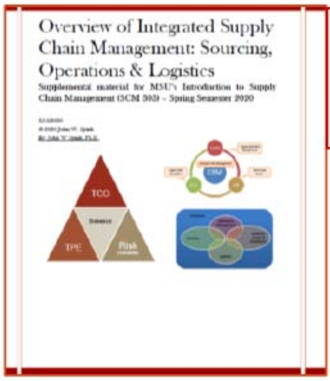


Overview of Integrated Supply Chain Management: Sourcing, Operations & Logistics

Supplemental material for MSU's Introduction to Supply Chain Management (SCM 303) – Spring Semester 2020

Spink, John, ***Overview of Integrated Supply Chain Management: Sourcing, Operations & Logistics, ISBN 978-x-xx-xxxxxx-x*****. IN PRESS, Section 8 (Date 6/1/2020, Version 60)**

Chapter 8 FUNCTIONS: Cross-functional or Corporate-wide activities

Under the concept of overall management systems or "internal controls/ integrated framework" (see above, there are functions that support the basic supply chain functions of procurement, operations, and logistics, there are support functions that are integrated and managed across the entire organization, including quality management, risk management, corporate social responsibility, and including the lean systems approach. These are independent functions that have their own terminology and methods, but they succeed when they are integrated and calibrated to and from the overall corporate strategic goals.

8.1 FUNCTIONS: Quality

Quality management developed from an original focus on improving the efficiency of manufacturing and reducing off-specification product costs, to an over-arching philosophy of continuous improvement with methodical processes to calibrate and refine a level of product or service performance. Starting with Juran and others, through Demming and Crosby, codified in international standards such as ISO 9000, the modern version is a complex corporate culture defined by systems such as Six Sigma. The concepts have been adopted and adapted over time to the point that they are widely accepted as common sense and fundamental for any successful organization.

Expanding on the value chain discussion from the section above, quality assurance or quality management is a specific activity type that is now applied to every business function. Also, other sections in this book that introduced or mentioned quality management explained how the activity fits into the overall Supply Chain Management discipline or how it supports ongoing management of the enterprise (see previous sections).

Referring to those value chain activity types, in "Competitive Advantage" published in 1985, Michael Porter stated that "the role of indirect and quality assurance activities are often not well understood, making the distinction among the three activity types (direct, indirect and quality assurance) an important one for diagnosing competitive advantage." [5] Over the 35 years, quality assurance has become much more of a focus area and much more valued and so widely adopted that there is frequently a "quality culture" at companies – an intensive and thoroughly ingrained value of quality.

The general quality concepts are universal and apply from ISO 9000 Quality Management to all business functions and all businesses. There is a specific and unique focus on supplier quality assurance to reduce the variability from outside your control, your suppliers. There are standards and common practices to require and communicate a level of compliance and quality.

When applying these concepts here, there is a specific definition and scope where:

- "***Supply chain quality management (SCQM)*** is defined as a systems-based approach to performance improvement that leverages opportunities created by upstream and downstream linkages with suppliers and customers. [15]

Quality Management Foundation

Quality management principles and philosophy developed over many years, generally recognized to start after World War II to help increase manufacturing efficiency. Through the years, the philosophy matured led by researchers such as Juran, Demming, Crosby, and others. Other specific concepts developed such as total quality management, quality functional deployment, Six Sigma, Lean Systems, and then further hybrids such as Lean Six Sigma.

While this was all developing, it became clear that consensus and harmonization would be efficient, and this resulted in the creation of ISO 9000 Quality Management.[16] The ISO 9000 standard incorporated other related standards such as ISO 31000 Risk Management and then incorporated into other such as ISO 22000 Food Safety, ISO 28000 Supply Chain Security, and ISO 22380 General principles for product fraud risk and countermeasures. [17] The evolution expanded from management systems to more prescriptive approaches such as a product fraud classification model (presented as the Product Counterfeiting Incident Clustering Tool – PCICT) in ISO 12931 Performance criteria for authentication solutions for anti-counterfeiting in the field of material goods. [18]

The Role of Supply Chain Functions

As there are specific functions in supply chain management of procurement, operations, and logistics, there are specific quality concepts that apply to each. The different supply chain functions have different and interrelated roles in quality assurance and quality management. For the ***supply chain quality management scope***, there are three critical points of differentiation are for incoming products, work in progress and outbound, and then an overall consideration of all branded product in the marketplace (this final point is defined to include technology transfer, contract manufacturing, substandard or rejected product, waste products or packages, and even counterfeit or stolen branded product in the marketplace.)

"Functional influences on product quality [13]

- Supply or procurement managers
  - description of purchase requirements
  - selection of suppliers

        - establishment of contracts and associated incentives and penalties
        - management of and interactions with suppliers
    - Manufacturing and service operations managers
        - design and execution of processes and procedures
        - design of work policies
        - interactions with customers
        - management of facilities and equipment
        - scheduling of work
    - Logistics managers
        - selection of transportation providers
        - development of tracking and other information systems
        - design of packaging, storage, and material handlings processes
        - Management of and interactions with transportation providers."

A corporate overseer function, often first assigned to corporate security or system-wide brand management, is an additional key function that oversees the entire supply chain through to the retailer and customer, including reverse logistics and disposal. A key is that the "three poor quality opportunities" include "before a purchase commitment is made to a supplier, during the commitment to the supplier, and after the purchase commitment has been made." [13]

The corporate security initiative countermeasures or control systems would be implemented and managed by the supply chain functions.

The supplier management function influences the quality focus on need identification and optimization, development of specifications and common product requirements, identifying and then managing the supply of raw materials or incoming goods.

