Chapter 6
Business Decision-Making and ERM/ COSO

Summary

This chapter presents the details of the business decision-making that is based on the managerial accounting regulatory requirements laid out in Enterprise Risk Management (ERM). ERM is based on accounting principles developed by COSO (the Committee for the Sponsoring Organizations of the Treadway Commission that, itself, was created to add internal control requirements such as for the Sarbanes-Oxley Act of 2002). The overall resource-allocation decision-making is addressed under an enterprise-wide system such as the formal concept of "Enterprise Risk Management."

The Key Learning Objectives of this chapter are:

- ***'(1) Introduction to Enterprise Risk Management***: Introduce the concept of an enterprise-wide risk assessment method that "compares everything to everything." This allows an evaluation of this new risk in relation to all other risks and also to determine whether specifically above-defined "risk tolerance."
- ***'(2) Applying ERM to Food Fraud Prevention:*** Then there are steps to apply the enterprise-wide methods specifically to a Food Fraud Vulnerability Assessment and to incorporate in a Food Fraud Prevention Strategy.
- ***'(3) Implementing an Iterative Process:*** Finally, there are methods and procedures to implement an iterative process that continually evolves and innovates to more efficiently and effectively balance the evolving fraud opportunity in relation to the enterprise-specific risk tolerance.

On the Food Fraud Prevention Cycle (FFPC), this chapter addresses the "(3) Vulnerability Assessments," with "(4) Risk Rank" that is determined by the "(5) Enterprise-Wide Risk Assessment" (Fig. 6.1).

© Springer Science+Business Media, LLC, part of Springer Nature 2019

J. W. Spink, *Food Fraud Prevention*, Food Microbiology and Food Safety,
https://doi.org/10.1007/978-1-4939-9621-6_6

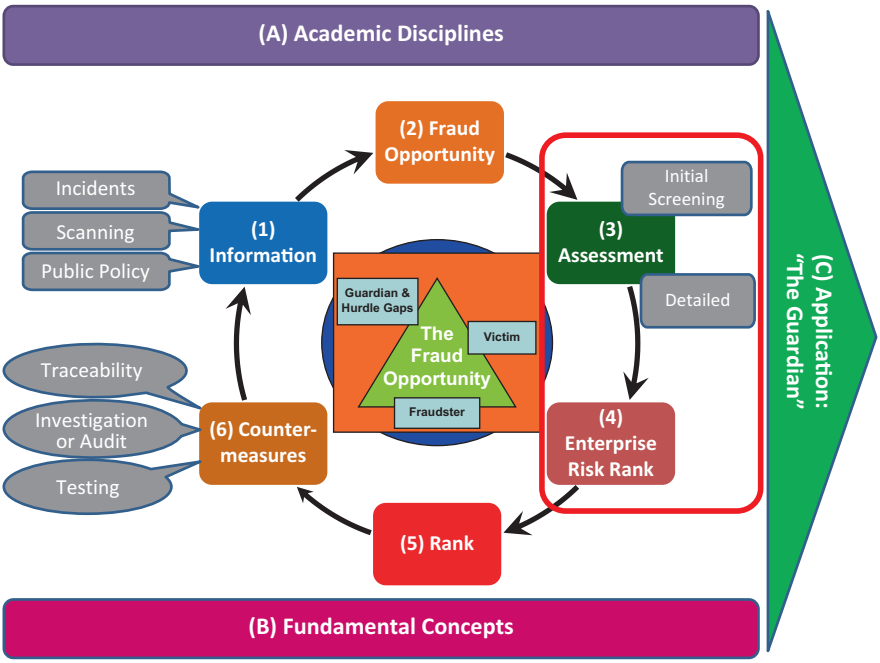


Fig. 6.1 Where this chapter applies Food Fraud Prevention Cycle—where this chapter applies to the overall concept: "(3) assessments" and "(4) enterprise risk rank." (Copyright Permission Granted) (Spink 2014; Spink et al. 2019)

Introduction

Overall, businesses are financial entities judged by financial metrics. While the main focus of a food company is obviously on the food, ultimately they are a business. The first level of regulation and controls are on business functions. There are specific and unique requirements for financial reporting. One of those requirements is for internal controls to manage and report risks.

Companies produce a product and sell into the markets. Some additional regulations and controls focus on those details. Product-specific regulations would include the US Food Safety Modernization Act (FSMA) and the US Food, Drug, and Cosmetics Act (FDCA). Market- or trade-related specific regulations would include import and export laws such as from the World Trade Organization (WTO), the World Customs Organization (WCO), or the likes of the US Customs-Trade Partnership Against Terrorism (C-TPAT).

Without this calibration at best you are relying on "someone else" to figure it out—and no one probably knows the problem better than you. The basic concepts are not private or confidential. These are common business practices that are taught in undergraduate university courses.

Legal Requirements and "Opportunities"

Beyond the legal requirements, there are certifications or standards compliance to consider. For food safety, an example is the Food Safety Management System in the Global Food Safety Initiative (GFSI) Guidance Document. While there are specific regulatory requirements for financial reporting, there are programs managed by an organization such as COSO (Committee of the Sponsoring Organizations of the Treadway Commission) who created Enterprise Risk Management (ERM) to address US Sarbanes-Oxley Act requirements specifically.

Companies are instructed to implicitly or explicitly create these monitoring systems by their stakeholders (e.g., owners would include shareholders who put in place a Board of Directors to oversee the corporate-level officers). While finance and securities laws regulate public companies, even private owners (e.g., individuals, private equity firms, etc.) would also require some oversight and reporting mechanism. Investors don't just give a billion dollars to a company and hope for the best—"good luck and see you in a year." Ultimately all resource-allocation decision-making are accountable by the Board of Directors. Whether the frontline "business case" is in the same format or not, there is a central decision. Usually, there is a conversion of ERM concepts into everyday metrics—you might not be aware of your success measures integrated into the ERM system. There are two types of considerations to the decision with one being an increase in earnings (revenue) and the other is the cost of operation (operational costs and managing risk). From COSO [emphasis added]:

> **Opportunities:** the possibility that an event will occur and positively affect the achievement of objectives, supporting ***value creation*** [increase sales or profit] or ***preservation*** [reduce risks]. (COSO 2013)

A central enterprise-wide system is the control mechanism. For many companies that system is a formal Enterprise Risk Management system. This chapter will introduce business resource-allocation decision-making and how food fraud (and all food risks) would fit into an ERM system (Fig. 6.2).

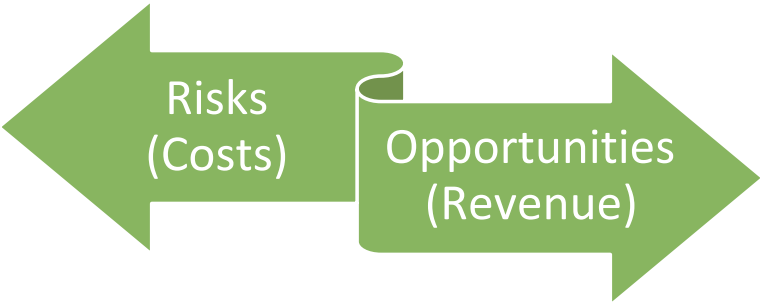


Fig. 6.2 Considerations for resource-allocation decision-making are a balance of increasing revenue and controlling costs

Key Learning Objective 1: Enterprise-Wide Risk Management System

This section reviews the enterprise-wide management systems that connect from the frontline tactical resource-allocation decisions to calibrate all the way up to the strategic assessment within the "risk appetite" of the owners of the company. Whether to meet regulatory compliance—or just competent business practices—these fully integrated mechanisms exist and are critical for a Food Fraud Prevention Strategy.

The section focuses on the basics of Enterprise Risk Management (ERM/COSO).

The Key Learning Objectives of this section are:

- (1) An overview of the legal, regulatory requirements for managerial accounting practices such as under the US Sarbanes-Oxley Act for Enterprise Risk Management (ERM/COSO).
- (2) Consider internal controls to harmonize the way separate business units assess, report, and manage risks.
- (3) Examine the integrated framework that connects and calibrates the separate internal control procedures.

COSO: Regulatory Compliance for Securities and Finance

Fortunately for Food Fraud Prevention, the enterprise-wide management structure concepts are already developed and include standards, training, certifications, and many case study examples. Whether formally published by COSO or in scholarly journals, there are many resources and examples. The key for Food Fraud Prevention is to leverage those processes to (1) use refined systems, (2) leverage current and already adopted regulatory training and certification, and (3) communicate clearly with financial group colleagues.

Regulatory compliance requires "a" process but not explicitly ERM/COSO. The requirement is an overall control system. It is important to explain the difference between "formal, full ERM regulatory compliance" and "ERM-like" systems. A full and formal ERM "compliance" can be extremely costly and resource intensive. This would cover all aspects of the corporation and all transactions. The system would include a comprehensive and formal audit of all internal controls and the integrated framework. An "ERM-like" system can apply the general principles. These general principles would integrate with any of the related systems.

From COSO (2013):

> ***Enterprise risk management*** is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
>
> The definition reflects certain fundamental concepts. Enterprise risk management is:

- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in [during] a strategy setting
- Applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board of directors
- Geared to the achievement of objectives in one or more separate but overlapping categories.

This enterprise risk management framework is geared to achieving an entity's objectives, set forth in four categories:

- Strategic – high-level goals, aligned with and supporting its mission
- Operations – effective and efficient use of its resources
- Reporting – reliability of reporting
- Compliance – compliance with applicable laws and regulations.

