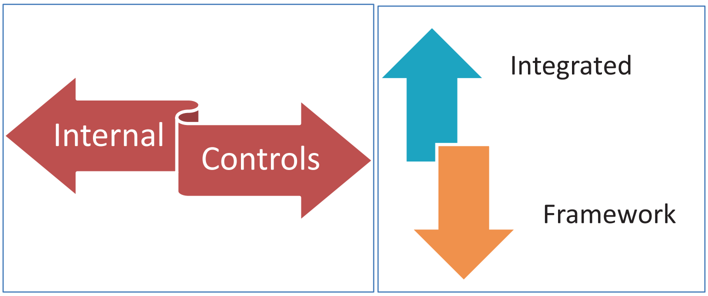


Fig. 4.5 Visual of the horizontal internal controls and the vertical integrated framework—together they "connect everything to everything"

ERM/COSO best practices and connects the ongoing updates of the "fraud opportunity" with the shifting "risk appetite." Each level of these "internal control" steps includes an "integrated framework" reviews and calibrates to the other functions. Each new activity or information has a place to add to the cycle.

ERM/COSO is already a function and standardized method for monitoring the risks. Overall ERM is referred to as "internal controls and integrated framework." The "integrated framework" includes assessments across and within the operations. An example of calibrating the actions within the organization includes correlating the assessments that are conducted. For example, "Principle 8" is "Assess Fraud Risk" and includes a method to root out fraud in fraud assessments (for more, see the Chapter on Business Decision-Making) (PWC 2014; COSO 2016).

Sidebar: ERM/COSO Five Concepts and 17 Principles
The ERM/COSO system explains how the activities are connected when they present the Five Components and 17 Internal Control Principles and this Guide's Five Fraud Risk. This emphasizes that "a comprehensive fraud risk management program is not only the risk treatments or countermeasures but the organization and coordination of the entire process."

"For organizations desiring to establish a more comprehensive approach to managing fraud risk, this [COSO Fraud Risk Management Guide] includes more than just the information needed to perform a fraud risk assessment. It also includes guidance on establishing an overall Fraud Risk Management Program including:

- Establishing fraud risk governance policies
- Performing a fraud risk assessment
- Designing and deploying fraud preventive and detective control activities
- Conducting investigations, and monitoring and evaluating the total fraud risk management program."

The full details of the 5 concepts and 17 principles are presented here. To establish the frame, COSO defines the overall scope of the organization covers the entire enterprise from the very highest board level throughout the operations to all products and services. From COSO:

- **The Organization:** “for purposes of the framework, the term ‘organization’ is used to collectively capture the board, management, and other personnel, as reflected in the definition of internal controls” (COSO 2013) .
  – **Internal Control:** “is a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives related to operations, reporting, and compliance.”

Also, the classification of risk treatment of activities includes (COSO 2016):

- **Preventive Controls: “**designed to avoid a fraudulent event or transaction at the time of initial occurrence.”
- **Detective Controls:** “designed to discover a fraudulent event or transaction after the initial processing has occurred [and hopefully before the accounting transaction is complete].”

Fraud Risk Management Principles (ERM/COSO) (COSO 2016):

Principle 1: Control Environment—The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the Board of Directors and senior management and their commitment to high-integrity control and ethical values regarding managing fraud risk.

1. The organization demonstrates a commitment to integrity and ethical values.
2. The Board of Directors demonstrate independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Principle 2: Risk Assessment—The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

(continued)

7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
   (a) [Note: for food fraud prevention, this defines the requirement to conduct a holistic and all-encompassing assessment.]
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
   (a) [Note: for food fraud prevention, this considers that—beyond risk assessors who may not be well trained or expert on the task—there may be "fraud in fraud assessments."]
9. The organization identifies and assesses changes that could significantly impact the system of internal control

Principle 3: Control Activities—The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.
    (a) [Note: for food fraud prevention, there should be a prevention strategy before tactical countermeasures or control systems are selected.]
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Principle 4: Information and Communication—The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.

13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.

Principle 5: Monitoring Activities—The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the Board of Directors.

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.
    (a) [Note: for food fraud prevention, it is clear that *not* having visibility or correlation into the ERM/COSO system would be a nonconformance.]

The "Internal Controls" are not just monitoring of activities across the business but also vertically. A corporate auditing firm may separately (and confidentially) audit the Board of Directors, the C-suite, and the business operations, and then audit up and down between those functions. This creates transparency (Fig. 4.6).

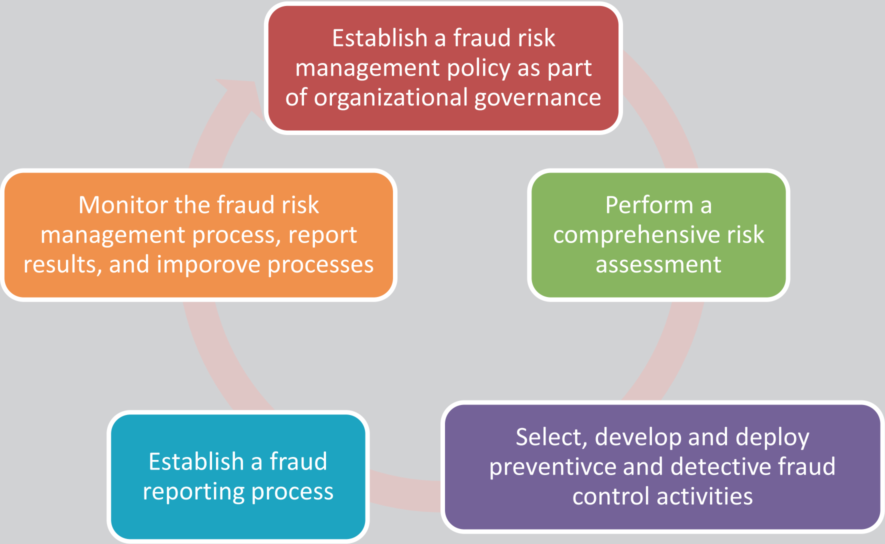

Establish a fraud risk management policy as part of organizational governance
Perform a comprehensive risk assessment
Select, develop and deploy preventivce and detective fraud control activities
Establish a fraud reporting process
Monitor the fraud risk management process, report results, and imporove processes

Fig. 4.6 Ongoing, comprehensive fraud risk management process (based on the 2013 COSO framework). (Adapted from (COSO 2012))

(continued)

For food fraud prevention, could you provide a documented report on examples and evidence that you competently address each concept and principle? Would you be comfortable presenting your document to an auditor, inspector, or investigator? A first step to providing an answer is to fully understand the details and expectation stated in the question. If you are a manager, you might start by asking your food fraud prevention manager or team to answer these questions.

COSO Principles in Detail: Fraud in Fraud Assessments

COSO is a very rigorous and thoroughly developed concept. There are main principles clustered in five groups (COSO 2013). Also, this process is conducted at different levels (board, c-suite, and then operations including comparing assessments across multiple businesses) and within levels (comparing assessments between levels). These "internal controls" and the "integrated framework" are critical to maintaining control of the risk tolerance across an enterprise. For a corporation—big or small—there may be one group or business unit that conducts business way above the risk tolerance of the enterprise thus putting the entire company at risk. In other instances, one group or business unit may be operating way below the risk tolerance and then theoretically reducing the financial return for the enterprise (assuming that taking on more risk provides an opportunity for more reward).

It is completely logical for there to be "fraud" in "fraud assessments." Whenever anyone is subject to a positive or negative consequence, there is a potential for bias based on an inherent "fraud opportunity." COSO/ERM considers this and has identified controls in several of their principles:

> ***Principle 8: The organisation considers the potential for fraud in assessing risks to the achievement of objectives.*** (COSO 2016)

- "Fraud risk scenarios might include material bias in the development of complex accounting estimates, the overriding of controls in stuffing inventory into distribution channels to manipulate revenue recognition, and noncompliance with the Foreign Corrupt Practices Act."
- "In identifying and evaluating those risks, management investigates incentives, pressures, opportunities, attitudes, and rationalization that might exist throughout the company in different departments and among various personnel. This undertaking equips management to determine the mitigating actions it should take to reduce to acceptable levels any risks of material misstatement due to fraud."

So, "fraud" in "fraud assessments?" The concept of the related bias in business decision-making is a science that has been studied extensively by leaders such as Bazerman (Bazerman and Neale 1993; Bazerman et al. 2002, 2003; Bazerman and Chugh 2006). Here are several basic scenarios that apply to food fraud prevention:

- ***I want to grow my group:*** An up-and-coming manager who wants to increase their responsibility would have a bias toward finding *more* fraud and expanding their budget and head count. People don't get promoted for identifying there is "no need for change."

- ***I want to reduce my work:*** Another manager may want to reduce their workload and thus would be predisposed to *under-estimate* the risks to *avoid* more responsibility or employees to supervise.
- ***I really do/don't like this topic":*** Then there is a motivation to become—or avoid becoming—experienced in a new type of fraud or fraud prevention in general. Many times a manager is put into "cross-functional" positions for career growth. A "sales" track manager who is put in charge of "Brand Protection" may be biased to stay focused more on "sales." (If they get "too good" at the new work functions, they may be forced to stay!) Growing experience in controlling a problem—rather than succeeding in a high growth or high impact area—may not be attractive.
- ***Contractor or supplier—I want more business:*** An external consultant who is hired to investigate or mitigate fraud risks would receive more business if there is more fraud. So a fraud investigator would have an inherent bias to find fraud to justify more future fraud investigations.

Overall, based on psychology theory and empirical business research, there is a potential for "fraud" in "fraud assessments" if the risk assessor has a vested interest or benefit from the outcome of the assessment. COSO/ERM considers this in their "Principle 8."