> "[Strategic Supply Management] is a strategic, planned effort to create a capable supplier base and leverage the benefit of supply management. It is a key strategic planning process in purchasing management. On the other hand, QM is viewed as a philosophy aimed at continuously improving the quality of products and

> processes to achieve customer satisfaction." [...] A favorable QM culture drives organizations to improve their efficiency beyond organizational boundaries and along the supply chain. A total quality initiative steers the buyer firm to improve the capabilities and performance of its suppliers." [19]

Quality Principles and Concepts

There are some basic fundamental principles and concepts that define the supply chain management aspects of quality and quality management. While the original focus was on the assurance of the quality of the manufactured product (e.g., Porter's focus on "Quality Assurance), the application is now applied across the integrated supply chain and also universally applied across an entire company (e.g., common programs such as Six Sigma create a harmonized approach and focus to any business function). To start, it is important to establish that there is the cost of quality, and the end customer defines the optimal balance of the total cost of ownership and total product experience – the prince and level of acceptable quality. The first step is to identify the ***Market Niches for Quality,*** which is: (1) better than competitors, (2) same, or (3) less. [14]

The consideration of nick creates a need to define quality which results in eight dimensions generally:

"Eight Dimensions of Quality [14]

1. Performance: The primary function of the product or service
2. Features: The bells and whistles.
3. Reliability: The probability of failure within a specified time period.
4. Durability: The life expectancy.
5. Conformance: The meeting of specifications.
6. Serviceability: The maintainability and ease of fixing.
7. Aesthetics: The look, smell, feel, and sound.
8. Perceived quality: The image in the eyes of the customer."

Further, the definitions of quality can be applied to different types of quality that include: "***Product Quality***: fitness for consumption in meeting customers' needs and desires, ***Design Quality***: a match between designed features and customer requirements, ***Conformance Quality***: meeting design specifications, and ***Quality Management***: organization-wide quality focus."

Quality Management Tools and Techniques

As the focus on quality management has become refined and modified, there have been specific tools and techniques adopted and adapted for particular needs. These programs included with general continuous improvement and the Demming wheel of "plan-do-check-act," this incorporated metrics and analytics in Statistical Process Control (SPC), then evolved to total quality management (TQM), Quality Functional Deployment (QFD), then to a more formalized, structured, and enterprise-wide adoption of Six Sigma and the driving out of waste and costs by applying the Lean Philosophy.

Plan-Do-Check-Act ("the Deming Wheel"): [13]

- Guiding Methodologies:
- **Plan**: identify problem and actions for improvement
- **Do**: implement a formulated plan
- **Check**: monitor results
- **Act**: take corrective action and institutionalize changes

"Total Quality Management (TQM) – Supply Focus [14]

- A philosophy and system of management focused on long-term success through customer satisfaction.
- Quality integrated throughout the organization's activities
- Employee commitment to continuous improvement
- **Suppliers** are partners in the TQM process
- Uses tools including continuous improvement or *kaizen,* quality function deployment (QFD), and statistical process control (SPC) to achieve performance improvements

"Total Quality Management (TQM) – Operations and Logistics Focused: [13]

- **Total Quality Management (TQM)** – an integrated strategy aimed at embedding awareness of quality. The word *total* has important connotations:
- A product's quality is determined by a customer's acceptance and use.
- Quality management is a *total, organization-wide activity,* rather than a technical task.

- Quality improvement requires a *total commitment from all employees.*

Quality Function Deployment (QFD): [13]

- "QFD is a process, supported by a set of tools, to translate customer requirements, or "voice of the customer" (VOC), into specifications.
- Helps to understand what value represents to the customer and provides direction
- Across-functional activity, involving input from operations, marketing/sales, engineering, accounting/ finance, and supply.
- It can be applied to both products and services."

Six Sigma

- A philosophy that work are processes that can be defined, measured, analyzed, improved and controlled (DMAIC)
- Six sigma quality (6 ▯) represents 3.4 defects per million opportunities
- six standard deviations are very close to zero defects and correspond to a "Cpk" value of 2.0
- Uses a set of tools, such as SPC, control charts, and flowcharting, to drive process improvements.
- Well-defined projects with measurable goals:
- e.g., cost reduction or profit increase through improvements in cycle time, delivery, safety, etc.
- Team members have training in statistics
- Applies to product manufacturing and services

Six Sigma Concept of DMAIAC: [13]

- **Define**: determine Critical to Quality (C T Q) characteristics from the customer's perspective.
- **Measure**: gather data on C T Q processes.
- **Analyze**: determine the cause of defects.
- **Improve**: modify processes.
- **Control**: ensure improvements are maintained.

Statistical Process Control (SPC): [13]

- "A technique that involves testing a random sample of output from a process in order to detect if nonrandom changes in the process are occurring
- *Causes of variation:* Common causes and special or nonrandom, assignable causes
- *Process capability: the* ability of the process to meet specifications consistently."

There are other risk management systems or tools that also provide support such as Failure-Mode-Effects-Analysis (FMEA), Probabilistic Risk Assessment (PRA), and others. [20]

The Application of Six Sigma

The Six Sigma approach to quality management is widely implemented in part because of its very comprehensive and formal training and certification resources. This topic is one of the quality management systems that build upon the PDCA cycle and the ISO 9000 concepts. This topic provides a very rigorous yet flexible system that can be universally implemented across an enterprise, not just to monitoring production efficiency or measuring incoming or outgoing goods performance.

> "Six Sigma approaches are strikingly similar to prior approaches to quality management, and it provides an organizational structure not previously seen. This emergent structure for quality management helps organizations more rigorously control process improvement activities, while at the same time creating a context that enables problem exploration between disparate organizational members. Although Six Sigma provides benefits over prior approaches to quality management, it also creates new challenges for researchers and practitioners." [21]

Six Sigma approaches have an intense focus on calibrating the customer needs into the control activities. 'A fundamental aspect of Six Sigma methodology is the identification of ***critical-to-quality (CTQ)*** characteristics that are vital to customer satisfaction."[22]. The baseline and desired process sigma measure levels are, in fact, defined relative to customer requirements. As a result, customers requirements help establish project improvement goals and direct improvement efforts of Six Sigma teams." [21]

A key to the broad application is that the basic concepts are standard and applicable to any process or activity. The implementations create "an organized, parallel-mesostructured to reduce variation in organizational processes by using improvement specialists, a structured method, and performance metrics with the aim of achieving strategic objectives." [21] This topic means that experts can apply their methods – and communicate the programs – across all business functions. This topic creates a business function that is dedicated to improving the operation and efficiency of an enterprise.

Cost of Quality and "How Much is Enough?"

Quality is not free. Improving operations is not free. Improving the performance of the finished good is not free. There is an optimal level based on the total cost of ownership and the total product experience, balanced with a way to address uncertainty or risk. Quality is a key factor in the value proposition, which is based on the requirements of key customers in balance with the return on the investment required by the stakeholders or investors.