There has been a benefit to assessing Food Fraud Vulnerability within an enterprise-wide framework even if there is currently no formal connection or calibration to the corporate-level system was developed or connected. The foundation in regulations and standards provides confidence that the Food Fraud Prevention Strategy is compatible with, and is compliant with, enterprise-wide regulatory financial and security compliance requirements. For example, the food fraud incidents can be reviewed within a Food Fraud Vulnerability Assessment; the results of that assessment can be plotted on an unofficial corporate risk map. What is meant by "unofficial" is that—even without contact with chief executive officer, chief financial officer, chief risk officer (CEO/CFO/CRO), or enterprise risk team—the food risk assessors create what is believed to be the risk appetite in terms of very high to very low likelihood and consequence. By using the same system as the CEO/CFO/CRO teams, they can use the assessment. Even if the risk ranks are not correlated between the food fraud assessment and the enterprise-wide system, this is a baseline or starting point that can be adapted. For example, the food fraud measures of likelihood and consequence can be adapted and then vulnerability assessment re-calibrated. If done correctly and thoroughly, the Food Fraud Vulnerability Assessment can be directly used in the ERM assessment.

While this may seem very formal and require additional steps, there is usually no need for a food safety or food fraud manager to be formally certified or trained in full ERM regulatory compliance.

The COSO/ERM concept and components are presented in "the COSO Cube" (Fig. 6.3) (COSO 2013).

The components of the COSO Cube include (COSO 2013):

1. Internal Environment
2. Objective Setting
3. Event Identification (re, awareness of a food fraud incident, suspicious activity, or identified fraud opportunity)
4. Risk Assessment (re, Food Fraud Vulnerability Assessment)
5. Risk Response (re, Food Fraud Prevention Strategy)

6. Control Activities (re, countermeasures and control systems),
7. Information & Communication
8. Monitoring (Re, a control system to continuously evaluate the evolving fraud opportunity)

The COSO Cube presents "components of enterprise risk management" in eight interrelated management components. This COSO Cube is an effective tool to explain this simplicity of connecting a new Food Fraud Vulnerability Assessment into the enterprise-wide decision-making system. A new food fraud incident—or the first full Food Fraud Vulnerability Assessment—would enter at the star on the front of the cube in the "Event Identification" component.

> **Event Identification:** Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes. (COSO 2013)

Now that there is a specific component—or management function—to receive information on new "Event Identification," there is now an "accountable" person and also a way to structure the information so it can actually be assessed in relation to all other enterprise-wide risks. After "Event Identification" the next step would be "risk assessment" and then a "risk response" decision that integrates information to and from the other sides of the cube including the four categories of objectives (e.g., strategic, operations, reporting, and compliance) and entity unit (e.g., entity-level (enterprise-wide), division (or operating company), business unit, and subsidiary.

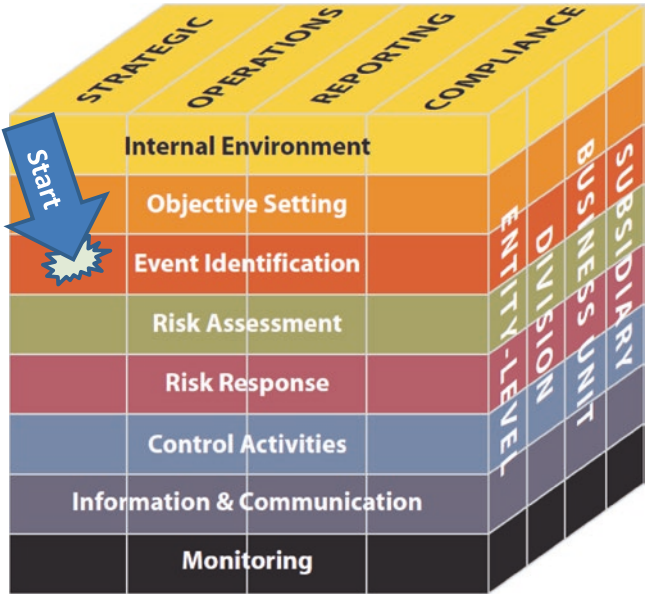


Fig. 6.3 "COSO Cube" representation of the organization of activities and work functions—the "start" point for a new concern at the "strategic" and "event identification" point. (Copyright Permission Pending) (COSO 2013)

Once the "enterprise-wide assessment" is added to the Food Fraud Prevention Cycle (FFPC), there is an actual decision-making system to evaluate "how much is enough."

Internal Controls: ERM and ERM-Like

In the USA, the major push for additional regulations occurred after incidents at Enron, WorldCom, and Parmalat. In these examples, investors were defrauded which led to bankruptcy costing losses of $62 billion ($700 million of overstated profits), $136 billion ($3.8 billion misappropriated), and $20 billion ($17.6 billion in hidden losses) (Oppel and Sorkinnov 2001; Romero and Atlas 2002; Boland 2008). Each company conducted fraudulent operations that circumvented the then current audit and control practices. The failures of these companies—among others—contributed to the worldwide financial meltdown of 2001. Each of those three corporations went bankrupt, and the implications even extended to the corporate auditor companies such as Arthur Anderson.

The US securities and finance regulations expanded "internal controls" and an "integrated framework" to increase transparency of transactions and accountability of the individual leaders and managers. The regulations were successful in the sense that company employees have been prosecuted and sent to federal prison. Even if there is no prison sentence, most CEO/CFOs would rather not be convicted felons.

It is important to note that even though the regulatory requirement only applies to public companies, private and non-US companies usually have implemented similar controls.

- ***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 relating to operations, reporting, and compliance" (COSO 2013).
- ***Integrated framework:*** "The original framework has gained broad acceptance and is widely used around the world. It is recognized as a leading framework for designing, implementing, and conducting internal control and assessing the effectiveness of internal control. […] The Framework will enable organizations to effectively and efficiently develop and maintain systems of internal control that can enhance the likelihood of achieving the entity's objectives and adapt to changes in the business and operating environments" (COSO 2013).

Other related COSO glossary terms are below (note the similarity and harmonization with ISO 31000 Risk Management):

- "***Inherent risk***—the risk to an entity in the absence of any action management might take to alter either the risk's likelihood or impact."
- "***Residual risk***—the remaining risk after management has taken action to alter the risk's likelihood or impact."

- "***Risk appetite***—the board-based amount of risk a company or another entity is willing to accept in pursuit of its mission (or a vision)."
- "***Risk tolerance***—the acceptable variation relative to the achievement of an objective."

Other related COSO concepts that demonstrate the application to Food Fraud Prevention include (COSO 2013):

- ***Enhancing risk response decisions:*** Is a risk tolerable? How do you know? Who would dare to let a risk remain in a business operation? ERM provides a way to measure and calibrate new or changing risks.
- ***Reducing operational surprises and losses:*** By creating a system to look at all current risks and potential vulnerabilities—and monitor changes—the enterprise works to move quickly. An example is that before the subprime lending crisis of 2007, several financial firms such as Goldman Sachs shifted out of investments that eventually crashed (Taleb 2007). With an ERM-type system, the vulnerabilities were evaluated to have increased above their "risk appetite."
- ***Identifying and managing multiple and cross-enterprise risks:*** Supporting the previous item, the enterprise-wide system helps evaluate a wide variety of risks and vulnerabilities within one system. For example, is it a better investment to hire two new salespeople or put in a metal detector at a plant? Without an enterprise-wide system, these two could not be quantitatively or analytically compared.
- ***Seizing opportunities:*** A company can become crippled if they feel they must address every risk. An ERM system helps evaluate the optimal amount of risk which frees up resources to pursue new or expanding revenue.
- ***Improving deployment of capital:*** Building on seizing opportunities, and outside the risk management, is creating a general mechanism to evaluate all financial and capital resource-allocation. New or different measures could be used such as value at risk (VaR) or return on capital employed (ROCE).

ERM/COSO is a critical part of Food Fraud Prevention Strategy since it provides a frame for assessing the risk, making decisions, integrating with other enterprise-wide systems, and organizing the activities.

ERM/COSO: Connect Everything to Everything

The ERM system provides internal controls and an integrated framework to increase transparency and accountability. The processes work to "connect everything to everything." Each step in the process reviews the other steps—horizontally across a function or vertically from the front line to the board.

It is important to note that even if/when ERM systems are in place, they may not be evident to everyone across the enterprise. We have several instances where we have heard "we don't do ERM." Then later—and sometimes later in the same meeting—someone says "yes we do, we just don't show you those charts!" The assess-

ment and judgment would be extremely commercially sensitive and actually not helpful for day-to-day decision-making for many organizations "as-is." Also, the overall ERM assessment would include a very broad range of risks. For example, a food safety group would not provide data or analysis of employee kidnapping threats, but that doesn't mean those risks are not real or important.

In reality, the board-level ERM assessments are comprised of a series of connected measures or activities. The overall ERM charts or questions are reduced to specific questions or data requirements from the specific operations or functions. Thus, the food safety group probably does provide quarterly statements about food safety risks, sometimes even with a requirement for the statement to be notarized. These statements feed upwards to a more formal ERM statement. The Sarbanes-Oxley Act requires a quarterly statement that is referred to as the 10-Q and an annual statement in 10-K.

The ERM system would include assessments and audits, and then the assessments and audits, themselves, would occasionally be audited.

The bottom line for the Board of Directors or CEO is that (1) a monitoring process is in place, and (2) the process is competently implemented adapted. A formal Food Fraud Prevention Strategy is becoming required to meet that compliance goal.

Sidebar: Fraud in Fraud Assessments—Intentionally Over- or Underestimation

Reportedly the guru investor Warren Buffett said "don't ask a barber if you need a haircut." The barber has a vested interest in the outcome of the analysis. The authors of the *Freakonomics* books would refer to this as the "influence of incentives" (Levitt and Dubner 2014). The same is understood to be for fraud assessments. This is often hard to even comprehend since most people think they make rational, fact-based decisions, without emotion or bias (see sidebar on "How (Un) Ethical Are you?").