Iterative Cycle: Review of the Process Itself

An important process step is to take the time to review the base method or process itself (MSU-FFI 2017; MSU FFI 2017). Food fraud prevention is an evolving vulnerability, and there are many new innovations in not only countermeasures and controls systems but also in implementing the process. For example, Enterprise Risk Management/COSO is not well known by food safety professionals and with even less actual application of the concepts. The Sarbanes-Oxley Act was unknown to those people developing or managing HACCP plans.

For food fraud prevention, there is an iterative cycle; meaning that when there is new information (e.g., a new incident, a changing fraud opportunity, or reduced enterprise-wide risk appetite), the entire system is reviewed and could re-calibrate. Usually, when resources (e.g., funding or employee time) is allocated, there is no mechanism to dial back down the investment. A new countermeasure or control is put in place to combat a concern or new issue, but there is no standard method to review "how much is enough?" and if systems should be reduced. It is fundamentally contradictory for a food safety professional to *increase* a risk. The key is not just "risk" but to clearly understand and address the level of "unacceptable risk."

Without the method to reevaluate the current countermeasures and controls systems in relation to the shifting fraud opportunity, then costs will go up and up even if the business is well within the risk appetite. At the same time, there may be some risks that are unknown and where the business may be operating at an unacceptably high level of risk.

Sidebar: "How Much Testing Is Optimal?" It Depends

An example would be to test for horsemeat in beef. When there is a crisis, new countermeasures and control systems are put in place for detection and emergency response. There are many unknowns, so a broad testing plan is critical to getting a perspective on the entire supply chain. Also, there is concern that there is an illegal product in the current supply chain so thorough testing is critical. Once the new system is in place, usually one of two things happens:

1. After the crisis is over, the testing stops.
2. The high "crisis-level" testing never stops.

What is the "right" level of activity rests on "what is the right question?"

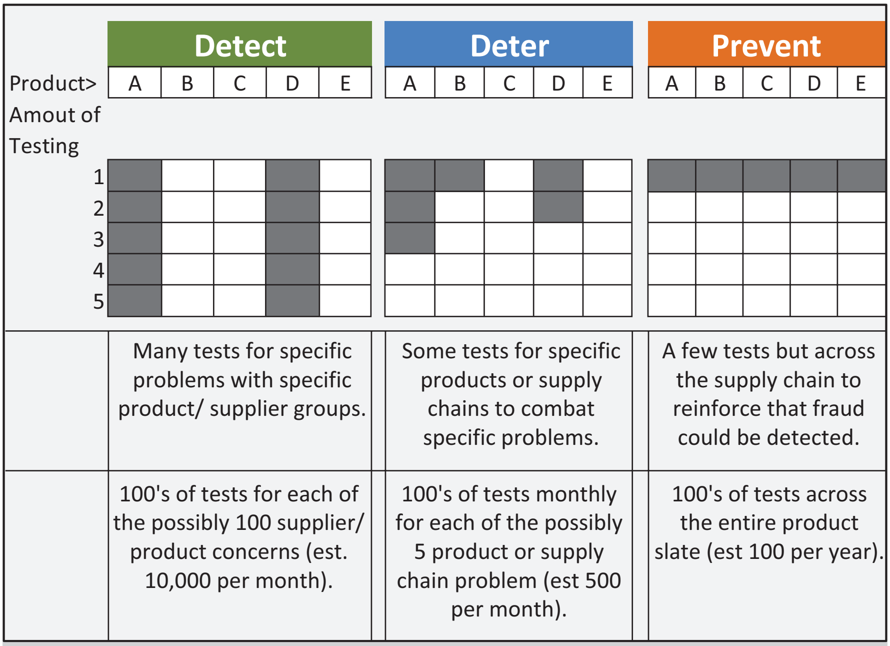
In the midst of a crisis where horsemeat is found in the marketplace, then massive and holistic "detection" programs should be implemented. This would be similar to traditional food safety monitoring tests. After the crisis, if there are still active perpetrators or product still trickling in, then a lesser but still random "deterrence" protocol is ideal. Once the incident has passed and the vulnerability is understood within the Food Fraud Prevention Strategy, then an extremely efficient yet very small "prevention" program can be implemented and defined.

To provide a more direct application, a hypothetical example is provided for the amount of testing to support the activity of "detect," "deter," and "prevent." There are appropriate protocols for different objectives such as "detection test plan, "deterrence test plan," and "prevention test plan" (Fig. 4.7).

Detection test plan: The goal is to quickly and thoroughly "detect" the fraudulent activity and remove the product from the supply chain to reduce future product recalls or liability. The focus of the "detect" activity is for an intervention to find known (or confirmed suspicious) incidents. There would be a (1) clear identification of a single or few products and (2) particular fraud acts or adulterant-substances. During the "detect" focus, there could be (1) 100's of food authenticity tests conducted on (2) possibly 100 supplier/product combinations which (3) could result in 10,000 tests per month throughout the year crisis. The 10,000 tests per month do attract a lot of attention for supplier research and development investment.

- Application: Using the horsemeat incident as an example, during and after the incident, there were massive-scale horsemeat species test plans put in place. There were also often species tests for related species depending on regions such as zebra, fox, pork, water buffalo, and others. The goal was to conduct a comprehensive and all-encompassing process to make sure there was no fraudulent horsemeat in the proprietary supply chain.

Deterrence test plan: The goal is to "deter" a specific fraudulent activity, so fraudsters are persuaded not to attack. The focus on the "deter" activity is to combat a specific fraud opportunity that is probably unique to an ingredient,



	Detect					Deter					Prevent				
Product>	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E
Amout of Testing															
1	▨			▨		▨	▨		▨		▨	▨	▨	▨	▨
2	▨			▨		▨			▨						
3	▨			▨		▨									
4	▨			▨											
5	▨			▨											
	Many tests for specific problems with specific product/ supplier groups.					Some tests for specific products or supply chains to combat specific problems.					A few tests but across the supply chain to reinforce that fraud could be detected.				
	100's of tests for each of the possibly 100 supplier/ product concerns (est. 10,000 per month).					100's of tests monthly for each of the possibly 5 product or supply chain problem (est 500 per month).					100's of tests across the entire product slate (est 100 per year).				

Fig. 4.7 Review of the optimal amount of food authenticity testing for specific objectives of detect, deter, or prevent (with hypothetical example)

product, or supplier/region combination. Although there is no active incident—or this would be in the "detect" category—there is a concern that there is a fraudulent product in the supply, and the goal is to find the fraudulent product but more to specifically lead the fraudsters to be concerned they may be caught. There would be a (1) broad set of target products and (2) particular fraud acts or known adulterant-substances. During the "deter" focus, there could be (1) 100 s of food authenticity tests conducted on (2) possibly 5 supplier/product combinations per ***year*** which could result in (3) 100 tests per ***year***. The 100 tests per ***year*** is a lot less attractive market for a supplier than the 10,000 tests per month in the detect test plan.

- ***Application:*** Using the horsemeat incident as an example, after the company conducted the deter test plan, there was a frequent but lesser series of species tests conducted. For example, the company may have reduced the focus to the only test for horsemeat and also only for incoming goods.

Prevention test plan: The goal is to "prevent" food fraud across the entire product slate and to address "unknown-unknowns"—this is a real intelligence analysis science concept. The first "unknown" is that we don't understand who the perpetrators are or even *if* they will attack (e.g., something that is

(continued)

completely a surprise and what is sometimes referred to as a "black swan event"—responses are often "why in the world did they try to do that?"). The second "unknown" is that if they do act, we don't know when or where they will attack (e.g., it is known melamine is a type of food fraud, but we don't know where they will attack). For melamine in infant formula, it is a known type of attack (the first "known") but with an unknown exact time and place (the second "unknown").

- Application: Using the horsemeat incident as an example, a company may move beyond horse to consider ***all*** types of protein fraud—other species, lower quality cuts of meat, spoiled meat, non-animal protein, alternate protein products such as powdered ground meal, country of origin, declared processing method, etc. The company would select a wide range of tests to be conducted on a wide range of products and on a very small scale.

To continue focusing on the "prevent" plan, these unknown-unknowns, a focus on reducing all vulnerabilities is efficient because the perpetrators are so creative that we may not yet be aware of how or where they may attack; we don't know what to try to detect or deter. The focus on the "prevent" activity is to focus on "vulnerabilities" regardless of whether there is any known or even suspicious activity. This is partially just alerting fraudsters that they "could" get caught in a random test but also to conduct very broad and random information gathering.

- For a "detect" or "deter" focus on preventing food fraud, there would be a (1) broad set of target products to protect (a medium size company could have 1000 products) and (2) a broad set of fraud acts or adulterant-substances to test for (how many adulterant-substances could be used?).
- For a "prevent" focus, there could be (1) 100's of food authenticity tests conducted on (2) possibly 5 supplier/product combinations, which could (3) result in 500 tests per month during the crisis.

Thus, an efficient and insightful Food Fraud Prevention Strategy could actually require a very small set of authenticity tests to effectively monitor the supply chain and holistically reduce the fraud opportunity.

Key Learning Objective 3: The Process Steps

This section reviews specific key process steps of (1) scanning, (2) Enterprise Risk Management-based corporate risk map, and (3) an iterative that is referred to here as the "corkscrew approach." And once the theory is in place, then the overall management process can be implemented to support the defining the operation of these specific functions. This section brings together all the concepts and explains how the overall system operates in motion.