There is a ***cost of quality***, which is a combination of the impact on the profitability of an enterprise of financial, human resource, or asset application drains. The "Five Major Cost of Quality Categories" is "Prevention costs, Appraisal costs, Internal failure costs, external failure costs, and Morale costs." [13]

The "Check" in "Plan-Do-Check-Act"

A key aspect of efficient and effective supply chain management is to expand from providing precise specifications for the supplier that meets the needs of finding ways to monitor and verify the ongoing quality. One risk is a change in effort or process that changes the level of quality. Another is a lack of awareness of the drift of critical specification attributes to unacceptable levels. Then there is also a ***quality fade*** that is an intentional reduction of the quality over the duration of the supply agreement. Actually, a fourth risk is an intentional action with the goal to defraud economically, which could be from supply chain disruptions such as stolen goods, rejected sub-standard products, product fraud, or intellectual property rights infringing product counterfeiting.

The fist need is to set the expectation of the process and product attributes. A process attribute could be the adoption and certification of a quality management system such as an ISO or GFSI. For food, the GFSI endorsed Food Safety Management System is a preventive approach to the supplier-customer relationship where a third party accreditation confirms quality management systems and controls are in place to reduce non-conformities or defects. The product attributes could be monitored and verified through ongoing samples of the incoming goods or finished goods in the marketplace. A ***sampling plan*** could include tests that are random, sequential, complete (100%), or testing. [14]

Quality management is an enterprise-wide activity that focuses explicitly on specifying, monitoring, and verifying the movement and processing of goods and services as they move from the supplier through the supply chain to the consumer, which includes reverse logistics and disposal.

8.2 FUNCTIONS: Risk Management

Risk management has expanded and matured as an enterprise-wide focus as there is more computing power to analyze more information, in more detail, farther across the organization and around the world. To real-time monitoring, while this has been an important ongoing topic, key problems such as corporate fraud at Enron/ WorldComm/ Parmalot and the sub-prime lending crisis led to laws, regulations, standards, and certifications. In the U.S., the Sarbanes-Oxley Act of 2007 is a legal requirement for all publically traded companies, and the associated COSO/ ERM-type practices are required by most corporations around the world. In addition, international standards such as ISO 31000:200934Risk Management have further harmonized the terminology and standardized the best practices.

Risk assessment is a specific function within the concept of risk analysis. The entire process includes gathering information and processing it into a useful and reliable form. This section is an excerpt from Spink, 2020 [20]):

[3] Note: in this manuscript, the year listed with an ISO standard is the year it was first adopted.

[4] Note: an ISO standard is identified by a number and then the year adopted. For example, ISO 31000:2009 refers to standard 31000 Risk Management and associated with the publication year 2009.

Introduction to Risk Analysis

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

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

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

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

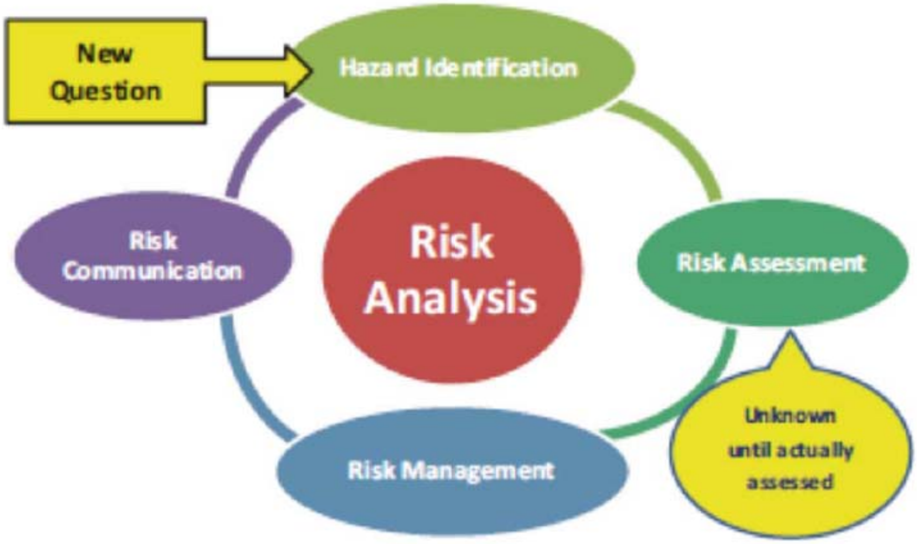


Figure 7: Risk analysis cycle including hazard identification, risk assessment, risk management, and risk communication (Copyright permission granted) [20]

Introduction to Risk and Vulnerability: Foundational Terms

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

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

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

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

- **Event:** "An event is essentially something that occurs (summarizing: ISO31000; CNSSI 2010; Merriam-Webster 2004). There is no evaluation yet of the change in the consequence."
- **Incident:** "A type of event is an incident that has occurred and evaluated, and that could have a negative consequence (DHS 2008; ANSI 2009; CNSSI 2010)."
- **Vulnerability:** "[A] weakness or flaw that creates opportunities for undesirable events related to the system ("system design") (ISO 2007a; ISO 2002, 2012; DHS 2013; NIST 2011; CNSSI 2010; NRC 2009; COSO 2014; Merriam-Webster 2004). The result of a vulnerability assessment is usually a qualitative statement of the susceptibility of the system e this influences the likelihood (NRC 2009)."
- **Risk:** "Risk is an uncertainty of an outcome that is assessed in terms of likelihood and consequence (ISO 2007a; NIST 2002; CNSSI 2010; DHS 2013). Often the consequence is sub-divided to other factors such as onset, severity, or other. Risk is based on factors of the probability of the threat and the susceptibility from vulnerability (NRC 2009). In other applications, it is an unwanted outcome (DHS 2008; Codex 2014, 21 CFR 50 (A) (.3)(k), Merriam-Webster 2004)."
- **Hazard:** "Also, a hazard is an event that has not occurred and could cause harm if not addressed (ISO 2007b; PAS 96 2014; NRC 1996; 21 CFR, Merriam-Webster 2004) -- this includes damaging potential (ISO 2007b). For food, this is often applied to unintentional events that have the potential to harm. A new note to add is that the US FDA further defines an unacceptable level of protection as a "hazard that requires a preventive control" (FDA 2015) (for more on the appropriate level of protection see (WTO 1995; CODEX 2003)).
- **Threat:** "...is the cause of an unwanted event that includes generally known variables or attributes of the source of the negative consequence ("threat source") (ISO 2012; ISO 2002; 21 CFR 121, ANSI 2009; PAS 96 2014; FSMA 2016; NIST 2002; CNSSI 2010; UNODC 2010; DHS 2013) – this includes incident, hazard, damaging potential, etc. In crime and security science, this is often a person(s) who have the intent and capability to cause harm. This is often applied to intentional acts with the intent to harm. The result of a threat assessment is usually a quantitative probability of the event to occur – but not an assessment of the consequence."
- **Mitigation:** "...is intended to reduce the consequence of the event (ISO 2007a, b; ISO 2007; DHS 2013; Merriam-Webster 2004). This assumes the hazard event will occur, so the goal is to mitigate or reduce the negative consequence. This focuses on reducing the risk that cannot be eliminated."