- **Overestimate Fraud Opportunity:** A manager who is trying to get promoted or grow their group has an incentive or personal benefit to overestimate the fraud opportunity. A higher fraud opportunity would lead to more high-profile projects, bigger budget, and more direct report employees to supervise.
- **Underestimate Fraud Opportunity:** A manager who is near retirement or not looking for more work may underestimate the fraud opportunity not to increase their work.

In both cases, the enterprise is at risk. In the first case, the enterprise overinvests in prevention and has fewer funds to pursue new markets or products—sacrificing revenue-generating opportunities. In the second case, the enterprise is exposed to strategic risks.

The internal framework concept includes an awareness of this inherent conflict and puts processes in place to calibrate the risk assessments. Essentially the internal controls look for fraud in fraud assessments.

Sidebar: Detail of an ERM/COSO Corporate Risk Map that Is Expanded to Include Both Risks and Opportunities

From COSO publications, the range of risks are presented on a "Combined Risk and Opportunity Map" where (Fig. 6.4) (COSO 2012). They state "This allows a direct comparison of the highest rated opportunities and risks for consideration and prioritization" (COSO 2012). Essentially, the costs of reducing risks are balanced with investments that increase revenue. It is important to note that the optimal risk level is not "zero risk." There is an important balance between managing operational risk and investing in the business.

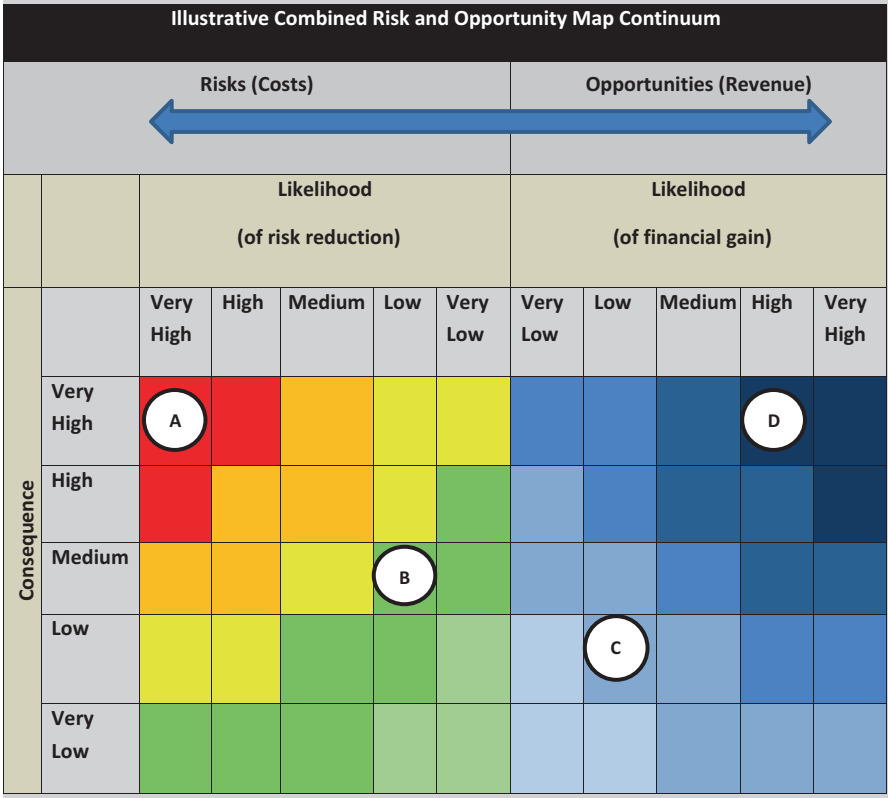


Fig. 6.4 ERM/COSO Combined Risk and Opportunity Map with examples. Note: The risks above the "risk tolerance" (the general range in red and orange such as point "A") are either reduced or managed (to at least the point "B"). The investments that reduce the risks are balanced with the opportunities to increase revenue or profit margin. The revenue-generating opportunities include a range from low confidence/low benefit ("C") to high confidence/high benefit ("D"). (Copyright Permission Granted from Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission) (Base adapted from COSO (2012) and examples are new)

These ERM/COSO principles and practices help create a foundation for resource-allocation decision-making. Once these are understood and implemented, then the next Food Fraud Vulnerability Assessment results can be plotted and determine what are "acceptable" what are "unacceptable." Without this type of method to "connect everything to everything," then "how much is enough" is a guess and does not have a measure of success. The Combined Risk and Opportunity Map is important to understand the process for resource-allocation decision-making. When this is better understood by the risk assessors and risk managers, then more efficient and effective countermeasures and control systems can be proposed and selected.

Sidebar: "How Much Is Enough?" and Optimal Risk-Taking

"How much is enough" is often a type of threshold that is calculated within a managerial accounting standardized system such as by COSO in their Enterprise Risk Management (ERM/COSO) (COSO 2012). COSO explains that there is a "sweet spot" of "optimal risk-taking" (Fig. 6.5) (COSO 2012).

From COSO publications, the risks are plotted on a "risk map" or "heat map" (Fig. 6.6) (COSO 2012).

From COSO publications, the risks are plotted on a "risk map" or "heat map" (COSO 2012).

COSO then provides guidance on how to "assess risk":

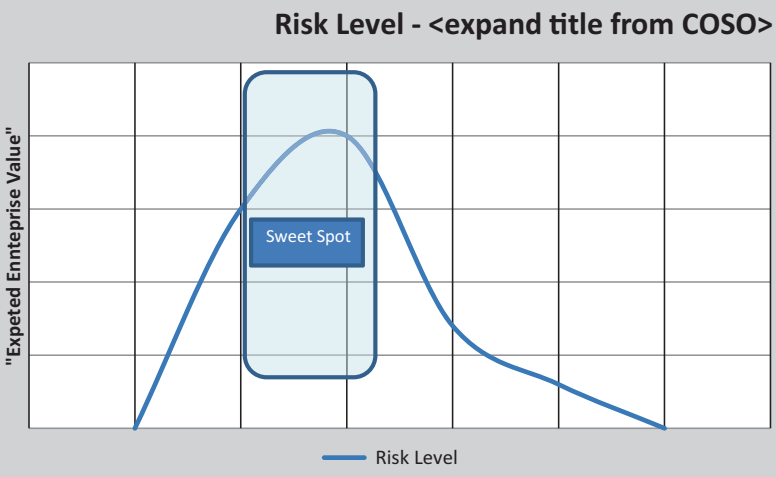


Fig. 6.5 An example of the "sweet spot" of the ideal risk tolerance for an enterprise—optimal risk-taking with the identification of the "sweet spot." (Copyright Permission Granted, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission) (Adapted from COSO (2012))

(continued)

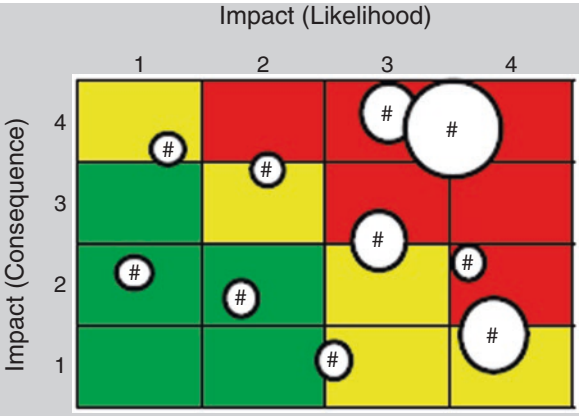


Fig. 6.6 Adapted from COSO, an "illustrative heat map" where the dots represent a risk and the size of the dots represent the speed of onset (Note: the term impact was adapted to the ISO 31000 terminology of consequence)

> Assessing risks consists of assigning values to each risk and opportunity using the defined criteria. This may be accomplished in two stages where an initial screening of the risks is performed using qualitative techniques followed by a more quantitative analysis [detailed assessment] of the most important risks. (COSO 2012)

Thus, the decision of "how much is enough" of a risk treatment is supported by ERM/COSO identification of a "sweet spot" of "optimal risk-taking" and supported by a presentation on a corporate risk map.

Sidebar: The Influence of Michael Porter and Corporate Strategy

Michael Porter is considered the "father of corporate strategy." His major work that summarized the overall "Competitive Strategy" was published in 1984 (this is covered in more detail in the other chapter on Market and Competitors) (Porter 1980). This work creates an overall theory to consider markets, how companies position products and services, as well as how companies manage or monitor the changing internal and external landscape. His follow-up book "Competitive Advantage" provides more focus on implementing the concept to achieve success (Porter 1985).

Key concepts from Porter that support the Food Fraud Prevention Strategy include:

- Identify the business functions.
- Measure and calibrate risks and rewards.
- Provide an overall perspective on optimizing decision-making.

Overall, there is an advantage—a strategic advantage as well as efficiency—of considering "fraudsters" or "counterfeiters" as a competitor. The fraudsters generally make business decisions based on macro (global-level trends) or micro (local or individual attributes) factors that are essentially corporate strategic decision-making. Essentially, the bad guys use the same decision-making theory as the good guys.

It is also a strategic decision to mention Porter's theories since he was a guru from the mid-1980s to the end of 1990s. He influenced a lot of business

academic thinkers and students. The age of those students would now be in their mid-50s to mid-60s and who are probably leading your companies or agencies. Since those resource-allocation decision-makers will recognize the terminology and theories of Michael Porter, his concepts are an important anchor for explaining the food fraud problem.