The Key Learning Objectives of this section are:

- (1) To understand scanning that gathers and processes new information or insight
- (2) Apply Enterprise Risk Management (ERM/COSO) for decision-making
- (3) The "corkscrew approach" that starts light and goes as deep as directed by the needs of the resource-allocation decision-maker

New Information: Monitoring for Changes

There are several functions that make up the scanning concept including (1) incident reviews (of known and internal incidents), (2) scanning (broader scouting of changes such a market supply fluctuations or external incidents), and (3) public policy changes. These three are interrelated, and the information is used to provide new insight to understand the "fraud opportunity." For each of these functions, there are no current standard operating procedures *yet*. It is most efficient to adapt current or new work processes to the specific fraud opportunity and needs.

- ***Incident reviews*** are known incidents where there is some specific type of information. These provide the most detail and value.
- ***Scanning*** is both seeking broader changes such as market conditions or of external incidents.
- ***Public policy*** changes could be either new laws, statements of new priorities, or identification of new investigations.

Together these provide broad coverage of the types of new information that could influence the fraud opportunity.

Sidebar: Selection of Strategic Authentication and Tracing Programs

Previously published blog post (Fig. 4.8):

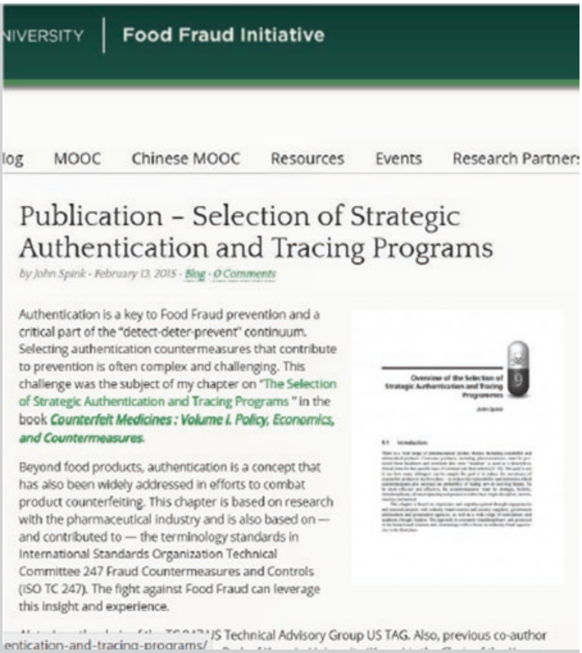
Title: Publication—Selection of Strategic Authentication and Tracing Programs

By John Spink • February 13, 2015 • Blog (MSU-FFI 2018)

Authentication is a key to food fraud prevention and a critical part of the "detect-deter-prevent" continuum. Selecting authentication countermeasures that contribute to prevention is often complex and challenging. This challenge was the subject of my 2012 chapter on "The Selection of Strategic Authentication and Tracing Programs" in the book Counterfeit Medicines Volume I*:* Policy, Economics, and Countermeasures (Spink 2012).

Beyond food products, authentication is a concept that has also been widely addressed in efforts to combat product counterfeiting. This chapter is based on research with the pharmaceutical industry and is also based on—and contributed to—the terminology standards in International Standards

(continued)



Publication – Selection of Strategic Authentication and Tracing Programs

by John Spink - February 13, 2015 - Blog - 0 Comments

Authentication is a key to Food Fraud prevention and a critical part of the "detect-deter-prevent" continuum. Selecting authentication countermeasures that contribute to prevention is often complex and challenging. This challenge was the subject of my chapter on "The Selection of Strategic Authentication and Tracing Programs" in the book *Counterfeit Medicines : Volume I. Policy, Economics, and Countermeasures.*

Beyond food products, authentication is a concept that has also been widely addressed in efforts to combat product counterfeiting. This chapter is based on research with the pharmaceutical industry and is also based on — and contributed to — the terminology standards in International Standards Organization Technical Committee 247 Fraud Countermeasures and Controls (ISO TC 247). The fight against Food Fraud can leverage this insight and experience.

S Technical Advisory Group US TAG. Also, previous co-author

entication-and-tracing-programs/

Fig. 4.8 Blog post image (Copyright Permission Granted) (MSU-FFI 2018)

Organization Technical Committee 247 Fraud Countermeasures and Controls (ISO TC 247). The fight against food fraud can leverage this insight and experience. (Note: I am the chair of the TC 247 US Technical Advisory Group US TAG. Also, previous coauthor and research colleague Dr. Hyeonho Park of Yong In University (Korea) is the Chair of the Korean TAG.)

The Goal of Authentication Countermeasures

The chapter discussed the pharmaceutical focus on all fraud versus only counterfeiting. This is similar to the food industry discussion of combating all fraud or adulteration. There is an emphasis on the goal of reducing crime, not just catching fraudulent product or the fraudsters. The goal is *not* to catch product but to prevent the attack in the first place. A couple of quotes from this chapter addressed these concepts.

- "The term 'fraudster' is used as a descriptive, formal term for this specific type of criminal and their activity."
- "The goal is not to see how many infringers can be caught: the goal is to reduce the prevalence of counterfeit product in the first place – to reduce the vulnerability and determine which countermeasures also increase our probability of finding new or evolving threats. To be most efficient and effective, the countermeasures must be strategic, holistic, interdisciplinary, all-encompassing and proactive rather than single-discipline, narrow, reactive and tactical."

Start with Intervention

Often the selection of countermeasures is a reaction to a single catastrophic incident. When horsemeat was found in beef, the logical, urgent, and necessary response was to immediately start conducting horse species authentication tests (Lam and Spink 2018; Spink 2019a, b). The supply chain had to be investigated *right now*. No discussion of strategy or prevention, the response had to be immediate. As we covered in our 2009 article titled "Defining the Public Health Threat of Food Fraud," the starting point after an incident is intervention, then we move to response, and only after we have more information do we shift to prevention. Unfortunately, enterprises—companies and countries—often feel they cannot take the time to shift to prevention or that activity is the responsibility of "someone else." There are good intentions to be proactive, but often a new crisis arises that takes the available resources. To break the reactive cycle, resources need to be assigned explicitly to prevention.

Intervention Shifting to Response Then to Prevention

To shift from response back to prevention, there must be a strategic priority and a systems approach. The Food Fraud Prevention Strategy does not have to be complex or big. The hardest part is taking the time to develop the corporate policy and establishing the strategy.

Picking a single countermeasure—such as immediately conducting horse species tests on all inventories—is a single tactical solution and not in and of itself strategic. It is a "product," not a "program" or "strategy." The countermeasure has a very specific and defined objective, which is detection.

- "Picking a single technology and hoping it is a magic solution is easy, but technology is only one of the many aspects of an anti-counterfeit strategy. The solutions are systems, not tools, and must include what is referred to as a layered approach. What is difficult is strategically explaining why and how it will help – including in comparison with all other countermeasures – and to not only expect but also anticipate how the bad guys will try to circumvent this system or countermeasure."

If there is a known hazard, it is logical and necessary to drop everything and address this problem which is probably considered a "reasonably foreseeable hazard." If there are known incidents, then it is by definition "reasonably likely to occur." Beyond what may be written or published in a law, regulation, or rulemaking, this is a legal and brand equity liability.

Systems Approach and Foundation

Without a shift to prevention, there will be *déjà vu* of reactionary emergency responses that are resource intensive and do not prevent future occurrences. Taking the time and effort to focus on a preventative systems approach is consistent with quality management principles such as Six Sigma or food HACCP programs.

(continued)

- "Understanding anti-counterfeit strategy is based on understanding the nature of the fraud and the fraudster. When this is achieved, there is a better chance of not only combating current risks but, by understanding the inherent vulnerability, predicting and anticipating the next moves as well. [The] counterfeit and substandard medicines 'public health threat is similar to a disease that requires continual surveillance, monitoring and treatment (e.g., diabetic populations) rather than treating a single event (e.g., a broken bone)'." (Spink 2012)

Foundation: Harmonize Terminology

An important foundation is to establish agreement on definitions. Your company or country may have unique terminology, so, in that case, it would be even more important to define your terms in relation to the other common usage of the terms. Refer to standards or regulations whenever possible. From the International Standards Organization, International Standard ISO/DIS 12931: Performance criteria for authentication solutions for anti-counterfeiting in the field of material goods, counterfeiting of material goods, or physical product (Spink 2012):

- "**Counterfeit**: (verb) to simulate, reproduce, or modify a material good or its packaging without authorization" (ISO 2011).
- "**Counterfeit good**: material good imitating or copying an authentic material good."

For combating food fraud, it would also be important to define food authenticity programs in relation to the ISO definition of authentication. The traditional food adulteration concept is similar but usually focused on testing the specification of the product; it does not really cover components that are authenticated to define that the product is genuine. Our ISO TC 247 felt that terminology was very important and it is the subject of a New Work Item Proposal (NWIP) and Work Group (WG).

- "As of January 2011 and led by Technical Committee 247 Fraud Countermeasures and Controls (ISO TC 247), ISO became involved in anti-counterfeiting. The current draft standard ISO/DIS 12931 [11] includes working definitions of:
  - '(a) ***authentication*** as the 'act of establishing whether a material good is genuine or not.'
  - '(b) an ***authentic good*** as a 'material good produced under the control of the legitimate manufacturer, the originator of the good or holder of intellectual property rights.'
  - '(c) an ***authentication tool*** as a 'set of hardware and/or software system(s) that is part of an anti-counterfeiting solution and is used to control of the authentication element.'"

An ISO development that occurred after this chapter was published the definition of product fraud and fraud opportunity and the related food fraud topic of vulnerability (ISO/TC247 WG2 N0010 PWI). From that ISO draft:

> Scope of ISO TC 247: Standardization in the field of the detection, prevention, and control of identity, financial, product and other forms of social and economic fraud.