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

Building on these definitions and applying to a specific problem such as food fraud (Spink et al. 2017), the terms are:

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

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

Other related terms defined in ISO 31000 include [23]:

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

When focusing on how to address risks and determine "how much is enough" for countermeasures and control systems, ISO 31000 Risk Management presents several key concepts [23]:

- **Residual risk:** risk (2.1) remaining after risk treatment (2.25) [SOURCE: ISO Guide 73:2009, definition 3.8.1.6]
- **Risk acceptance:** informed decision to take a particular risk (1.1) [ISO Guide 73]; Note 1 to entry: Risk acceptance can occur without risk treatment (3.8.1) or during the process of risk treatment; Note 2 to entry: Accepted risks are subject to monitoring (3.8.2.1) and review (3.8.2.2).
- **Risk aggregation:** a combination of a number of risks into one risk (1.1) to develop a more complete understanding of the overall risk [ISO Guide 73] [Note: also referred to as risk summing or risk overview.]
- **Risk appetite:** amount and type of risk (1.1) that an organization is willing to pursue or retain [ISO Guide 73]
- **Risk attitude:** organization's approach to assess and eventually pursue, retain, take or turn away from risk (1.1) [ISO Guide 73]
- **Risk aversion:** attitude to turn away from risk (1.1) [ISO Guide 73]
- **Risk perception:** stakeholder's (3.2.1.1) view on a risk (1.1) [ISO Guide 73];
    - Note 1 to entry: Risk perception reflects the stakeholder's needs, issues, knowledge, belief, and values.
- **Risk review:** activity undertaken to determine the suitability, adequacy, and effectiveness of the subject matter to achieve established objectives *Note* Review can be applied to a risk management framework (2.3), risk management process (2.8), risk (2.1) or control (2.26)." [ISO Guide 73:2009, definition 3.8.2.2]
- **Risk tolerance:** organization's or stakeholder's (3.2.1.1) readiness to bear the risk (1.1) after risk treatment (3.8.1) in order to achieve its objectives [ISO Guide 73]; Note 1 to entry: Risk tolerance can be influenced by legal or regulatory requirements.

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

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

ISO 31000 Risk Management was published in 2009 after years of a consensus-driven process involving national standards organizations. Even though this was a comprehensive and interdisciplinary approach, it was not without critics. There was support with seemingly simultaneous criticism such as "The consequence of this is that certain ideas about risk and its management have got a boost in credibility and prominence while others have lost out" (Leitch 2010). The meaning is that while the field of risk management received credibility from an ISO standard and future research that was more harmonized, some fields would have to change their current terminology to be compliant. In some cases, this is simple, but often they are very formalized and in-depth research using one or another of the terms. Any change in the terms would lead to an update of all that previous research or possibly an insinuation that the original authors were not knowledgeable or even correct in their most basic theories. An example may be the early research on food fraud and economically motivated adulteration. Some research was published using economically motivated adulteration. Still, the later research shifted to food fraud—there could be confusion or a lack of prestige from those who changed their terminology. This insight was true for some of the risk assessments and use of terms such as probability versus likelihood, severity versus consequence, and prevention versus mitigation.

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

From ISO 31000, there are some key definitions (including a few terms that have been presented and defined earlier in this book) [23]:

- ***"Risk:*** effect of uncertainty on objectives;
    - NOTE 1: An effect is a deviation from the expected – positive and/or negative.
    - NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product, and process).
    - NOTE 3 Risk is often characterized by reference to potential events (2.17) and consequences (2.18) or a combination of these.
    - NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (2.19) of occurrence. ISO 31000:2009(E)"
- ***"Risk attitude*** (referred to in later ISO documents or COSO as 'risk tolerance' or 'risk appetite'): organization's approach to assess and eventually pursue, retain, take or turn away from risk [ISO Guide 73:2009, definition 3.7.1.1]"
- ***"Consequence:*** outcome of an event affecting objectives
    - NOTE 1: An event can lead to a range of consequences.
    - NOTE 2: A consequence can be certain or uncertain and can have positive or negative effects on objectives.

  - NOTE 3: Consequences can be expressed qualitatively or quantitatively.
  - NOTE 4: Initial consequences can escalate through knock-on effects. [ISO Guide 73:2009, definition 3.6.1.3]"
- ***"Likelihood:*** the chance of something happening
  - NOTE 1: In risk management terminology, the word 'likelihood' is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively and described using general terms or mathematically (such as a probability or a frequency over a given time period).
  - NOTE 2: The English term 'likelihood' does not have a direct equivalent in some languages; instead, the equivalent of the term 'probability' is often used. However, in English, 'probability' is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, 'likelihood' is used with the intent that it should have the same broad interpretation as the term 'probability' has in many languages other than English. [ISO Guide 73:2009, definition 3.6.1.1]"
- **"Risk source:** an element which alone or in combination has the intrinsic potential to give rise to risk, NOTE: A risk source can be tangible or intangible. [ISO Guide 73:2009, definition 3.5.1.2]"

This set of definitions is published in coordination with other ISO standards including:

- **ISO Guide 73:2009, Risk management—Vocabulary:** A thorough glossary of terms with detailed definitions.
- **ISO/IEC 31010:2009, Risk management—Risk assessment techniques**: A further review of the process of analyzing and managing risks. ISO 31000 has a focus on the sources of risks or broadly how they are generated, root cause analysis, and then an integrated focus on how best to implement and manage a risk treatment.