Sidebar: Information Requirement of How Much Is Enough?
Regarding how much information to gather and how to present the assessment, an important question is "how much is enough"? The answer is as much—or little—as the resource-allocation decision-maker needs to make a decision. In some cases, they may have enough information to make a decision then; obviously, no further assessment is needed. Sometimes a simple review or story can lead to an instant decision. Since a resource-allocation decision often needs more information, to provide more structure to the process, there is usually a need for a more systematic review of the proposal.

There were two major theoretical new breakthroughs for Food Fraud Prevention that frame the question by examining (1) the root cause (2) the decision-making process, which will then define the (3) risk treatment needed.

To address this need and the first step in understanding the root cause, a first Food Fraud Prevention innovation was to expand from food science to apply the Criminology theory of Situational Crime Prevention. The second innovation was to apply managerial accounting and decision sciences to understand the process to determine "how much is enough." Finally, after an understanding of the root cause and an awareness of the decision-making process, the countermeasure and control system risk treatments can be considered. To not, a countermeasure or control system could be food authenticity testing, market monitoring, enhanced traceability, stronger supplier agreements, expanded investigation and enforcement, and others.

For a wide range of industries, this "last" step of selecting countermeasures and control systems was informal, at best, and frequently a random process that was a reaction to a single incident. For example, after a counterfeit incident or lawsuit, a company might figure they need to do "something," but they do not have a systematic way to identify "how much is enough?" Sometimes the decision might be made by the General Counsel to consider "how much do we need to do to not look bad?" In other instances, a certain budget amount may be allocated such as "spend no more than one million dollars." In both cases, there would not be a systematic approach. There is no systematic way to judge what level of effort would be "enough to not look bad," and there was also no real rationale as for why spending one million dollars (or whatever) was the optimal resource-allocation.

(continued)

When applying ERM, the problem is presented in a way that it can be systematically evaluated in relation to other enterprise-wide concerns. Basically, ERM helps assess this risk in relation to other risks.

In every—emphasis on "each and every time"—a new incident or problem is identified; it should be run through a systematic review that includes:

'(1) A review of the suspicious activity (such as using the Food Fraud Suspicious Activity Report method—FFSAR (Spink et al. 2019)
'(2) Conduct a vulnerability assessment.
'(3) Then plot the problem on the corporate risk map.

Until this review is conducted, it is not defined as to whether the problems are unacceptable or shifts to outside the risk tolerance.

Key Learning Objective 2: Applying Enterprise Risk Management to Food Fraud Risk

This section reviews the ERM concepts of risk appetite and a corporate risk map which creates a theoretical leap for Food Fraud Prevention Strategy (FFPS). Before including these concepts, the assessments were stand-alone, not comparable to other risks, and that led to decisions that usually either stalled or way over- or underinvested.

The Key Learning Objectives of this section are:

- (1) Introduce the concept of risk appetite as a measure of a threshold.
- (2) Consider the two-stage process for the ERM assessment approach of first an initial screening and then a detailed assessment when needed.
- (3) Review these concepts in relation to business economic crimes.

Risk Appetite and Corporate Risk Map

An overarching objective of ERM/COSO is to create an internal framework to consider all risks across the entire enterprise. The goal is to seek and monitor even the most unlikely or unknown threats to the business. The overall ERM activity requires a center point to support decision-making to "connect everything to everything." Each resource-allocation decision is evaluated with every other decision in relation to the financial goals—the financial goals include a "risk appetite" defined by the owners through their proxy, the Board of Directors. To note, the "owners" could be individuals who own mutual funds or individual stocks in their retirement accounts—those individuals expect a consistent rate of return and level of risk that they expect the Board of Directors to assure. The ERM system evaluates these risks on a "corporate risk map."

While the exact single "corporate risk map" may not exist—or be so commercially sensitive that it is considered extremely confidential and made public or distributed widely—this is an effective way to present a novel risk such as food fraud.

The most important result of implementing enterprise-wide risk management is defining the "risk appetite" and presenting the risks on a "corporate risk map" (COSO 2013). Enterprise Risk Management (ERM) is a process to assist resource-allocation decision-making "…designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (MSU-FFI 2017).

Traditional food safety risk assessors often do not realize that many of the "limits" are actually a qualitative judgment of a vulnerability-defined point. While there may be a quantitative measure, the determination of that limit may have been more arbitrary. There were defined limits for food safety such as (1) the legal 5-log reduction or (2) scientifically based appropriate level of protection (ALOP) or appropriate level of sanitary protection (ALOSP) (WTO 1995; CODEX 2003) or a defined food safety objective (FSO) (Buchanan 2007, 2016). For example, the US FDA Juice HACCP guidance requires a 5-log kill step (evidence that there is a manufacturing step that reduces the prevalence of pathogens by five orders of magnitudes). Why exactly is 5-log required? Is a 4.9-log reduction 100% lethal, and 5.1-log is 100% safe? Why not decide on a 4-log or 6-log requirement?

Sidebar: Introduction to Food Risk Assessments

This is an excerpt from the report "Applying Enterprise Risk Management to Food Fraud Prevention" (MSU-FFI 2017).

It is essential to review the concept of "risk" and an "optimal level" that is referred to as "risk tolerance" or "risk threshold." Many Food Scientists and food safety managers use the term "risk" to define a point of the unacceptable or intolerable level. In Codex Alimentarius (CODEX) this is defined as an "Appropriate Level Of Protection" or ALOP. More broadly – including by statisticians, data scientists, and business decision-makers – risks are not all bad; it is usually inefficient or impractical to eliminate all risks. A company or agency that is operating with too-little risk is usually inefficient in meeting the overall objectives set by its stakeholders. There are situations of "insufficient risk-taking" that are the opposite of "excessive risk-taking." To use US FDA terminology, there are "hazards," and only some of those are "hazards that require a preventive control." From COSO:

> **The Risk Assessment Process:** Within the COSO ERM framework, risk assessment follows event identification and precedes risk response. Its purpose is to assess how big the risks are, both individually and collectively, in order to focus management's attention on the most important threats and opportunities and to lay the groundwork for risk response. Risk assessment is all about measuring and prioritizing risks so that risk levels are managed within defined tolerance thresholds without being over-controlled or forgoing desirable opportunities. (COSO 2012)

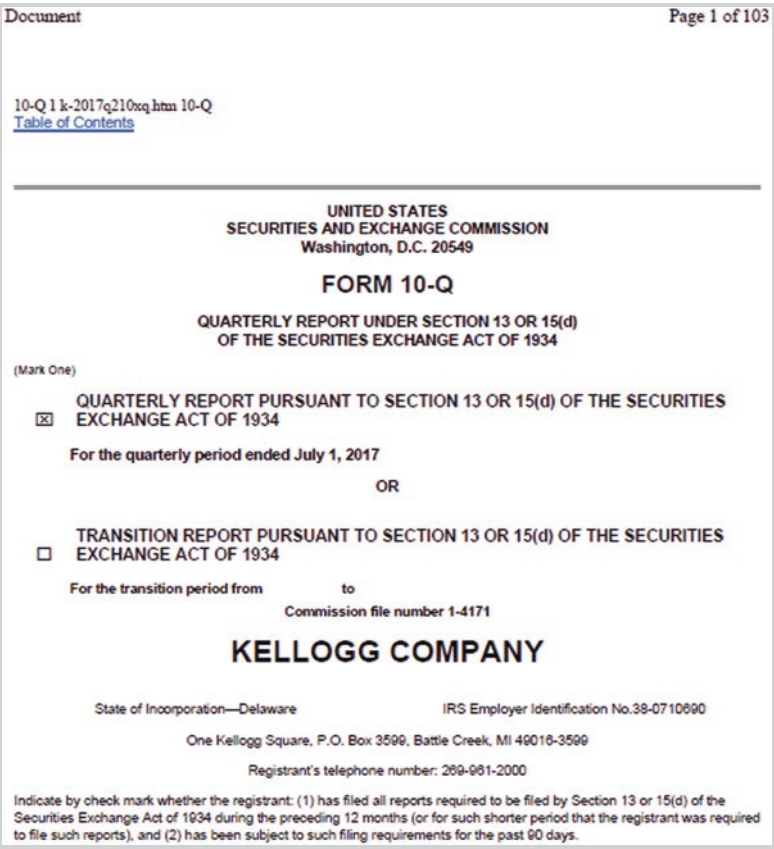
(continued)

In this COSO report "risk" is used as a negative or positive uncertain outcome which is different from the traditional food safety concept of an "unacceptable risk" or a "hazard that requires a preventive control." This ALOP threshold could be referred to as an "optimal" level of risk. Several important points are:

- Not all vulnerabilities are risks
- Not all risks are hazards
- Not all hazards are the FSMA type "hazards that require a preventive control."

A risk is not always bad, or a negative result but uncontrolled risk-taking is unacceptable.

This excerpt provided insight on an introduction to risk assessments within the ERM/COSO principles.



Document Page 1 of 103

10-Q 1 k-2017q210xq.htm 10-Q
Table of Contents

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-Q

QUARTERLY REPORT UNDER SECTION 13 OR 15(d)
OF THE SECURITIES EXCHANGE ACT OF 1934

(Mark One)

☒ QUARTERLY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the quarterly period ended July 1, 2017

OR

☐ TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the transition period from to

Commission file number 1-4171

KELLOGG COMPANY

State of Incorporation—Delaware IRS Employer Identification No.38-0710690

One Kellogg Square, P.O. Box 3599, Battle Creek, MI 49016-3599

Registrant's telephone number: 269-961-2000

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days.