- "***Fraud:*** '1) wrongful or criminal deception intended to result in a financial or personal gain
  - '2) A willful act of deception that creates human or economic harm.
  - Note 1 – types of fraud may include: product related such as counterfeiting, illicit diversion, alteration, intellectual property infringement; Identity fraud such as identity theft (imposter fraud, disguise, credential alteration) and document fraud such as cheque fraud, banknote fraud, certificate fraud
  - Note 2 – the consequences of 'harm' and 'deception' may vary between jurisdictions and cultures."
- "***Fraud opportunity:*** The conditions which provide an attractive target for fraudsters, regardless of if a fraud has been perpetrated. This is similar to the criminology concept of the 'crime opportunity' in the 'Crime Triangle.'
  - Note1 – A crime triangle means 3 elements; 1. Motivated offender, 2. Suitable crime target, 3. The absence of a capable guardian."
- "***Vulnerability:*** area of exposure to fraudulent activities."

Assessing the Situation

The first step in a proactive, systems approach to food fraud prevention is assessing the situation. There have been many risks or vulnerability assessments developed over the years. There are current activities specifically for food fraud prevention. Understanding and explaining the foundation is the first step—ISO 31000 refers to this as "Establishing the Context."

- "This section provides an overview of an anti-counterfeit strategy to assist in risk assessment before choosing countermeasures. The first step is to conduct a risk assessment of the counterfeit product risk, which includes reviewing company and industry incidents. The second step is to seek to understand the nature of the fraud and fraudster, which includes understanding the criminology aspects of deterrence."

Defining the needs of data or "intelligence analysis" is critical to the effectiveness of assessments. This is a key focus in our "Analysis of Food Supply Chains for Risks and Resilience for Food Fraud/ Food Crime" UK grant with Professor Christopher Elliott and Queen's University Belfast. I am leading Work Package 3 "Incident data collection to assist in intelligence analysis" (note: results published in 2019 (Spink et al. 2019)).

(continued)

Also, my 2009 MSU Packaging Science doctoral dissertation was actually on this subject: “Analysis of counterfeit risks and development of a counterfeit product risk model” (Spink 2009).

To evaluate the situation, there are two parts to the preliminary assessment: incident review and the vulnerability assessment. A key point is to define exactly how the assessments will be used. Often the incident review is used to present the scope of a known vulnerability, as well as to conduct cluster analysis to identify key focus areas (see blog post on our article on a Product Counterfeiting Incident Clustering Tool). For evaluation by a company in an Enterprise Risk Management (ERM) system, the assessment must be in financial terms—public health may be the first priority, but it is because of the potentially catastrophic financial impact (see our previous blog post of our New Food article on decision-making).

The incident review is often very revealing, especially for managers who have not been familiar with the topic. Often the most significant threats are from within the legitimate supply chain which includes:

- “Rogue participants are not always autonomous and completely external to the supply chain, and can range from organizations outside the supply chain to companies in the legitimate supply chain that occasionally perpetrate fraud, to a single individual acting alone from within the supply chain.”
- “It is important to understand that, in the worst case, the counterfeiters are criminals not concerned with breaking the law, sociopaths not concerned with cheating others and not educated about the inherent public health or safety dangers.”
- “They are often ‘irresponsible defendants’ who flee, obfuscate ownership of their assets and effectively launder their money out of reach, who have networks that can re-form unnoticed, and who are often part of violent, criminal network.”

The Value (and Risk) of Preliminary Assessments

We are accustomed to conducting extremely data-driven food safety risk assessments. For food fraud prevention, as with many other risks and risk assessments—such as Military Standard 882D and Delphi method—expert opinion and preliminary qualitative assessments have a role. Even though it may seem rudimentary and straightforward, a preliminary, top-down, qualitative vulnerability assessment helps scope the overall situation. This simple method often helps reveal a previously unknown—or until now underappreciated—hazard. It is not uncommon for a full policy and strategy development process to get sidetracked to address an identified hazard. Even if this is a simplistic, preliminary exercise, the process may identify a severe hazard.

If the hazard is now known and occurring, it is by definition "reasonably likely to occur" and a "reasonably foreseeable hazard." Countermeasures must be taken.

Selection of Countermeasures

The published chapter provides a thorough overview of the selection of product fraud countermeasures. The key point is:

- "For every countermeasure, there should be a precise description of exactly how it detects or deters specific types of fraud and fraudsters."

The chapter also includes a comprehensive list of product authentication countermeasures (MSU-FFI).

End of the blog post.

Sidebar: Selecting Countermeasures—Specific Scoping Questions

There are specific scoping questions from the chapter on "The Selection of Strategic Authentication and Tracing Programs" in the book Counterfeit Medicines Volume I: Policy, Economics, and Countermeasures (Spink 2012).

"To turn attention to assessing anti-counterfeit countermeasures, several practical questions are necessary:

- **Overall Anti-counterfeit Goal – To Do What?**
- '(a) Where is the product being compromised?'
- '(b) Where will the product be verified?'
- '(c) Who will verify it, using what methods?'
- '(d) How will you use the results of the investigation?'"

Then next, "To add to this set of questions, an optimal anti-counterfeit programme must include":

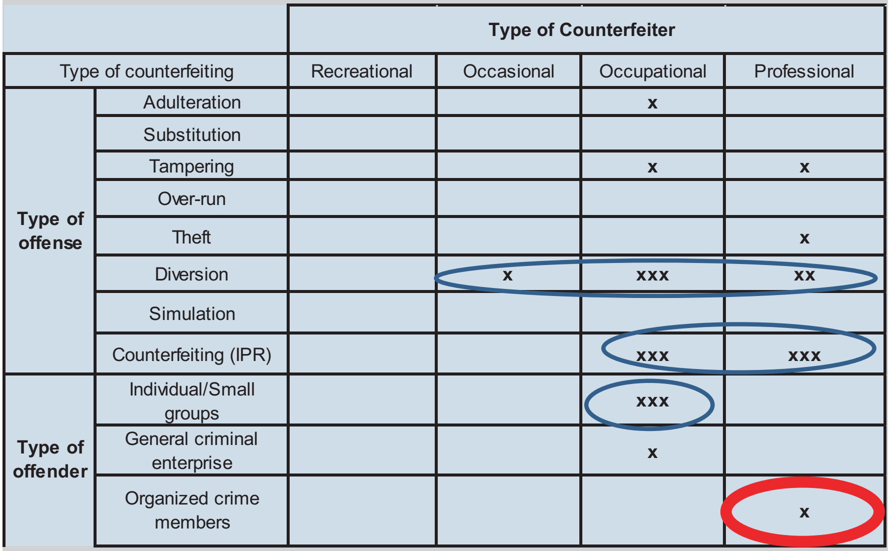
- **Basic Understanding of the Fraud Opportunity—Why Will It Work?**
- '(a) an understanding of how the counterfeit product is entering the marketplace'
- '(b) the technical capabilities of the range of counterfeiters'
- '(c) the capabilities and willingness of supply chain stakeholders to partner in fighting the risk'
- '(d) the capabilities and willingness of governmental enforcement'
- '(e) consumers' awareness of the problem'
- '(f) consumers' willingness to participate in anti-counterfeit actions (e.g., consumer authentication)'

Sidebar: Product Counterfeiting Incident Clustering Tool—PCICT

There is often a significant challenge of organizing and assessing a wide range of food fraud incidents. To help this challenge, the Product Counterfeiting Incident Clustering Tool (PCICT) was developed and was published in a peer-reviewed, refereed, scholarly journal (Spink et al. 2014). The application of the PCICT was further formalized when it was codified in ISO 22380 Security and resilience—authenticity, integrity, and trust for products and documents—general principles for product fraud risk and countermeasures (ISO 2018). The tool is published in ISO as a recommended method for organizing and analyzing incident data.

The PCICT is based on basic criminology theory of incident clustering. Clustering is used to identify a group of crimes or criminals usually visually presented on a map or in a table. This can be used to inform the assessment of the "fraud opportunity" and to complete the Food Fraud Vulnerability Assessments.

An example of the PCICT is provided (Fig. 4.9). A product fraud data set was gathered and plotted based on the "type of counterfeiter," "type of counterfeiting," and "type of offender organization." The example shows that the incidents were primarily conducted by "occupational" and "professional" counterfeiters and the "diversion" and "counterfeiting" types of fraud. The offenders were usually "individuals" or "small groups." This assessment helps prioritize countermeasures and control systems. The findings from the incident clustering would lead to a focus on "diversion" and "counterfeiting." The



		Type of Counterfeiter			
Type of counterfeiting		Recreational	Occasional	Occupational	Professional
Type of offense	Adulteration			x	
	Substitution				
	Tampering			x	x
	Over-run				
	Theft				x
	Diversion		x	xxx	xx
	Simulation				
	Counterfeiting (IPR)			xxx	xxx
Type of offender	Individual/Small groups			xxx	
	General criminal enterprise			x	
	Organized crime members				x

Fig. 4.9 Product counterfeiting incident clustering tool (PCICT) with examples of clustering (Copyright Permission Granted) (Spink et al. 2014; ISO 2018)

types of counterfeiters are "occupational" and "professional" so would seem to be informed adversaries who would respond to warnings of tighter supply chain controls. Also, the offender organization is identified as "individual/ small groups" so possibly from within the supply chain. Knowing that the perpetrators are probably already operating within the legitimate and authorized supply chain leads to a realization that they can be directly communicated through messages sent to current suppliers. By using this tool and method, there is the opportunity to directly deter the "motivated offenders"—remember, the goal is not to catch food fraud but to prevent it from occurring in the first place.