Quantitative or Qualitative Analysis: Both Are Supported in ISO 31000

ISO 31000 repeatedly emphasizes to conduct the assessment that is most logical and efficient for the question being asked. This process can be very formal and quantitative or more informal and qualitative (Purdy 2010). "Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances."[23]

This statement is reiterated in the ISO 31000 standard:[23]

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

The bottom-line summary is to select a system and specification that meets *your* needs. Occasionally levels of detail or methods are defined in standards; however, often, they are not.

The general "risk treatments" are presented with flexibility for the risk assessor (ISO 2009): "Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:

1) Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
2) Taking or increasing the risk in order to pursue an opportunity;
3) Removing the risk source;
4) Changing the likelihood;
5) Changing the consequences;
6) Sharing the risk with another party or parties (including contracts and risk financing); and
7) Retaining the risk by informed decision."

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

ISO 31000 also provides a basic framework that is a logical starting point (Fig. 15.5): "Establishing the context" is one of the most important steps and is so basic that it is often overlooked by traditional food science risk assessors. Often an incident such as melamine is identified, and the risk assessors quickly use currently available and understood control measures to select and implement risk treatments. The incident is melamine in the product (risk identification), this is a product recall, so it is a problem (risk analysis and risk evaluation), and so applying traditional food safety controls would be to implement a melamine detection test (risk treatment). "Experts" who believe they are already familiar with the incident almost automatically jump to conclusions.

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

Steps including:

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

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

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

4. **"Risk Evaluation":**

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

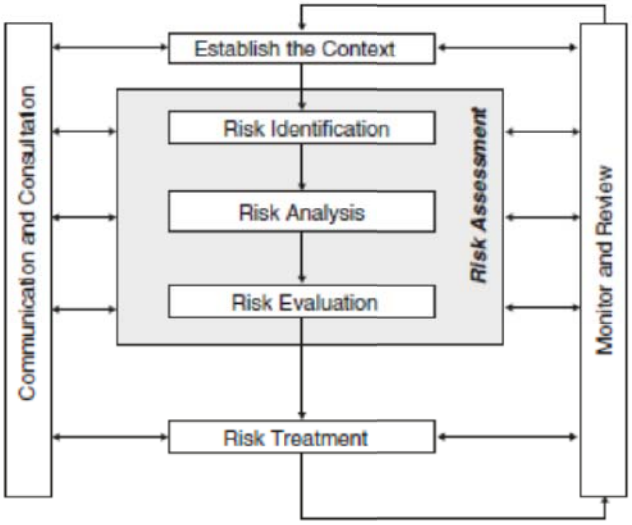


Figure 8: <title>

This section provided insight into ISO 31000 Risk Management, presented the terms and concepts and then presented the application to food fraud prevention. This concept is a valuable exercise to present the underlying consensus-based standards base and also to explain the logic of the process. The ERM/COSO system is most efficient and effective for a company to utilize when calibrating the enterprise-wide risks and assessing the vulnerability in relation to the risk tolerance. Those conclusions are logical if they consider past incidents and food safety, public health risk-based approach. However, "Establishing the context" may not be "detect melamine in the product that is being received." The best overall goal could be to "reduce the fraud opportunity of a range of adulterant-substances to be sent to the company."

Several related ISO risk terms include:

- **"Risk assessment:** the overall process of risk identification (2.15), risk analysis (2.21), and risk evaluation (2.24) [ISO Guide 73:2009, definition 3.4.1]."
- **"Risk criteria:** terms of reference against which the significance of risk (2.1) is evaluated [SOURCE: ISO Guide 73:2009, definition 3.3.1.3]
  - Note 1 to entry: Risk criteria are based on organizational objectives, and external (2.10) and internal context (2.11).
  - Note 2 to entry: Risk criteria can be derived from standards, laws, policies, and other requirements."

- **"Risk management policy:** statement of the overall intentions and direction of an organization related to risk management (2.2) [SOURCE: ISO Guide 73:2009, definition 2.1.2]."
- **"External context:** external environment in which the organization seeks to achieve its objectives [SOURCE: ISO Guide 73:2009, definition 3.3.1.1]
    - Note 1 to entry: External context can include:
    - – the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
    - – key drivers and trends having an impact on the objectives of the organization; and
    - – relationships with, and perceptions and values of external **stakeholders** (2.13)."
- **"Internal context:** internal environment in which the organization seeks to achieve its objectives [SOURCE: ISO Guide 73:2009, definition 3.3.1.2]
    - Note 1 to entry: Internal context can include:
    - – governance, organizational structure, roles, and accountabilities;
    - – policies, objectives, and the strategies that are in place to achieve them;
    - – the capabilities, understood in terms of resources and knowledge (e.g., capital, time, people, processes, systems, and technologies);
    - – information systems, information flows and decision-making processes (both formal and informal);
    - – relationships with, and perceptions and values of, internal stakeholders;
    - – the organization's culture;
    - – standards, guidelines, and models adopted by the organization; and
    - – form and extent of contractual relationships."

Foundational Definitions: Accuracy, Precision, Certainty, and Robustness

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

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

- ***Accuracy:*** 'how close the measured result is to the actual result" (Capra and Canale 1998). In addition: "The accuracy of an analytical procedure expresses the closeness of agreement between the value which is accepted either as a true conventional value or an accepted reference value and the value found. This is sometimes termed ***trueness***" (Teasdale et al. 2017).
- ***Precision:*** "how two measurements agree with each other regardless of the 'accuracy'" (Capra and Canale 1998). The quote is: "The precision of an analytical procedure expresses the closeness of agreement (degree of scattering) between a series of measurements obtained from multiple sampling of the same homogeneous sample under the prescribed conditions. Precision may be considered at three levels: ***repeatability***, ***intermediate precision,*** and ***reproducibility***. Precision should be investigated using homogeneous, authentic samples. However, if it is not possible to obtain a homogeneous sample, it may be investigated using artificially prepared samples or a sample solution. The precision of an analytical procedure is usually expressed as the ***variance***, ***standard deviation,*** or ***coefficient of variation*** of a series of measurements" (ICH 2005).
- **Bias (also referred to as Inaccuracy):** "is defined as systematic deviation from the truth" (Capra and Canale 1998). In this context, it is very different from a more general dictionary definition, such as "an attitude that always favors one way of feeling or acting especially without considering any other possibilities" (Merriam-Webster 2004). This term creates confusion due to the difference in scientific and popular definition.
- ***Uncertainty (Imprecision):*** "on the other hand, refers to the magnitude of the scatter" (see Certainty) (Capra and Canale 1998).
- ***Certainty:*** "[A] parameter, associated with the result of a measurement that characterizes the dispersion of the values that could reasonably be attributed to the [thing being measured]" (JCGM/WG1 2008). Is generally a statement of confidence in a measurement? Further from that definition, "The parameter may be, for example, a standard deviation (or a given multiple of it), or the half-width of an interval having a stated level of confidence" (NIST 2018). A general dictionary definition is "1. Fixed, settled, 2. Of a specific but unspecified character, quantity, or degree, 3. Dependable, reliable, indisputable, etc." (Merriam-Webster 2004).