Fig. 6.7 Example of a quarterly submission 10-Q form (Kellogg Company 2017)

Sidebar: The Sarbanes-Oxley Personal Statements by the CEO and CFO

The legal, regulatory document required by the US Securities and Exchange Commission referred to as an annual submission is referred to as a "10-K form" and a quarterly submission which is a "10-Q form" (see Fig. 6.7) (MSU-FFI 2017) citing (Kellogg Company 2017). The submission includes personal signed statements by the CEO and CFO for both the 10-Q form and Sarbanes-Oxley compliance (see Figs. 6.7 and 6.8). They are legal and formal statements publically available that are the base for the required corporate "annual report to shareholders."

The Sarbanes-Oxley requirements are very explicit and, as the signed 10-K forms demonstrate, *very* personal. Your CEO and CFO are held accountable, and they, then, hold the businesses accountable. You might argue "that's not my job" or "I thought someone else was doing that," … however, that's not very convincing. If you are responsible for Food Fraud Prevention compliance, you are responsible for making sure your company addresses *all* types of fraud and for all products.

Exhibit Page 1 of 1

EX-32.1 4 k-2017q2ex321.htm EXHIBIT 32.1

Exhibit 32.1

SECTION 1350 CERTIFICATION

I, John A. Bryant, hereby certify, on the date hereof, pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that

(1) the Quarterly Report on Form 10-Q of Kellogg Company for the quarter ended July 1, 2017 (the "Report") fully complies with the requirements of Section 13(a) or 15(d) of the Securities Exchange Act of 1934; and

(2) the information contained in the Report fairly presents, in all material respects, the financial condition and results of operations of Kellogg Company.

/s/ John A. Bryant

Name: John A. Bryant

Title: Chairman and Chief Executive Officer

A signed copy of this original statement required by Section 906 has been provided to Kellogg Company and will be retained by Kellogg Company and furnished to the Securities and Exchange Commission or its staff on request.

Date: August 4, 2017

Fig. 6.8 Signed Sarbanes-Oxley compliance from the CEO (Kellogg Company 2017)

Assessments of ERM/COSO Initial Screening and Detailed Assessment

As mentioned, ERM is a thorough, precise, and formal method. The COSO principles are clearly defined and presented in many formal publications. These publications define a "two-stage process continuum from a quick, qualitative 'initial screening' which is '…followed by a more quantitative analysis of the most important risks' (COSO 2012). The goal of the initial screen, or pre-filter, is to produce a quick and simple assessment before additional detailed requirements are defined by the resource-allocation decision-maker. In many cases the initial screening may be enough for a decision – for the specific decision at hand, the resource-allocation decision-maker (e.g., CFO, CRO, CEO, etc. or their proxy) defined the required level of accuracy, precision, and certainty."

The continuum could be from one vulnerability assessment for the entire enterprise all the way to the other extreme of one for each supplier/product/manufacturing location (Fig. 6.9).

For even a moderately sized company, they could have 300 suppliers with an average of 10 products per supplier and possibly an average of 3 manufacturing plants for each product. The most detailed implementation in this company would result in conducting an impractical 9000 vulnerability assessments.

It is most efficient to address all types of food fraud at the same time and in the same system. The enterprise must address all of these risks. "All types of food fraud can result in enterprise-wide risks so an enterprise risk management system must cover all types of vulnerabilities. The model developed in this paper addresses the unmet need for the first stage referred to here as the Food Fraud Initial Screening (FFIS)" (Spink et al. 2016).

> While the desired outcome for risk mitigation planning are detailed vulnerability assessments, broader initial screening can make the process much more manageable. Often a detailed, by-individual-product assessment is not practical due to the nature of the risk, the time allotted, or the detail needed for resource-allocation decision-making. (Spink et al. 2016)

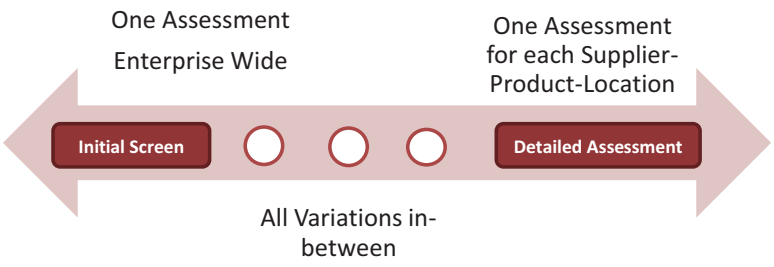


Fig. 6.9 Example of the continuum of the two-stage process for ERM risk assessment including from one initial screen for the entire enterprise through to one assessment for each supplier-product-manufacturing plant

Based on many factors—including the level of risk, cost of countermeasures and control systems, and certainty of the incident data, regulatory scrutiny, and vulnerability of the end consumer—different levels of assessments may be appropriate for different products. For example, "salt" may be able to be addressed with one overall initial screen for the entire corporation whereas due to many concerns "iodized salt for infant formula" may require a more detailed vulnerability assessment by source country, supplier, manufacturing plant, and transportation mode.

Overview of Business Economic Crimes Including Fraud

It is logical that food fraud, product fraud, and product counterfeiting have *not* been a primary focus of business economic crime or fraud investigations. The nature of the food fraud risk and root cause are so different from that of the other types of business fraud problems and that the current investigation or auditing fundamentals do not apply. A review of the types of business fraud often includes the likes of (PWC 2007, 2016):

1. "***Asset misappropriation*** including embezzlement and deception by employees
2. ***Accounting fraud*** either to benefit the enterprise or a specific business function
3. ***Corruption and bribery*** including racketeering and extortion
4. ***Money laundering*** of a wide range of revenues
5. ***IP infringement*** (a general category for Intellectual Property related issues) including trademarks, patents, counterfeit products and services, industrial espionage, etc."

The first four would be investigated using forensic accounting and forensic audits. The investigation processes for these four are traditional accounting audits, whereas the fifth requires completely different activities, expertise, and skills. The fifth is a catch-all category for all intellectual property infringement beyond trademark and patent where the investigation would include market monitoring, field investigations, or other analysis.

The first four types of business fraud generally occur within the company or at least at their facilities. The audits would occur *inside* those proprietary known locations or on those known computer systems. The fifth category of incidents probably occurs *outside* the company facilities and proprietary computer systems.

Also, the first four occur on a relatively frequent basis, and the methods of responses are very similar. Known assessment methods or standard operating procedures could be used to investigate the incidents. For the fifth, there sometimes appears to be as many types of fraud incidents as there are fraudsters.

Finally, for the first four, there is a lot of research, data, and analysis of the quantitative, analytical assessment of how much occurs. There are specific methods to analyze the extent of the economic impact. For the fifth, the losses are often unknown and possibly unknowable. There is even debate on the confidence in estimates of the economic impact of counterfeiting and piracy, see OECD (2007). Also, there is

uncertainty as to how much an IP infringement actually costs the company. There is reduced legal liability if someone is injured—as long as the offending product can be confirmed a counterfeit. Also, even lost sales are hard to quantify since abnormally low prices attract some buyers (e.g., a bulk product "near expiration" and "selling at a deep discount") or some consumers actually seek counterfeit products (e.g., fake luxury goods).

How (Un-)Ethical Are You?

What a question. This was the title of a 2003 Harvard Business Review article by Max Bazerman. The article essentially reviews and defines how we are not aware of our own sources of bias. This is an essential concept for Food Fraud Vulnerability Assessments. Our own "sources of bias" severely endanger our objectivity when conducting risk assessments.

Key biases that cloud our judgment include:

- **"The illusion of objectivity":** we believe that what we know is right and objective. If you've been in "food safety" for a "long time," then you think you've seen everything. Regarding food fraud, an example is an analytical chemist trying to conduct an authenticity test on stolen goods. Stolen goods are illegal, unfit for commerce, subject to a recall, could be mishandled, and become a health hazard, and they are a major concern for a company. That said, an authenticity test would only confirm the product is authentic but nothing about being stolen.
- **"Lack of awareness":** Combining the previous concepts, we frequently find a lack of awareness of the business process from other operations or divisions. We frequently heard "we don't do ERM" only to hear later—sometimes years—"oh, we have an ERM manager."
- **"Narrow focus":** "It's not my problem." Business is busy enough that we don't need to go looking for work… or, we don't *want to* go looking for more work. When new concepts are presented, there is often a belief that "someone else must be addressing this." Or "if we don't have a process, then it must not be important."

Early in the development of Food Fraud Prevention as a separate research concept, there were repeated statements that the FDA 2009 definition of "economically motivated adulteration" already covered everything. Also, there was a belief that the Food, Drug, and Cosmetics Act already covered everything in the "Adulterated Foods" and the "Misbranded Foods" sections. There is a difference between all types of food fraud being illegal and the regulations promoting a preventive approach. There is a difference between addressing the food safety health hazards that result versus addressing all food fraud vulnerabilities.

When applying the FDA EMA working definition in relation to the FDCA definition of what was actually illegal, there were three revelations occurred:

- (1) Economically motivated "adulteration" (a "substance" only) was different from "adulterated" as defined in the FDCA Adulterated Foods section (any problem including spoilage of genuine product or stolen goods).

- (2) The food adulteration laws administered by FDA prioritized on health hazards and did not consider unique root causes that could be addressed with a preventive control.
- '(3) The laws and regulations were focused on compliance and not prevention (of course, increased compliance or enforcement penalties had a secondary motivation to persuade companies to prevent).

Building on the Bazerman concepts are "confirmatory bias" and "trust-bias."

- **"Confirmatory bias"**—We seek confirmation for our beliefs… then we often conduct no more additional research. Once we find one article or report that supports our view, then we feel we've "researched" it.

The application to food fraud is that when other researchers or risk assessors heard those statements that "everything is already covered," they stopped looking and thinking… done and now move on to the next thing.