The PCICT includes the type of offense which is similar to the types of fraud. The types of counterfeiter can also be presented as a type of fraudster. The types of counterfeiters or fraudsters include ((Spink et al. 2013b) which is also cited in (ISO 2018)):

- **Type of Counterfeiters/ Types of Fraudsters:**
  - **Recreational:** for entertainment or amusement.
  - **Occasional:** infrequent, opportunistic.
  - **Occupational:** incidents at their place of employment either as an individual act, or in collaboration with the company.
  - **Professional:** crime fully finances their lifestyle .
  - Removed – **Ideological:** Domestic or international terrorist who commits this act to make an ideological statement or to economically harm an entity (note: later this type was removed since the goal of this perpetrator is "economic gain." Later they would use their funds to conduct the ideologically motivated act.).

- Food fraudsters seem to be most likely "occupational" type; meaning that they conduct their operation within their business (their occupation) in the legitimate supply chain. This type of criminal can be patient and wait for a favorable *fraud opportunity*.

  And the final factor is (Spink et al. 2013b):

- **Type of Offender Organization**
- **Individual/Small Groups:** "Although there are IPR cases involving solo or small groups of individuals who operate out of their homes, garages, or small storage facilities, there is little reporting and no actual analysis of the relative importance of such operators to the threat. … This lack of reporting and analysis may be a reflection of the fact that individuals and small operations are a less attractive target for law enforcement than larger enterprises engaging in a more significant infringing activity or also committing other more serious offenses."

(continued)

- **General Criminal Enterprises (Members):** An example used to identify this group is “a criminal enterprise of 30 defendants charged with smuggling into the United States counterfeit cigarettes worth approximately $40 million and other counterfeit goods, including pharmaceuticals worth several hundred thousand dollars.”
- **Organized Crime Members (Members):** “‘Organized crime groups are a specialized subset of criminal enterprises that maintain their position through the use of actual or threatened violence, corrupt public officials, graft, or extortion. For example, members of an organized crime group in New York trafficked in counterfeit goods and were charged with attempted murder and conspiracy to commit murder.’ A challenge of deterring this group is their use of violence and the risk of retaliation to a company or investigators (e.g., violence or sabotage).”
- **Terrorist Organizations (Supporters):** “Terrorist supporters have used intellectual property crime as one method to raise funds. Central to this judgment is the distinction between terrorist supporters who merely provide funding and resources to a terrorist organization versus terrorist organization members who engage in the actual terrorist activities of violence. … It is widely reported terrorist supporters may use IPR crimes to provide indirect financial support to terrorist organizations, but little current evidence suggests terrorists are engaging directly in IPR crimes to fund their activities.” There are many confirmed cases of product counterfeiting for funding terrorist acts” (for more on this see (Spink 2015a, b)).
- Gangs (Supporters): “According to the National Gang Intelligence Center (NGIC), there are three subtypes of gangs: street gangs, prison gangs, and outlaw motorcycle gangs. Of these three groups, street gangs most often engage in and profit from IP theft, therefore this analysis focuses exclusively on this subtype.”
- **Foreign Government Offenders:** “The primary motivation in this offender group is the theft of sensitive United States information including trade secrets and economic espionage. There are examples of state-sponsored counterfeits of branded products.”
- **Warez Groups:** “[A] less common motivation for committing IPR [infringement] is personal fame and notoriety. These individuals are often members of Warez groups, sophisticated and hierarchical criminal groups operating in the United States and abroad that specialize in distributing infringing movies, music, and software via the Internet.”

In the types of offender list, there is an additional differentiator defined by the FBI as “member” or “supporter” (FBI 2012) in (US National Intellectual Property Rights Center [IPR Center] 2011).

- **Member:** “may have known ties to a larger criminal organization but is acting separately for the operation of the fraud. (For example, a member of a gang may be producing and selling counterfeit products with or without this being a formal activity of the gang.)”

- **Supporter:** "may agree with the ideology of a group, but does not participate in their group activities, and provides some type of product or service such as funding. (For example, a supporter of a terrorist organization may be producing and selling counterfeit products and then donating some of the proceeds to that terrorist organization)."

In the PCICT figure, there is a particular emphasis on "Organized Crime Members." While this may be considered by many as "just another group of offenders" a company's Corporate Security team usually takes a special interest in this group. Organized Crime—not just "crime that is organized" but the organized and structured large-scale criminal enterprises—is an especially concerning adversary since they may post a wider range of threats including sabotage, violence, and unfair competitor practices, and depending on their infiltration into the local government could create regulatory or criminal threats (e.g., corruption or integration into the local government could lead to the use of government regulators to retaliate).

The PCICT was included and codified in the 2018 publication of the ISO 22380 standard (ISO 2018). When using the PCICT, above referencing a peer-reviewed, scholarly journal article, an additional level of credibility or authority can be used by reference to ISO 22380.

Sidebar: Analysis of Product Fraud by Using the Counterfeit Product Risk Model (CPRM)

There are many reasons to assess the product fraud risk information, and they each require a different type of methods or tools. A hierarchy of goals is provided with an explanation of the need and then examples of methods, tools, or processes (Table 4.1).

This section will review the "Counterfeit Product Risk Model (CPRM)" which was the subject of a 2009 Ph.D. Dissertation (Spink 2009).

From the report abstract:

> Product counterfeiting is growing in both scope and scale. There is a need to take a holistic, all-encompassing approach to the anti-counterfeit strategy, including the development of a Counterfeit Product Risk Model (CPRM) to support the need for an assessment. This research process collaborated and leveraged a wide variety of academic and industry expertise utilizing a literature review and interdisciplinary peer consultation to develop the Counterfeit Product Risk Model for consumer products. The range of disciplines for the research included: Packaging, Food Safety, Criminal Justice, Supply Chain/Logistics, Risk Analysis/Risk Assessment, Food Law, Food Safety, food defense, Intellectual Property Rights Law, Political Science, and Social Science. For example, the Criminal Justice concepts include 'the chemistry of a crime' and 'the crime triangle.' The Counterfeit Product Risk Model focuses on the probability portion of a traditional probability versus severity matrix, uses qualitative ranking, and due to the nature of the risk and the data, emphasizes extensive use of expert panels.

(continued)

Table 4.1 Hierarchy of risk assessment goal, explanation, and examples of methods or tools from this book

Goal	Explanation	Examples from this book include:
To rank all risks in relation to the enterprise-wide risk tolerance	Gather information and insight to conduct a Food Fraud Vulnerability Assessment. To be complete, this will compare this new suspicious activity or problem with all other risks within the organization	e.g., FFIS/ FFVA
Sort incidents and vulnerabilities to understand the type of counterfeiting, counterfeiters, and offender organizations	After gathering a wide range of incident information or after action reports, there is a need to sort and categorize the findings to identify root causes. The output would be general insight such as a cluster of incidents in a specific type of fraud conducted by a specific type of fraudster and offender organization	e.g., PCICT
Monitor market commodity price fluctuations	Review the changes in supply and demand based on fluctuating current and futures product prices. An increase in price, which could be signaled by a projected short supply of product, is new information to consider in a Food Fraud Vulnerability Assessment	e.g., Bloomberg commodity news feed, etc.
Monitor public information for new incidents or trends	This is a scanning function to gather new information and insight on suspicious activity or potential problems. The processed information would feed into the FFVA	e.g., open source monitoring such as Internet keyword searches, keyword news alerts, or social media monitoring
Review suspicious activity to understand the problem in detail such as if it is an illegal act	This is a method to process suspicious activity concerns to evaluate if there is a fraud opportunity or incident and also the likelihood and severity. The information would be fed into the FFVA	e.g., FF-SAR
Use available information to identify the root cause of the system weakness	This is a variation of the other new information or insight gathering that expands to gather enough information on how the fraud act was conducted. The analysis would provide support for selecting countermeasures and control systems	e.g., open-source searches for vulnerabilities in hot spot analysis, pinch-point review
Review the overall counterfeit product risk	Review known information and expert insight to assess the overall fraud opportunity of the enterprise. This provides insight into the general system weaknesses	e.g., CPRM

> This research defines five factors related to counterfeiting: Counterfeit-History, Counterfeit-Attractiveness, Counterfeit-Ability, Counterfeit-Hurdles, and Market Profile. The Model defines the derivation and integration of sub-factors, which ‘roll-up’ to determine the rank of the factors.

The model was then validated using a survey of 33 industry and agency experts. The survey included 17 ratings by people at a Corporate- or Vice-Presidential level, and included six $1–$5 billion revenue companies and sixteen over $5 billion revenue companies. A broad and representative balance of industries was included: food, beverage, healthcare, pharmaceutical, medical device, law, finance, insurance, risk, consumer electronics, software, industrial original equipment manufacturers, and consumer packaged goods.

Assessing Agreement analysis was conducted on the surveys, and the interpretation of the result was an 'almost perfect agreement' with the model. Fleiss' Kappa analysis was conducted to assess agreement over random chances, and this result was also an 'almost perfect agreement.' The research included a Case Study to demonstrate the use of the Model.

This research provides a valuable analysis of anti-counterfeit strategy, including an extensive look into the historical information. It provides a theoretically supported Counterfeit Product Risk Model that will assist in disrupting the 'chemistry of the crime.

The overall CPRM hierarchy of risk factors and sub-factors builds to the overall risk rank (Fig. 4.10) (Spink 2009). The first step is to develop a *draft* of what seem to be the most important factors and sub-factors—the details are expected to adjust and change as more information is gathered and as the risk assessor becomes more familiar with the model and problem.

Once the factors and sub-factors have been identified, then the ranks can begin to be assessed. The CPRM emphasizes a start beginning with a very simple set of information which could be only subject matter expert insight. As the "low certainty" and "low robustness" assessment is concluded, there can be a process check to identify if or exactly what additional information is needed.

It is highly recommended to start the application of the CPRM with a very low-intensity prefilter or initial screen (as is consistent with ISO 31000, COSO/ ERM, and others).