- ***Robustness:*** "The robustness of an analytical procedure is a measure of its capacity to remain unaffected by small, but deliberate variations in method parameters and provides an indication of its reliability during normal usage" (ICH 2005).

It is usually helpful to provide a case study to explain concepts, definitions, and, most importantly, how the terms relate to each other. Of course, without a methodical and thorough review, accuracy and precision cannot be judged. What can be judged is the method and process to gather data (Re., seeking many, varied sources and considering insight and patterns) in relation to what is known about the overall data set (Re., all types of food fraud).

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

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

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

Sidebar: *Appropriate Precision, Accuracy, Certainty, and Presentation of Findings*

Albert Einstein is reported to have said: "everything can be counted, but not everything counts." This statement applies to food fraud prevention both in the evaluation of the underlying data sets and the subsequent assessments. Judgments of the source and type of information (e.g., raw data, information, and then more advanced and formally defined intelligence) are covered in more detail in the Criminology chapter. A series of incidents are provided that contribute to very important insights into the fraud opportunity, and the final reports should take into consideration the nature of the underlying data. For example, a wide range of statements of the economic impact of counterfeiting and piracy are presented with high-level statistical analysis but based on an underlying assumption of all counterfeiting and piracy in the range of "5 to 7 percent of world trade" (Spink and Levente Fejes 2012). The high-level statistics were conducted on a data set with a very informal and qualitative foundation. This statement could be considered "excessive precision."

Describing the Nature of the Data

Further, to describe the data and analytics in more detail, there is the "5 V's of Big Data"—or sometimes these range from 4 to 7 and are summarized here (McAfee and Brynjolfsson 2012; Schniederjans et al. 2015; Haan et al. 2015; Meehan 2016; Sivarajah et al. 2017):

The 5 V's of Big Data

1) ***Volume:*** the amount of data. "Big Data" is judged in terabytes or above.
    - For example, how much information is in the data set, such as the number of food fraud incidents?
2) ***Velocity:*** The speed of data collection with Big Data defined in real-time or near real-time.
    - For example, how recently is information collected, and how they would include recent incidents? For example, is the entire data set reviewed and updated at least monthly, weekly, daily, hourly, etc.)?
3) ***Variety:*** a range of forms, including pictures, text messages, GPS signals, sensor readings, etc.
    - or example, how many different data sources are used, including in how many languages?
4) ***Veracity:*** the trust in the accuracy, precision, and certainty as well as if the data set is representative of the entire event.
    - For example, how complete is the data set in covering all problems in the real world and not just "everything we could find"?
5) ***Value:*** this is a rough judgment of the actual usefulness of the data set to address the specific question or the thoroughness recommendation based on this data set. • For example, how much more or other information would need to be collected to make a final decision such as recalling a product, putting a product on hold to conduct authenticity tests, canceling a supply contract, or contacting a government agency to report suspicious activity?

For another perspective on "data analytics" and the "V's of Big Data," consider the US National Institute for Standards and Testing (NIST) report on the "Big Data Interoperability Framework"(NIST 2015). The NIST reference is especially important due to the formal and authoritative role of the influence on US laws and integration to international standards such as ISO.

The NIST report expands the "V's" list and provides more detail on the veracity term:

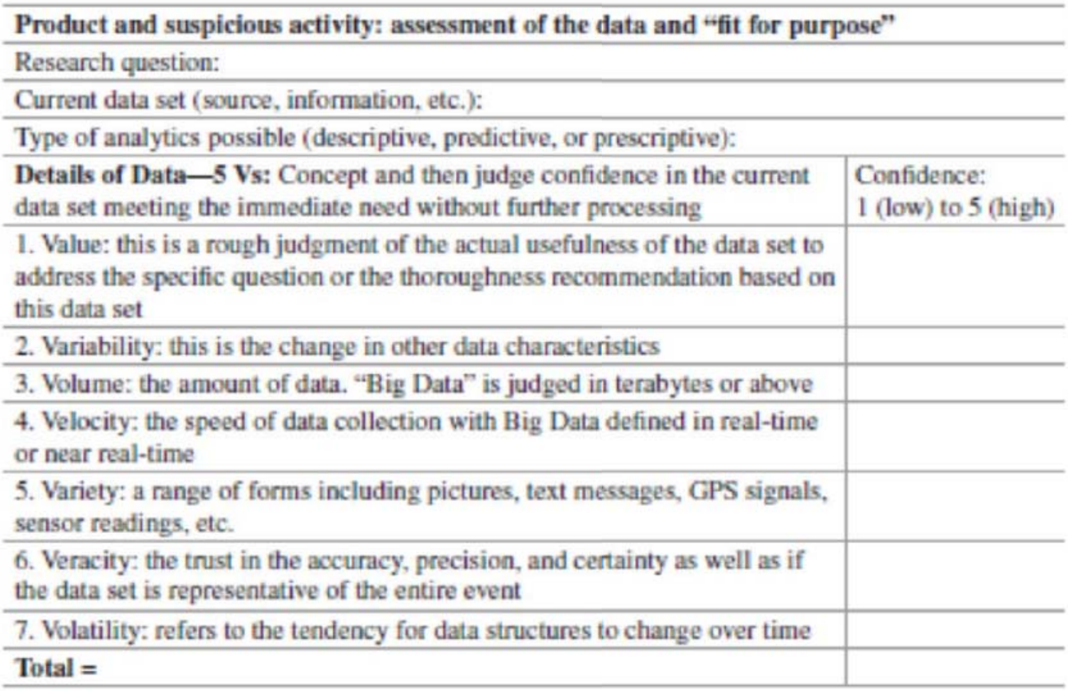
1. ***Value*** refers to the inherent wealth, economic and social, embedded in any data set (i.e., the value of the analytics to the organization, also sometimes referred to as ***validity*** [i.e., appropriateness of the data for its intended use]).
2. ***Variability*** refers to the change in other data characteristics.
3. ***Variety*** refers to data from multiple repositories, domains, or types.
4. ***Velocity*** refers to the rate of data flow.
5. ***Veracity*** refers to the accuracy of the data.
6. ***Volatility*** refers to the tendency for data structures to change over time (i.e., the tendency for data structures to change over time).
7. ***Volume*** refers to the size of the data set.