- **"Truth bias" or "Truthiness"**—We trust the people we know (Levine et al. 1999; Alba and Hutchinson 2000; Lapinski and Levine 2000; Park et al. 2002; Skurnik et al. 2005; Levine 2014; Levine et al. 2014; Van Swol et al. 2015). Or, to consider it from another perspective, when we've had a long history of experience with someone, then we feel we have no reason to mistrust the people we know. We trust people whom we know, are familiar with, and have interacted with for a long time. We can't imagine we would cheat people we know, so we project that value system on other people who are around us. There is a comfort in the known. We aren't aware of a problem so everything must be ok. Right? Also, there is a danger or risk of finding out that our present decisions have been sloppy, dangerous, or incompetent. We don't seek problems especially when they could hurt us.

Thus, understanding how and why there is bias, we can present new risks such as food fraud into a frame that can be understood and directly addressed. It is important to understand not only how other people behave and abuse trust but also in how we are biased in our own assessments. This is extremely complex. To reduce the complexity, it is efficient to "take morals and ethics out of the equation" and only focus on the "fraud opportunity." Regardless of the environment or the adversaries, "if there's a fraud opportunity then there's a fraud opportunity." Considering this human nature and our biases can help shift focus to very effective and efficient risk treatments that are in control of the guardians (for more on guardians and guardianship, see the chapter on Criminology).

Key Learning Objective 3: Iterative Process or Mitigating Food Fraud Risk Using ERM

This section reviews the interdisciplinary nature of prevention by considering how the fraud opportunity is created and the many academic disciplines that help understand the selection of optimal countermeasures and control systems.

The Key Learning Objectives of this section are:

- (1) Detail of ERM by a further review of the COSO Cube
- (2) Integrating ERM concepts into quality assurance and food safety standard operating procedures
- (3) Examples of applying ERM to Food Fraud Prevention resource-allocation decisions

COSO Cube in Detail

COSO has presented the ERM concepts in what is referred to as the "COSO Cube" (above, see Fig. 6.3). This is a way to explain how all the control activities interrelate. This is also a visual representation of the process to explain how food fraud assessments and reporting is connected with the enterprise. This is a clear way to explain how the overall processes fit together.

For Food Fraud Prevention, the COSO Cube provides a visual identification of where and how the Food Fraud Vulnerability Assessment fits into the overall, enterprise-wide assessment. The "risk assessment" entry point is a place for the new assessment to be correlated and calibrated with other enterprise-wide risks. The ERM system can provide a structure and process for assessing the new risk in a way that it can be seamlessly integrated into the overall enterprise-wide decision-making system.

The original COSO Cube was 3 × 5 (and later expanded to 4 × 8) and included three sides: front, top, and side (COSO 2013):

- **Front:** The front consists of the control environment, risk assessment, control activities, information and communication, and monitoring activities. These are five separate processes that create an interconnected hierarchy. For Food Fraud Prevention, the entry point is at the risk assessment.
- **Top:** The top consists of operations, reporting, and compliance. These are three separate activities. For Food Fraud Prevention, this would remain in the risk assessment/reporting cell.
- **Side:** The side expands across the enterprise from an entity (corporation), division, operating unit, and function. For Food Fraud Prevention, until the overall Food Fraud Prevention Strategy is developed and implemented, the focus is on the strategic and entity-level. In many cases and unless there are some local anomalies, an entity-level Food Fraud Vulnerability Assessment (FFVA) is acceptable for each level of the entity.

When considering the overall concept of the COSO Cube, next there is a consideration of the relationship between *objectives* and *components*.

A direct relationship exists between *objectives*, *components*, and the organizational *structure* of the entity. Although they are not actually noted on the cube, these are fundamental concepts that explain the working of the cube.

- **Objectives:** The three categories of objectives—operations, reporting, and compliance—are represented by the columns. These are what an entity strives to achieve.
- **Components:** The rows represent the eight components: Control environment, risk assessment, control activities, information and communication, and monitoring activities. These represent what is required to achieve the objectives.
- **Structure:** The third dimension represents an entity's organizational structure: Entity level, division, operation, and function.

Sidebar: Integrated Framework Between the Organizational Structure
The "internal controls" are the process to review, manage, and communicate risks. The "integrated framework" is the process for each level of the organization to calibrate and coordinate the internal controls (Fig. 6.10).

How this report can be used depends on the roles of the interested parties (COSO 2013) (emphasis added for "accountable" and "responsible" persons):

- **The Board of Directors**—"The board should discuss with senior management the state of the entity's system of internal control and provide oversight as needed. Senior management is accountable for internal control and to the board of directors, and the board needs to establish policies and expectations of how members should provide oversight of the entity's

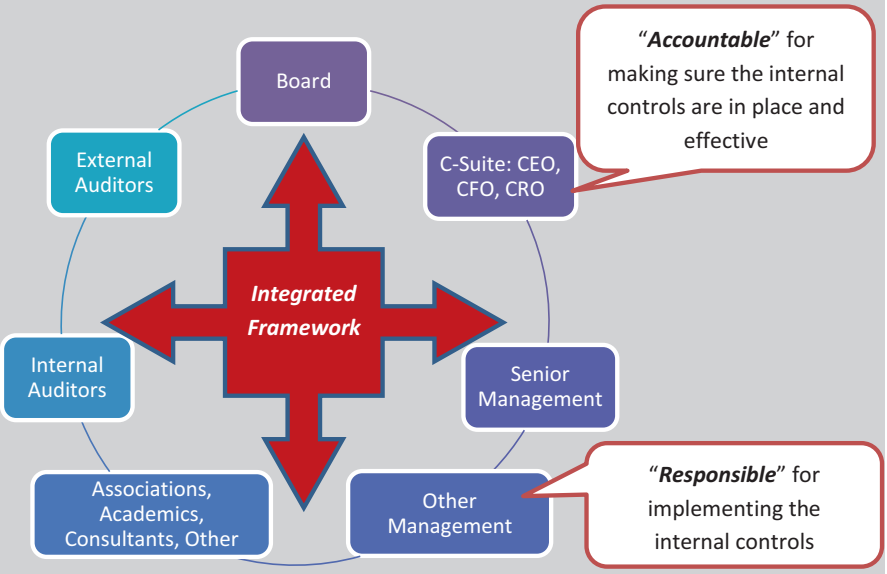


Fig. 6.10 Relationship between the internal controls (within business functions) and integrated framework (between functions)

(continued)

internal control." Also, "The board should challenge management and ask the tough questions, as necessary, and seek input and support from internal auditors, external auditors, and others."

- **Senior Management** (including C-suite of CEO, CFO, CRO, or their representatives or proxies): "Senior management should assess the entity's system of Internal Controls in relation to the Integrated Framework, focusing on how the organisation applies the seventeen [ERM] principles in support of the components of internal control."
- **Other Management and Personnel**: "Managers and other personnel… should consider how they are conducting their responsibilities in light of the Integrated Framework and discuss with [other] senior personnel ideas for strengthening Internal Controls. More specifically they should consider how existing controls affect the relevant principles within the components of Internal controls [presented in the COSO Cube]" (COSO 2013).
- **Internal Auditors [1st- or 2nd-party auditors]:** "Internal auditors should review their internal audit plans and how they applied the 1992 edition of the framework. Internal auditors also should review in detail the changes made to this version and consider possible implications of those changes on audit plans, evaluations, and any reporting on the entity's system of internal control" (COSO 2013).
- **Independent Auditors [2nd- or 3rd-party auditors]:** "In some jurisdictions [such as for GFSI related certification], an independent auditor is engaged to audit or examine the effectiveness of the client's Internal Controls over financial reporting in addition to auditing the entity's financial statements. Auditors can assess the entity's system of Internal Controls in relation to the Integrated Framework, focusing on how the organization has selected, developed, and deployed controls that affect the principles within the components of Internal Controls. Auditors, similar to management, may use the Illustrative Tools as part of this evaluation of the overall effectiveness of the entity's system of internal control" (COSO 2013).
- **Other Professional Organizations and Educators/Academia**:
  - **Other Professional Organizations**: "Other professional organizations providing guidance on operations, reporting, and compliance may consider their standards and guidance in comparison to the Integrated Framework" (COSO 2013).
  - **Educators/Academia**: "With the presumption that the Integrated Framework attains broad acceptance, its concepts and terms should find their way into university curricula" (COSO 2013).

Each of the interested parties has a role in the further development of internal controls as well as the strengthening of the integrated framework. Each interested party has a role in holding the other parties accountable for their responsibilities.

Integration with Standard Operating Procedures and Terminology

When presenting a new concept or theory, it is most efficient to anchor or root the resource-allocation decision-maker to some known and accepted concept. For example, if Food Fraud Prevention is presented as:

- "HACCP but for Food Fraud Prevention called vulnerability and VACCP."
- "This is just ERM but applied to Food Fraud Prevention."
- "It's basically total quality management or Six Sigma applied to Food Fraud Prevention."
- "We identify CCPs (critical control points), but instead of measuring oven temperatures for HACCP, we're verifying correct shipping documents for VACCP."

Explain Food Fraud Prevention by comparing it with a procedure or example they already know, understand, and trust. Using these types of explanations, someone not familiar with food fraud can have a clear vision and mental anchor of understanding from a comparison to a familiar and successful standard operating procedure. There is a reduced concern because new systems are not being developed. There is a reduced concern about an organization's adoption of new or different required procedures. At this point, the Food Fraud Prevention concepts have been presented in terms of common, implemented, widely accepted, and successful programs. Food Fraud Prevention research leveraged these concepts when forming the methods and processes.