The Overall Counterfeit Rank is comprised of five factors which, themselves, are comprised of several sub-factors. For example:

- Overall risk rank
  - Factor 5.0: Market profile
    - Sub-factors:
      - 5.1 Contract Manufacturing
      - 5.2 Single Distributors Per Country
      - 5.2 Refurbished or Remanufacturing market

An example of the sub-factor assessment is included (Fig. 4.11). This figure presented three sub-factors that feed into one factor that eventually is considered for the overall risk rank.

(continued)

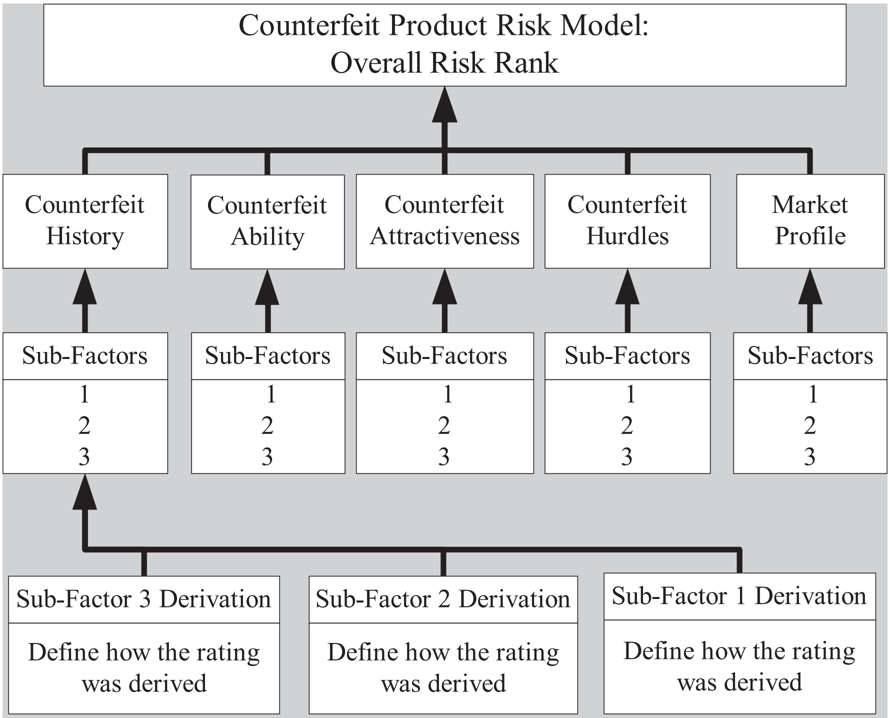
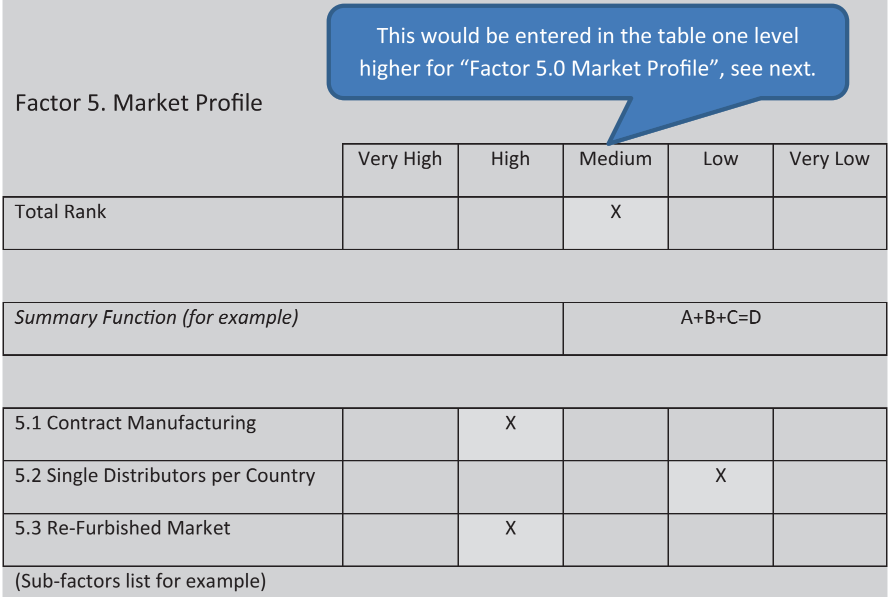


Fig. 4.10 Counterfeit product risk model overview (Copyright Permission Granted)



Factor 5. Market Profile

This would be entered in the table one level higher for "Factor 5.0 Market Profile", see next.

	Very High	High	Medium	Low	Very Low
Total Rank			X		

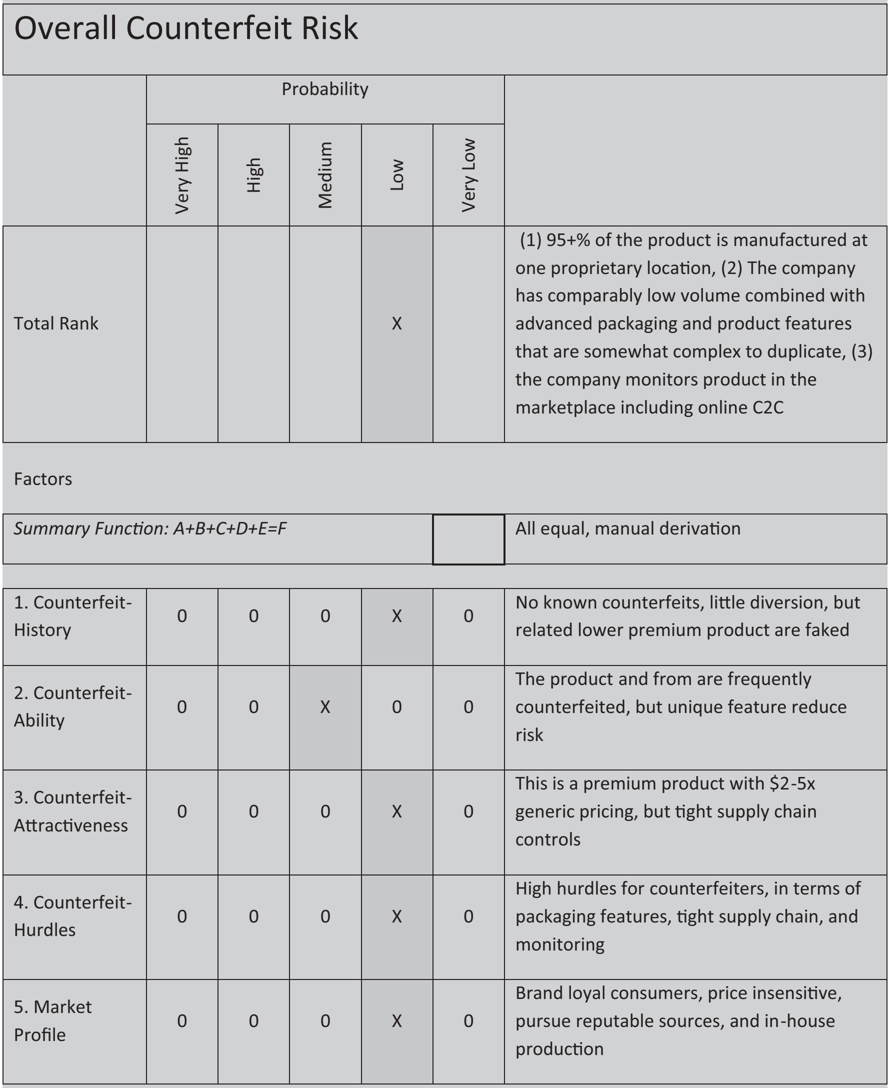
Summary Function (for example)	A+B+C=D

5.1 Contract Manufacturing		X			
5.2 Single Distributors per Country				X	
5.3 Re-Furbished Market		X			

(Sub-factors list for example)

Fig. 4.11 Example of the sub-factor derivation of the market profile factor (Copyright Permission Granted)

The assessment of the five factors is combined in a summary report which is provided with information from a case study (Fig. 4.12). The summary report provides a simple way to present the findings while also including much deeper insight into the factors and sub-factors. Also, the summary report includes comments so a risk assessor can understand some of the reasons for the conclusion.



Overall Counterfeit Risk

	Probability					
	Very High	High	Medium	Low	Very Low	
Total Rank				X		(1) 95+% of the product is manufactured at one proprietary location, (2) The company has comparably low volume combined with advanced packaging and product features that are somewhat complex to duplicate, (3) the company monitors product in the marketplace including online C2C
Factors						
Summary Function: A+B+C+D+E=F						All equal, manual derivation
1. Counterfeit-History	0	0	0	X	0	No known counterfeits, little diversion, but related lower premium product are faked
2. Counterfeit-Ability	0	0	X	0	0	The product and from are frequently counterfeited, but unique feature reduce risk
3. Counterfeit-Attractiveness	0	0	0	X	0	This is a premium product with $2-5x generic pricing, but tight supply chain controls
4. Counterfeit-Hurdles	0	0	0	X	0	High hurdles for counterfeiters, in terms of packaging features, tight supply chain, and monitoring
5. Market Profile	0	0	0	X	0	Brand loyal consumers, price insensitive, pursue reputable sources, and in-house production

Fig. 4.12 Case study overall counterfeit risk (Copyright Permission Granted)

(continued)

From the report conclusion (emphasis added):

> Companies and agencies constantly struggle to quantify the magnitude of the counterfeit threat from both a global and a specific product perspective. Although there are many examples of the dangers of product counterfeiting, the nature of the counterfeiters and counterfeiting makes it difficult or even impossible to determine the quantitative, hard data on the risk. Specifically, analysis of the risk, risk model literature review, in combination with peer-consultation, established a foundation for the Counterfeit Product Risk Model (CPRM) and for the supporting non-quantitative analysis. It is *not* practical to conduct quantitative or classical statistical tool-based risk assessments for the counterfeit threat because the results *cannot* be theoretically validated. This research set out to break new ground by presenting an overview of the product counterfeiting threat as a starting point for the development of a practical, useful and publically available, Counterfeit Product Risk Model.
>
> This research used a very broad, very interdisciplinary perspective that led to important theoretical justifications, such as using a probability versus a severity matrix, qualitative ranking, and the language of enterprise risk management. Many current anti-counterfeit research projects are extensions of existing research (with a narrow focus that is not all-encompassing) or are so theoretical in nature that they are not applicable (e.g., very complex models that are not all-encompassing). This analysis and the development of the model provides a unique and practical approach in the implementation of anti-counterfeit strategies.
>
> This type of research analysis and model has not been presented previously by other researchers for several reasons:
>
> - the extremely interdisciplinary nature of the strategy;
> - the fact that the hard data is elusive or non-existent—current industry actions are usually confidential, and agency actions are usually classified;
> - broad, all-hazards risk assessment is still evolving; and
> - a risk-based approach to regulation and legislation is only beginning to be applied to risks that are very real but very qualitative and hard to evaluate.