One of the most important concepts for the food fraud prevention application is veracity, so more detail is provided here:

> " ***Veracity*** refers to the completeness and accuracy of the data and relates to the vernacular 'garbage-in, garbage-out' description for data quality issues in existence for a long time. If the analytics are causal, then the quality of every data element is extremely important. If the analytics are correlations or trending over massive volume datasets, then individual bad elements could be lost in the overall counts, and the trend will still be accurate. As mentioned in Section 2.2, many people debate whether "more data is superior to better algorithms," but that is a topic better discussed elsewhere." (NIST 2015)

The "V's of Big Data" provides a framework for explaining the nature of a dataset.

Table 16.1 Evaluation of the value of data regarding data analytics: types of analytics and V's of Big Data (



Product and suspicious activity: assessment of the data and "fit for purpose"	
Research question:	
Current data set (source, information, etc.):	
Type of analytics possible (descriptive, predictive, or prescriptive):	
Details of Data—5 Vs: Concept and then judge confidence in the current data set meeting the immediate need without further processing	Confidence: 1 (low) to 5 (high)
1. Value: this is a rough judgment of the actual usefulness of the data set to address the specific question or the thoroughness recommendation based on this data set	
2. Variability: this is the change in other data characteristics	
3. Volume: the amount of data. "Big Data" is judged in terabytes or above	
4. Velocity: the speed of data collection with Big Data defined in real-time or near real-time	
5. Variety: a range of forms including pictures, text messages, GPS signals, sensor readings, etc.	
6. Veracity: the trust in the accuracy, precision, and certainty as well as if the data set is representative of the entire event	
7. Volatility: refers to the tendency for data structures to change over time	
Total =	

Figure 9: <TITLE>

8.2.1 Sidebar: The Black Swan: Experience versus Expertise

When a new food fraud article or interview is published, there often many people who say, "oh, I've been studying this topic for years." Do they have "experience" or "expertise"? If they're such experts and been working on this for so many years, then why is food fraud still a problem?

If you were leading a project to protect a bank, would you rather hire a bank manager who has "experience" being robbed or someone with "expertise" NOT being robbed? From "The Black Swan," author Taleb would define this as two terms that will be defined below, which are the "empty-suit problem" and "epistemic arrogance" (Taleb 2007). Some key definitions help provide insight on this question (the food fraud prevention application is added for several of the key terms) (Taleb 2007):

- ***Black Swan blindness:*** The underestimation of the role of the Black Swan and occasional overestimation of a specific one.
    - For food fraud prevention, this would be focusing on preventing a recent incident such as melamine or horsemeat and basically ignoring trends that may identify a new "fraud opportunity."

- ***Black Swan ethical problem:*** Owing to the nonrepeatable aspect of the Black Swan, there is an asymmetry between the rewards of those who prevent and those who cure.
  - For food fraud prevention, this would be the post-incident focus on the detection of the specific incident rather than focusing on the root cause and general vulnerability reducing control systems.
- ***Confirmation error*** (or ***platonic confirmation*** or ***confirmatory bias***): You look for instances that confirm your beliefs, your construction (or model)—and find them.
  - For food fraud prevention, this could be relying heavily on a published data set to be representative of all vulnerabilities.
- ***Empty-suit problem*** (or "expert problem"): Some professionals have no differential abilities from the rest of the populations but, for some reason, and against their empirical records, are believed to be experts.
  - For food fraud prevention, some professionals rely on their previous experience as an expert and have not reviewed new insight or methods. (It is amazing to hear absolutely positively incorrect statements made by industry experts—but the statements are made with high confidence.)
- ***Epistemic arrogance:*** Measure the difference between what someone actually knows and how much they think they know. An excess will imply arrogance and a deficit of humility. An epistrocrat is someone of epistemic humility, who holds their own knowledge in greatest suspicion.
  - For food fraud prevention, this could be a professional who has worked in food adulterant detection, and there is a belief that the food fraud prevention, opportunity reducing countermeasures, and control systems are from within their area of expertise (e.g., a food scientist who applies food safety microbiological prevention techniques to the human criminal adversary).
- ***Gray Swan*** (Mandelbrotian): Black Swans that we can somewhat take into account—earthquakes, blockbuster books, and stock market crashes—but for which it is not possible to completely figure out the properties and produce precise calculations or probabilities.
  - For food fraud prevention, the reality is that almost every single incident is a "Gray Swans" with an inevitability or warning signs. The incidents may even be "White Swans" if we assume they will eventually occur. Earthquakes do occur. Depending on the geographic location of your building, you will take more or fewer precautions.

- ***Ludic fallacy*** (or uncertainty of the nerd): The manifestation of the Platonic fallacy in the study of uncertainty, basing studies of chance on the narrow world of games and dice. A-Platonic randomness has an additional layer of uncertainty concerning the rules of the game in real life. The bell curve (Gaussian), or GIF (Great Intellectual Fraud), is the application of the ludic fallacy to randomness.
  - For food fraud prevention, this could be when a food safety or risk scientist applies statistical methods to a data set that is not appropriate or that is incomplete. For example, the most complex statistical analysis is usually based on the underlying assumptions of "5 to 7 percent of world trade" (Spink and Levente Fejes 2012).
- ***Narrative fallacy:*** Our need to fit a story or pattern to a series of connected or disconnected facts. The statistical application is data mining.
  - For food fraud prevention, this could be addressing the food fraud problem with current data sets or within current countermeasures systems. This could include food fraud being addressed in food safety early warning systems.
- ***Reverse-engineering problem:*** It is easier to predict how an ice cube would melt into a puddle than, looking at a puddle, to guess the shape of the ice cube that may have caused it ("the melting ice cube"). The "inverse problem" makes narrative disciplines and accounts (such as histories) suspicious.
  - For food fraud prevention, there are sometimes data sets that use themselves to validate the model (in sometimes unintentional or ignorance of circular references). For example, predicting the type of food fraud once fraud has been identified—the primary challenge is not really what type of fraud is occurring but to figure, first, if fraud is occurring. Another example is to use a known data set to create a model and then demonstrate the accuracy and precision by running examples from that data set.[5]

Others include:

- ***Frequency*** vs. ***probability:*** "Overconfidence is less significant when the problem is expressed in frequencies as opposed to probabilities." This also applies to vulnerabilities rather than risks or a probabilistic risk assessment.