It is just as important for a government agency to define their prevention actions in business terms since the concepts have been well researched, but also decision-makers or industry will be familiar with the methods. To note, many of the evaluators or critics of a government may be from the business world, so using business terms and methods is an efficient way to explain the functionality of the programs. A total quality management system or internal control framework is applicable to a government. The government agency does have a challenge that many of the final metrics are the social good (of course they must remain within budget, but success is ultimately a social measure such as "public health") versus clearly financial (e.g., return on capital employed, dividend amount, share price, or net profit).

A first important standard operating procedure is a quality management system. Initially, this was developed by Deming, Crosby, Juran, and others through total quality management, to now a Six Sigma-type program. This creates a framework—while keeping an eye on final performance—to shift focus to processes and systems that are the root cause of anomalies that could lead to a nonconformance. A version of quality management tailored for the food industry is the hazard analysis and critical control point plan (HACCP). The application is focused on identifying a critical control point (CCP)—e.g., a refrigerator staying at an appropriate and constant temperature—rather than just "is there a dangerous pathogen in the finished product." Expanding to focus on the controls, business adapted to create what ERM/COSO

defines as an "Internal Controls-Integrated Framework." The application is checking—and cross-checking—that the right controls are in place and they are properly implemented.

The goal is to present Food Fraud Prevention in a way that the thought is "oh, this isn't really anything new. This is just expanding our current program to address this new topic."

Decision-Making Examples to Find the Ideal Scenario

There is a continuum of the types of risk assessments from *operational risk* (e.g., tactical, quantitative, and expressed in "return on investment") and *enterprise-wide risk* (e.g., strategic, qualitative, and expressed as "vulnerability" and success is measured by reducing below the "risk tolerance") (Fig. 6.11). The *operational risks* that are tactical usually impact a specific group, product, or manufacturing plant and could impact the operation, though probably not put the entire enterprise as risk—there is usually a finite sample size that could often be 100% inspected (see other content on strategic and tactical actions), for example, metal shavings found in a packaged food product at the end of a manufacturing package fill line. If needed, the entire production lot could be set aside and tested with metal detectors. 100% inspection could be conducted. The *enterprise-wide risks* are strategic in the sense that they could

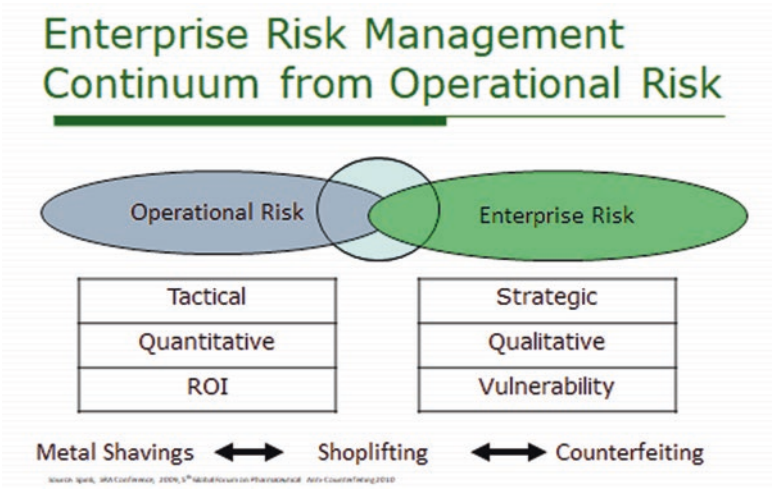


Fig. 6.11 Enterprise Risk Management Continuum from operational risk. (Copyright Permission Granted) (Spink 2009)

impact the entire enterprise and could be catastrophic could impact the entire company's brand, across the entire market, and could occur anywhere in the world, for example, the overall product counterfeiting threat. Assessing the risk or prevalence is extremely difficult because the sample population would be anywhere the product is sold anywhere in the world, including on the Internet and in illicit markets.

There is a continuum from the very specific and local event such as the metal shavings to the global event completely outside the legitimate supply chain. An example is assessing shoplifting losses in a retail store. Assessing the risk could include a physical inventory of the store, but it would not consider employee theft, incorrectly rung-up goods at the cash register, a damaged product that was destroyed but not recorded, or a product that was actually never received. This will be explained in more detail next in the example provided.

Example of Resource-Allocation Decision-Making with How to Measure Success

To provide an example of the different types of risks, several scenarios are presented. These examples span the continuum of operational/tactical to enterprise risk/strategic.

Metal Shavings

1. Incident: An incident is known with 100% certainty. If an incident occurs, then there is evidence there have been actual metal shavings in the finished products.
2. Scale: The inventory can be checked to approach 100% certainty. Each package could be tested.
3. Cost of nonconformance: This can be defined with certainty due to the cost of a recall, product disposal, and related costs, e.g., $4 million.
4. Cost of risk treatment: This is a "known" based on what countermeasure is selected, e.g., $1 million to purchase metal detectors.
5. How to measure success: Use the metal detectors. Create a process to calibrate, and make sure the metal detectors are used, e.g., high confidence if purchases quality equipment.
6. Confidence in the risk treatment: Create a process to calibrate, and make sure the metal detectors are used, e.g., high confidence if the operations are in control.
7. Financial assessment: In this case, an actual "return on investment" can be used. The very high-confidence savings (actually reducing in the loss of earnings—operations cannot be profit centers) of $1.5 million investment compared to the cost of $1 million will give an instant and—for a return of 1.5:1—a low rate of return but near 100% confidence in the return.
8. *Conclusion: Unless there are other pressing issues or business opportunities, this payback within 1 year would lead to a "yes" resource-allocation decision. This is a payback project within the year.*

Retail Shoplifting

1. Incident: There are probably reported and recorded incidents. The loss of inventory has many other root causes why a product may not be physically in the store. Other assessments or countermeasures and control systems may be needed for other issues such as employee theft. One assessment or countermeasure will not address the entire issue.
2. Scale: The inventory can be checked to approach 100% certainty but, again, not complete.
3. Cost of nonconformance: For the loss of inventory—though not only shoplifting—this can be defined with certainty due to the financial and inventory systems. Industry-wide, shoplifting—or "leakage"—is estimated to equate to 3% of corporate revenue, and so even industry-leading levels of shoplifting may be an additional 2% for a total of 5% of sales. For the last Fortune 500 company, with $500 million in revenue, this could be $10 million. Even if there are credits from the supplier or other offsets such as some type of insurance, every product that is stolen is lost revenue. That $10 million loss would be much higher than the metal shavings loss.
4. Cost of risk treatment: This is a "known" based on what countermeasure is selected. A $500 million retailer might have ten locations that each would be addressed, for example, $3 million for additional electronic article surveillance system upgrade.
5. How to measure success: Monitor the shoplifting alert, or capture and continue to count the inventory. Both of these will be very certain.
6. Confidence in the risk treatment: For shoplifting, the measures will provide high certainty but not for all inventory losses (unless the losses are almost or completely eliminated). For example, there is high confidence that the loss is from shoplifting, but only time will tell if that is the actual root cause of the problem.
7. Financial assessment: This will only become high confidence *after* implementing the system and measuring over time. So for resource-allocation decision-making, this financial benefit is uncertain.
8. *Conclusion: There could be a 50% confidence in the risk treatment reducing the $10 million loss by implementing the $4 million system for a return of 10:4 with a 50% confidence.*

Product Counterfeiting

1. Incident: An incident is known with a near 100% certainty—if you find a counterfeit product, then you know it is occurring. The data collection could either be reactionary (what people send you) or proactive (which could expand to seeking counterfeit product even in markets where there have been no past known incidents).
2. Scale: The scale is unknown and probably unknowable (Spink and Fejes 2012). If the OECD economic impact of counterfeiting estimate is used, then 5–7% of global sales could be lost to counterfeiting. For the last Fortune 500 company, with revenue of $500 million, that could be $25–35 million. Different industries

differ, so the estimate could be higher or lower. There is also a variable of whether there are deceptive or non-deceptive counterfeits. A deceptive counterfeit would be a 100% loss of a genuine product sale *if* there would not be *any* other replacement product (e.g., not finding a $50 pair of pants that usually retail for $200 may not lead to the consumer purchase the $200 genuine product; the consumer may opt for a $60 pair of discount pants—for more see (USITC 1988)). The economic impact of counterfeiting could really be defined as a broad range of possible financial impacts with a very low certainty of the actual dollar cost. It is known that it is occurring and that the corporation is incurring some costs. The most certain costs are the cost of lawsuits or anti-counterfeit countermeasures and investigations.

3. Cost of nonconformance: One counterfeit incident can lead to a worldwide recall and massive loss of brand equity. The estimate of "5–7%" loss could be for just *one* incident if that incident was significant. Thus the loss could probably be from $10 to $250 million per year, but let's use a very conservative $50 million here.
4. Cost of risk treatment: This is a "known" based on what countermeasure is selected—actually probably multiple countermeasures and control systems. For example, let's use a high $20 million for various countermeasures and control systems.
5. How to measure success: This is more complex since a primary source of estimating the impact is by conducting in-market inspections… all around the world, including in illicit markets. Conducting market monitoring in dangerous countries or marketplaces increases the liability risk and danger to the investigators. Basic food safety inspectors are not trained—or have the liability insurance—to engage criminals in situations where there could be physical violence. To start, increased surveillance would add to the cost. The countermeasures and control systems need to be continually updated to stay ahead of the evolving counterfeiters, so there are additional management costs.
6. Confidence in the risk treatment: The counterfeiters continue to evolve—e.g., possibly shift their focus from counterfeiting to stolen goods—so the overall enterprise risk reduction is difficult if not impossible to assess. Market investigations can determine whether *some* counterfeiters have been deterred, e.g., there is a low confidence—high uncertainty, many unknowns, and difficulty in data collection—in the countermeasures and control systems.
7. Financial assessment: In this case, if an actual "return on investment" can be developed, the uncertainty would be so high that the resource-allocation decision-maker would run out of money by funding other projects before selecting this low certainty, high-cost project.
8. *Conclusion: There would be a very low confidence (30%?) in reducing the counterfeit product in half from $100 to $50 million in losses with a cost of $20 million for a return of 50:20 with a maximum of a 30% certainty.*

When reviewing the details presented here, the CFO would instantly approve the metal shavings project, approve getting more detailed proposals for the shoplifting

countermeasures and control systems, and then possibly work with their General Counsel to determine "how little they can do" to address the counterfeit product. In all seriousness, the General Counsel and CFO then would assess the corporate risk appetite. These could use ERM/COSO type processes to define and defend "how much is enough."