Since addressing product counterfeiting is probably no more than 10%of any one academic discipline, it is not surprising that there is a lack of research focus and leadership in the area of anti-counterfeit strategy. Packaging is a logical starting point for this anti-counterfeit research since the most efficient anti-counterfeit actions are packaging components, but there are many other disciplines that are equally important in an anti-counterfeit strategy. Critical disciplines which should be considered in an all-encompassing, strategic perspective on deterring counterfeiting include criminal justice, supply chain, risk management, social anthropology, consumer behavior, health risk communication, retailing, intellectual property rights law, food law, healthcare (medicine, nursing, etc.), public health, political science, international trade relations, and many more.

From the further research section:

> The very nature of developing propositions for this research established a base for future research and model refinement. The logical next step is to use the model to gain insights, refine usability, and to present procedures for practical implementation.

> As the model is used in practice, more detailed risk-based and classical statistical tools could be used to better support anti-counterfeit strategy decisions. Valuable insights could be gained from running the model for various industries and by conducting reviews of inter-industry best practices.

This next table builds upon the future research section with additional comments from 2019 (Table 4.2).

The early assessments considered one part of the overall question or focused only on specific product groups. Over the 10 years since the publication of the CPRM, there has been an implementation of compliance requirements that dictate an overall, holistic, and all-encompassing approach. Once the overall assessments are conducted, there is an identification of further, more detailed assessments which could expand to include the CPRM and others.

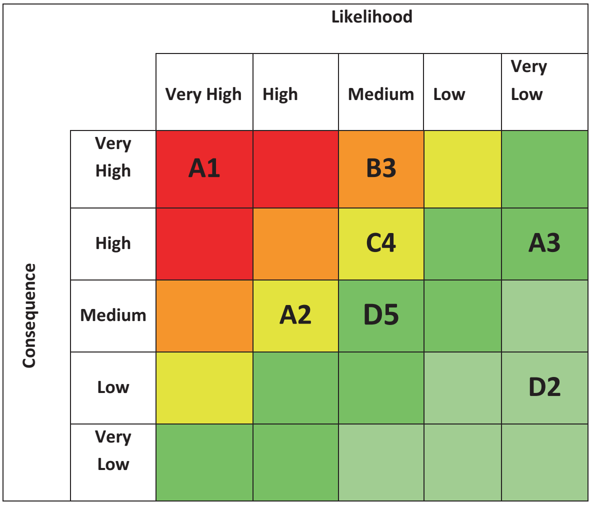
Table 4.2 Future research recommendation and result 10 years later

Commentary on the 2009 future research recommendations and the application over 10 years	
1. The logical next step is to use the model to gain insights, to refine usability, and to present procedures for practical implementation	*Yes*. This was a resource for new works such as the Food Fraud Initial Screening Tool and others
2. As the model is used in practice, more detailed risk-based and classical statistical tools could be used to better support anti-counterfeit strategy decisions	Somewhat. In 2017–2019 the Food Fraud Vulnerability Assessments are just beginning to be conducted and currently with a prefilter/initial screening approach. Also, the available data has not been through enough for high-level statistical analysis
3. Valuable insights could be gained from running the model for various industries and by conducting reviews of inter-industry best practices	Yes. The modification to the needs of the food industry compliance requirements has let to model development and a common approach that enables the sharing of best practices
4. Any future research should be combined with the evolving Enterprise Risk Management practice and with case studies to both understand and support how financial anti-counterfeit strategic decisions are being made within companies and agencies	*Yes*. There have been numerous food industry research projects and publications that expand to consider the enterprise-wide resource-allocation decision and specifically the COSO/ERM resources
5. Another important – probably the epicenter of all future anti-counterfeit strategy research – is exploring the behavioral aspects of 'the chemistry of the crime' and 'the chemistry of consumer consumption	*Yes*. Criminology—and specifically Situational Crime Prevention—has become a common topic in food fraud research and in the application
6. Finally, there should be an ongoing review of both the basic propositions and the model, itself, with refinements implemented as necessary	No. There has *not* been any further review or application of the CPRM. In 2012, part of the MSU research shifted from an all-products intellectual property rights infringement enforcement to food fraud and prevention. As the compliance requirements define a simple, basic starting point, further methods are now needed which could include the CPRM

Role of ERM in Decision-Making: Corporate Risk Map

The two critical parts of the FFPC is the "fraud opportunity" and the "risk appetite." The current or projected vulnerability is presented on a "corporate risk map" (Fig. 4.13) and then two examples in Figs. 4.14 and 4.15. The application of ERM is that when there is new information, the fraud opportunity is reassessed, and then the new vulnerability is plotted on the corporate risk map. A very quick review of "acceptable/unacceptable" can be conducted by plotting the new vulnerability.

While the first incidents will need to have a case-by-case review by the entire food fraud team, over time, there will be standard operating procedures and thresholds. Consider how other incidents are managed. If there is a transportation problem and regular customer deliveries may miss deadlines, then in some cases, expedited more expensive transportation may be approved. The first time this would need to



Consequence	Likelihood: Very High	High	Medium	Low	Very Low
Very High	A1		B3		
High			C4		A3
Medium		A2	D5		
Low					D2
Very Low					

Fig. 4.13 Corporate risk map plotting food fraud initial screening risk assessments (Copyright Permission Granted) (Spink et al. 2016)

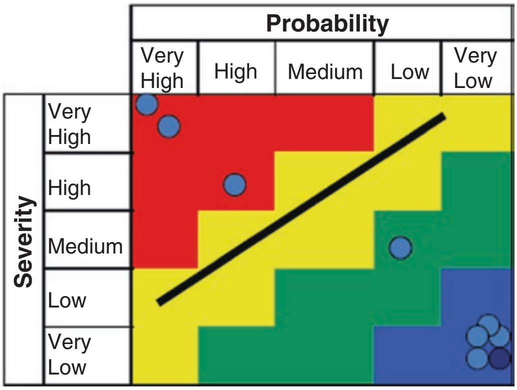


Fig. 4.14 Example of a risk map with a range of risks or vulnerabilities above and below the risk threshold (this could be a raw material and product categories or specific stock keeping units) (Copyright Permission Granted) (MSU-FFI 2017)

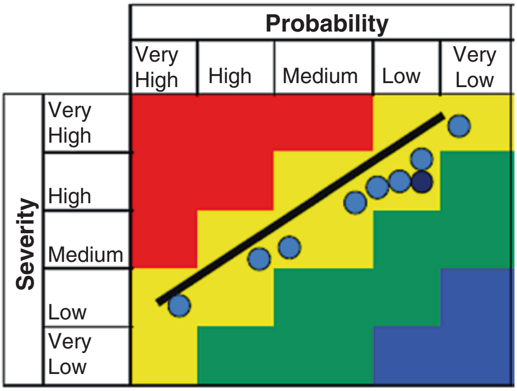


Fig. 4.15 Example of a risk map with a range of risks or vulnerabilities managed to just below the risk threshold (Copyright Permission Granted) (MSU-FFI 2017)

Table 4.3 Details of shifting vulnerabilities that are plotted on the corporate risk map example

Actions	Detail	Decision	Result
A to B	Reduce Food Fraud Prevention budget by $1 M	No	The change is defined to be an unacceptable option since the enterprise-wide vulnerability shift to an unacceptable situation above the risk tolerance
C to D	A lot less of "Action 1"	Yes	Even though there is a reduction in activity, the resulting situation is still within the risk tolerance
E to F	More of "Test 3"	Yes	Conducting more of this activity reduces the vulnerability to below the risk threshold

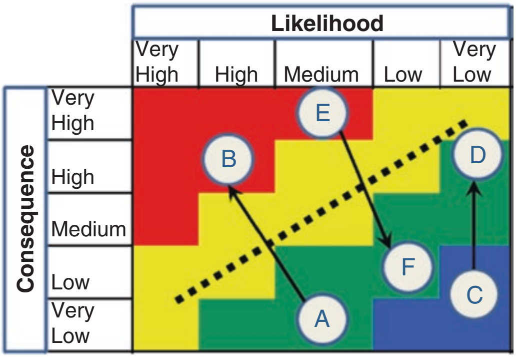


Fig. 4.16 Risk map presenting the shifting vulnerabilities from the examples

be discussed and debated with the resource-allocation decision-maker. Over time it might become clear that every time customer "X" missed a shipping or receiving deadline due to bad weather that the CFO approves rush delivery up to $1000.

To further demonstrate the use of an ERM/COSO risk map for resource-allocation decision-making, several other scenarios are presented here (Table 4.3 and Fig. 4.16).

The scenarios are plotted on a corporate risk map to provide a visual of all the shifting vulnerabilities and clear presentation of which are above the risk tolerance.

These scenarios included a very challenging question of basic financial allocation applied to a group such as a food fraud team or a food safety department. The corporate risk map can be used to at least start this type of discussion of “how much is enough” which is based on exactly what is—or then isn’t—being done. The “we need ‘more’” and “the business will be too risky” are subjective statements that cannot be compared to other vulnerabilities or risks. Once the reduction of funding is presented on a chart like this (the current financial allocation is at “Point A” which keeps the business under the risk tolerance, while reducing the budget by $1 million will raise the company to “Point B” and above the risk tolerance). Someone has to tell you “no, we don’t believe the business will be in a too risky position.” If there is an incident, there will be documentation of who reduced that budget. It won’t be you.

The use of ERM/COSO and the corporate risk map synthesizes all—literally *all*—risks across an enterprise. The corporate risk map provides clarity on the risk. Full integration of the vulnerability into ERM and the corporate risk map correlates and automates the process.

“How to Start” and “How Much Is Enough”?: “The Corkscrew Approach”

Now that the system has been presented and the sections reviewed in detail, there is a need to discuss how to start. While the very detailed implementation methods will be covered in a later chapter, at this point, it is important to present the overall concepts. The “corkscrew approach” is to start very high level but to make sure to fully complete the process. The first step is a very high-level review of the entire system including a brief recommendation of next steps. In some instances, the resource-allocation decision-maker will have enough information for the decision at hand. If not then the resource-allocation decision-maker will be able to explain exactly what they need in the way of more information. If a full system review is conducted, there can be “management by exception”; meaning they can define exactly what they like, don’t like, and what is needed next.

The next turn of the corkscrew will be more in depth. The process will advance only as far as the resource-allocation decision-maker defines value. The question of “How much is enough?” is defined by this process.

Conclusion

This second food fraud prevention chapter expanded on the interdisciplinary approach and began to frame the question as the needs for a vulnerability assessment, and prevention strategy was being envisioned. ***The first conclusion is*** that there are already a wide range of activities conducted by an industry or company that already contributes to reducing the fraud opportunity. It is important to search across a wide range of business activities to find information and data that is already being gathered. ***The second conclusion is*** that there should be an assumption that there *are* very competent and thorough current standard operating procedures that could immediately apply. Also, while understanding there are thorough and robust systems, they probably will not completely apply to food fraud prevention. ***The final conclusion is*** that while a food fraud is a food issue that is usually managed by food agencies that often require food authenticity tests, the selection of countermeasures and control systems may focus on many disciplines *except* the food sciences. The most important activity is often the most foreign or abstract which is plotting the food fraud risk on a risk map that compares this incident to all other incidents across the enterprise. There is a saying:

> ***When addressing food fraud prevention, assume it is twice as complex as you think it is and you know half as much as you think you know…and you'll usually be just about right.***

Appendix: WIIFM Chapter on Prevention Approach

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	Enterprise Risk Management insights can be adopted into frontline processes and which will create dynamic methods that will address "how much is enough?"
Quality team	This food fraud prevention approach is an enterprise risk assessment linked process that will help you assess a new risk in relation to all other corporate-wide risks which will enable direct, methodical resource-allocation decision-making for "how much is enough."
Auditors	This is more of an introduction to the strategically sound fundamentals behind the process.
Management	While this may seem very theoretical, it will end up being a very practical and directly applicable process to support very logical and obvious resource-allocation decision-making.
Corp. decision-makers	This may seem like an impossible task, but it works and allows frontline employees to use the enterprise-wide risk tolerance insight for decision-making (without revealing any commercially sensitive or expose and confidential risk assessments).

Appendix: Study Questions

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

1. Discussion Question:
   (a) What is the foundation of the FFFPC?
   (b) What are academic disciplines that are utilized by the FFPC?
   (c) For FF prevention, "how much is enough?"
2. Key Learning Objective1
   (a) What is the "Food Fraud Prevention Cycle (FFPC)"?
   (b) What is the central focus or driver of the FFPC?
   (c) How is a new countermeasure or control system technology reviewed in the FFPC?
3. Key Learning Objective2:
   (a) What is an "Integrated Framework"?
   (b) What is the authority and origin of the "Internal Controls/Integrated Framework" concept?
   (c) How are the Integrated Framework and Internal Controls connected and calibrated?
4. Key Learning Objective3:
   (a) What are the process steps in the FFPC?
   (b) Where does "New Information" (such as the awareness of a new industry incident) enter the FFPC?
   (c) Where does the FFPC start?

References

Banaji, M. R., Bazerman, M. H., & Chugh, D. (2003). How (un) ethical are you? *Harvard Business Review, 81*, 56–65.

Bazerman, M. H., & Chugh, D. (2006). Decisions without blinders. *Harvard Business Review, 84*(1), 88.

Bazerman, M. H., & Neale, M. A. (1993). *Negotiating rationally*. Simon and Schuster, New York.

Bazerman, M. H., Loewenstein, G., & Moore, D. A. (2002). Why good accountants do bad audits. *Harvard Business Review, 80*(11), 96–103.

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.

COSO, Committee of Sponsoring Organizations of the Treadway Commission. (2016). *Fraud risk management guide*. Washington, DC: COSO Publication, URL: https://www.coso.org/Documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf

COSO, Committee of the Sponsoring Organizations of the Treadway Commission. (2013). Internal controls – integrated framework, URL: http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

FBI, Federal Bureau of Investigation. (2012, Not Defined). Organized crime, glossary of terms. Retrieved January 30, 2012, from https://www.fbi.gov/investigate/organized-crime/glossary

GMA, Grocery Manufacturer's Association. (2014). Brand protection and supply chain integrity: Methods for counterfeit detection, prevention and deterrence – a best practices guide, Published by: FMI/GMA Trading Partner Alliance, Prepared by: Inmar and Authentix, URL: https://www.gmaonline.org/file-manager/Collaborating_with_Retailers/GMA_Inmar_Brand_Protection.pdf. Accessed 14 Dec 2017.

IPR Center. (2011). National Intellectual Property Rights Center, *Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad*.

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

ISO, International Standards Organization. (2011). ISO 12931 – performance criteria for authentication solutions for anti-counterfeiting in the field of material goods. 2012, from http://www.iso.org/iso/catalogue_detail.htm?csnumber=52210

Lam, J. K., & Spink, J. (2018). Developing a preliminary model to identify food fraud within the meat industry, Food Fraud Initiative report, May 25, 2018, Michigan State University, www.FoodFraud.msu.edu

MSU FFI, Michigan State University Food Fraud Initiative. (2017). The role of Enterprise Risk Management in food fraud prevention, MSU Food Fraud Initiative Report (FFIR), funded by an anonymous donor, URL: http://foodfraud.msu.edu/wp-content/uploads/2017/03/FFI-Backgrounder-the-role-of-ERM-in-Food-Fraud-prevention-v50.pdf, URL Video: https://youtu.be/Cg8T9C8nURs

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/

MSU-FFI, Michigan State University's Food Fraud Initiative. (2017). Applying Enterprise Risk Management to food fraud prevention – workings of ROI vs. Vulnerability, Risk to Vulnerability, and then a case study example of a complex Food Fraud management system (ERM2), MSU Food Fraud Initiative Report (FFIR), Funded by the Kerry Group's Global Supply Quality team's program, August 2017, URL: http://foodfraud.msu.edu/wp-content/uploads/2017/09/BKGFF17-FFI-Backgrounder-ERM-ERM2-v46.pdf, URL Video: https://youtu.be/DVl_k-7_NEw

PWC, PriceWaterhouseCoopers. (2014). Present and function: Fine-tuning your ICFR using the COSO Update [Internal Control over Financial Reporting], URL: http://www.pwc.com/us/en/risk-assurance-services/forms/icfr-coso-framework-download.html

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

Spink, J. (2012). Chapter 9: Overview of the selection of strategic authentication and tracing programs. In A. I. Wertheimer & P. G. Park (Eds.), *Identification and analysis of counterfeit and sub-standard pharmaceuticals*. London: ILM Publications, a Division of International Labmate Limited. 1: 154.

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. (2015a). Food risk continuum, food fraud overview MOOC (Massive Open Online Course), MSU Food Fraud Initiative MSU-FFI, May 19 & 26, 2015.

Spink, J. (2015b). Product fraud and product counterfeiting as a source of terrorist financing. *Security Journal, 30*(2), 640–645.

Spink, J. (2019a). Food fraud and adulteration: Where we stand today. In R. Stadler (Ed.), *Encyclopedia of food chemistry*, *Section 6: Food adulteration and contamination*. New York, Book ISBN: 9780128140260, [Published: 16th November 2018].

Spink, J. (2019b). Food fraud prevention – selecting the right test, method, and sampling plan. In M. Burns, L. Foster, & M. Walker (Eds.), *DNA techniques to Verify food authenticity: Applications in food fraud, food chemistry, Function and analysis series*. Royal Society of Chemistry, ISBN 1788011783, 9781788011785.

Spink, J., Elliott, C. T., & Swoffer, K. P. (2013a). Defining food fraud prevention to align food science and technology resources. *Food Science & Technology, Journal of the Institute of Food Science and Technology, 27*(4), 39–42.

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

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

Spink, J., Elliott, C. T., Dean, M., & Speier-Pero, C. (2019). Fraud data collection needs survey. *NPJ Science of Food Journal (Nature), 3*, 8, [Accepted 00/00/2018].

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.