Conclusion

When there is a new or novel incident, the response and responsibility are naturally assigned to an "intervention" stage activity (referring to the prevention-intervention-response plan). For example, when a contaminant in a health hazard was found in pet food, the intervention was to detect the contaminant that was causing harm. The next effort would be to implement actions to remove the contaminated product from the marketplace. A final activity may be to implement incoming goods' contaminant testing to try to prevent the additional fraudulent product from reentering the operations. This is a traditional food safety intervention, and often the proactive next step—of reducing the fraud opportunity—is not taken. The need to implement the last prevention step is often not done; for one, there is usually a regulatory definition of the "appropriate level of protection" or the scientifically measurable point of what is unacceptable. Waiting to respond *after* an incident is not proactive. Unlike for food safety and an adversary such as *E. coli*, for Food Fraud Prevention, the adversary is a human. This human behavior is studied within the field of social science and criminology. While studying the motivation of the adversary is the root cause, it does not include setting the limit. And in the absence of a regulatory or standards set unacceptable level, this is not a determination of the risk tolerance. *The first conclusion is* that business decision-making is a separate activity and discipline where systems are already usually in place including Enterprise Risk Management COSO. There are millions of theories or basic methods in the world, so the challenge is identifying what is applicable and adapting the response to a unique problem. Specific incidents are reviewed to refine and reassess the application continually. *The second conclusion is* that ERM-type systems can be adapted to create an efficient and straightforward application to Food Fraud Prevention. Once a general system is established, then there is a need for a standard operating procedure that both creates efficiency in the process and also continually monitor and evaluate the efficiency of the system. *The final conclusion is* that there is a need here based on ERM/COSO, for common internal controls paired with an evaluation system such as an integrated framework. There is a saying:

> ***Connect everything to everything – evaluate this new risk or vulnerability in relation to all other enterprise-wide problems in relation to the overall risk tolerance.***
>
> ***"We need to do 'more'" or "you should do 'more'" is not a business case. "This is really bad" is also not an assessment that can be compared. At worst you are not being proactive or providing the resource-allocation decision-makers with the information they need.***

Appendix: WIIFM Chapter on Business and ERM

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	ERM/COSO is very logical and provides a common language for enterprise-wide, top-to-bottom risk communication, and decision-making
Quality team	This chapter presents the widely adopted and very thorough COSO-based, ERM-type process that will be a foundation for "how much is enough?"
Auditors	The overall concepts provided ERM awareness and how it is implemented within the auditee organization
Management	This ERM overview will help with communication upwards into the organization and to the C-suite—you may want to apply it to all your business risk and decisions
Corp. decision-makers	Expect the front line and managers to be able to speak the language or risk and ERM/COSOs

Appendix: Study Questions

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

1. Discussion Question
   (a) Who defines the "risk tolerance" in a properly or improperly managed system?
   (b) What is the regulatory foundation for business decision-making and determining an acceptable risk tolerance?
   (c) How does a food fraud versus a food safety incident impact the risk tolerance and ERM-based decision-making?
2. Key Learning Objective 1
   (a) What is "Sarbanes-Oxley"?
   (b) Who is required by law to comply with Sarbanes-Oxley?
   (c) When Sarbanes-Oxley may not be a legal requirement, what systems are in place to manage risk and risk tolerance for a company?
3. Key Learning Objective 2
   (a) What is a "corporate risk map" or "risk heat map"?
   (b) How does a CFO decide if a risk or vulnerability is so bad it must be reduced (or disclosed to investors)?
   (c) What is the most challenging aspect of applying ERM to FF?

4. Key Learning Objective 3
   (a) What is a "2nd"- and "3rd"-party auditor?
   (b) What is the COSO Cube?
   (c) Where does a food fraud incident enter the COSO Cube, and who does the review advance?

References

Alba, J. W., & Hutchinson, J. W. (2000). Knowledge calibration: What consumers know and what they think they know. *Journal of Consumer Research, 27*(2), 123–156.

Boland, V. (2008, December 18). The saga of Parmalat's collapse. *Financial Times*, Milan. URL: https://www.ft.com/content/c275dc7c-cd3a-11dd-9905-000077b07658

Buchanan, R. (2007). Tools for prioritizing food safety concerns: An FDA perspective. In *Tools for prioritizing food safety concerns workshop*. Greenbelt, MD: CFSAN/FDA, JIFSAN.

Buchanan, R. L. (2016, April). *Introduction to risk management, food safety symposium*. Hosted by MARS Foods, Beijing.

CODEX, Codex Alimentarius (2003). *Guidelines on the judgement of equivalence of sanitary measures associated with food inspection and certification systems*, 1, CAC/GL 53-2003. www.fao.org/input/download/standards/10047/CXG_053e.pdf

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

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

Kellogg Company (2017). *Form 10Q, submitted to US securities and exchange commission*. Posted on EDGAR Company Filing website. URL: https://www.sec.gov/Archives/edgar/data/55067/000162828017008104/k-2017q210xq.htm

Lapinski, M. K., & Levine, T. R. (2000). Culture and information manipulation theory: The effects of self-construal and locus of benefit on information manipulation. *Communication Studies, 51*(1), 55.

Levine, T. R. (2014). Truth-default theory (TDT) a theory of human deception and deception detection. *Journal of Language and Social Psychology, 33*(4), 378–392.

Levine, T. R., Clare, D. D., Green, T., Serota, K. B., & Park, H. S. (2014). The effects of truth–lie base rate on interactive deception detection accuracy. *Human Communication Research, 40*(3), 350–372.

Levine, T. R., Park, H. S., & McCornack, S. A. (1999). Accuracy in detecting truths and lies: Documenting the "veracity effect". *Communications Monographs, 66*(2), 125–144.

Levitt, S. D., & Dubner, S. J. (2014). *Think like a freak*. New York: William Morrow.

MSU-FFI, Michigan State University's Food Fraud Initiative (2017, August). *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. 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

OECD, Organisation for Economic Co-operation and Development. (2007). Estimating the magnitude of counterfeiting and piracy. In OECD (Ed.), *The economic impact of counterfeiting and piracy*. Paris: OECD Publishing. URL: http://dx.doi.org.proxy2.cl.msu.edu/10.1787/9789264045521-5-en.

Oppel, R., & Sorkinnov, A. (2001, November 29). Enron's collapse: The overview: Enron collapses as suitor cancels plans for merger. *New York Times*. URL: http://www.nytimes.com/2001/11/29/business/enron-s-collapse-the-overview-enron-collapses-as-suitor-cancels-plans-for-merger.html

Park, H. S., Levine, T., McCornack, S., Morrison, K., & Ferrara, M. (2002). How people really detect lies. *Communication Monographs, 69*(2), 144–157.

Porter, M. E. (1980). *Competitive strategy: Techniques of industry and competitor analysis*. New York: Free Press.

Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance* (p. 1985). New York: Free Press.

PWC, PriceWaterhouseCooper (2007). *Economic crime: People, culture and controls*. The 4th biennial Global Economic Crime Survey Investigations and Forensic Services, PriceWaterhouseCooper (PWC). URL: http://www.pwc.com/extweb/pwcpublications.nsf/docid/1E0890149345149E8525737000705AF1/$file/PwC_2007GECS.pdf

PWC, PriceWaterhouseCooper (2016). *Food fraud home page*. URL: http://www.pwc.com/gx/en/services/food-supply-integrity-services/publications/food-fraud.html

Romero, S., & Atlas, R. D. (2002, July 22). Worldcom's collapse: The overview; Worldcom files for Bankrupcy; Largest U.S. case. *New York Times*. URL: http://www.nytimes.com/2002/07/22/us/worldcom-s-collapse-the-overview-worldcom-files-for-bankruptcy-largest-us-case.html

Skurnik, I., Yoon, C., Park, D. C., & Schwarz, N. (2005). How warnings about false claims become recommendations. *Journal of Consumer Research, 31*(4), 713–724.

Spink, J. (2009). *Emerging risk assessment for agencies on economically motivated adulteration, food fraud, and product counterfeiting*. Society for risk analysis: Annual conference 2009, Baltimore, MD.

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., Evans, B., & Freeman, E. (2019). *Introducing the food fraud suspicious activity report method (FF-SAR)*. Working paper, Food Fraud Initiative, Michigan State University. URL: www.FoodFraud.msu.edu

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

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

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

Taleb, N. N. (2007). *The black swan: The impact of the highly improbable*. New York: Random House.

USITC, United States International Trade Commission (1988). *Foreign protection of intellectual property rights and the effect on U.S. industry and trade*. Report to the United States Trade Representative, Investigation NO. 332-245, Under Section 332(g) of the Tariff ACt of 1930, USITC Publication 2065.

Van Swol, L. M., Braun, M. T., & Kolb, M. R. (2015). Deception, detection, demeanor, and truth bias in face-to-face and computer-mediated communication. *Communication Research, 42*(8), 1116–1142.

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