[5] Specifically for food fraud – while the presenters, conferences, and dates will not be revealed – this has occurred numerous times.

- ***Lack of awareness of ignorance:*** "In short, the same knowledge that underlies the ability to produce correct judgment is also the knowledge that underlies the ability to recognize correct judgment. To lack the former is to be deficient in the latter".
- ***Overconfidence:*** "Overconfidence can be influenced by item difficulty; it typically diminishes and turns into under-confidence in easy items."
- ***Randomness as incomplete information:*** Simply, what I cannot guess is random because my knowledge about the causes is incomplete, not necessarily because the process has truly predictable properties.
- ***Retrospective distortion:*** Examining past events without adjusting for the forward passage of time. It leads to the illusion of posterior predictability.
- ***Uncertainty of the deluded:*** People who tunnel on sources of uncertainty by producing precise sources like the great uncertainty principle, or similar, less consequential matters, to real-life, worrying about subatomic particles while forgetting that we can't predict tomorrow's crises.
- ***The Problem of Induction:*** "Things cannot be known with perfect certainty because their causes are infinite."

A new appreciation for our assumptions or bias is helped when stepping back and reviewing broader risk assessment concepts such as the Black Swan definitions.

[This is the end of the excerpt from Spink (2020). (ref BFF)]

8.2.2 Data Analytics, Big Data, and Business Statistics

Risk management, quality control, and general business analysis are based on data. While "the numbers don't lie," they're often factors that lead the numbers that were gathered to be incomplete information, or somehow nonsensical information for the question that is being asked. Two key concepts are (1) "look at your data" and then consider "where your data came from." [24] Even the way data was collected is important such as from observation or experimentation. Beyond that, to understand the underpinning of the data and trends to establish if "statistical inference" (your conclusion based on considering the probability and likelihood of a conclusion based on the data set you are analyzing) is "causal or casual" or that "association does not imply causation." For example, your data set may conclude that "every Tuesday it rains in your town." Unless it is found that there is a weather pattern or physical geography feature that consistently creates environmental conditions every seven days that lead to the atmosphere becomes saturated with water vapor to the extent that it condenses and precipitates (a cause of why something happens and then the causal effect is the reaction to that event – it rained each Tuesday because of the cycle of the weather pattern), then it is just due to a casual correlation of the data that is assessed (it just happens that when the test was conducted on a Tuesday that it happened to rain – the fact that the day of the week was Tuesday is NOT a reason why it rained). In business planning, these are key concepts that can lead to very costly decisions if the problem is not clearly understood and analyzed.

"***Statistics*** is the science of collecting, organizing, and interpreting numerical facts, which we call data." [24] "The goal of statistics is to learn from data. [...] But to learn from data, we must do more than calculate and plot because data are not just numbers; they are numbers that have some context that helps us learn from them." [...] Think about the context and state your conclusions in the specific problem setting of the problem. As you are learning how to do statistical calculations and graphs, remember that the goal of statistics is not calculated for its own sake, but gaining understanding from the numbers." [24]

Statistics and probability grew from mathematics and prediction to help guide decisions such as is done in business. "The business landscape has become increasingly dominated with teams that focus on "business analytics," "predictive analytics," "data science," and "big data." [24] The set of data has several factors including "***cases*** are the objects described by a set of data (cases may be customers at a pizza restaurant)," "***labels*** are special variables used in some data sets to distinguish the different case (labels may be the type of pizza ordered)," "***variables*** are a characteristic of the case (variables might be the time of day that the pizza is ordered)," and "different cases can have different ***values*** for the variable (values might be the number of the specific type of pizza order)." "A ***categorical variable*** [or qualitative] places a case into one of several groups or categories." "A ***quantitative variable*** takes numerical values for which arithmetic operations, such as adding and averaging, make sense." A ***parameter*** is a number that describes populations. A parameter is a fixed number, but in practice, we do not know its value. The entire group of cases that we want to study is called the ***population***. A ***sample*** is a subset of the population for which we collect data).

The data assessment as several factors are important: [24]

- "The design of a study is ***biased*** if it systematically favors certain outcomes.
- A ***simple random sample (SRS)*** of size 'n' consists of 'n' cases from the population chosen in such a way that every set of 'n' cases has an equal chance to be the sample actually selected."

- ***"Bias*** concerns the center of the sampling distribution
  - The ***distribution***of a variable describes what values the variable takes and how often it takes these values.
- A statistic used to estimate a parameter is an ***unbiased estimator*** of the mean of its sampling distribution is equal to the true value of the parameter being estimated.
- The ***variability of statistics*** is described by the spread of its sampling distribution. The spread is determined by the sampling design and the sample size. Statistics from larger probability samples have smaller spreads (a ***statistics*** is a number that describes a sample, but it can change from sample to sample. We often used a statistic to estimate an unknown parameter).
- The ***margin of error*** is a numerical measure of the spread of a sampling distribution (the ***sampling distribution*** of a statistic is the distribution of values taken by the statistic in all possible samples of the same size from the same population). It can be used to set bounds on the size of the likely error in using the statistic as an estimator of a population parameter.
- ***To reduce bias***, use random sampling. When we start with a list of the entire population, simple random sampling produces unbiased estimates – the values of a [statistically representative sample] neither consistently overestimate nor consistently underestimate the value of a population parameter.
- ***To reduce the variability*** of statistics from a [simple random sample], use a larger sample. You can make the variability as small as you want by taking a large enough sample."
- ***"Anecdotal evidence*** is based on haphazardly selected cases which often come to our attention because they are striking in some way. These cases need not be representative of any larger group of cases."
- "In a ***completely randomized*** experimental design, all the subjects are allocated at random among all the treatments.

A key focus for risk management is how the information is gathered, the level of trust of the results, and then how the effort helps inform a specific decision. The less additional processing or action needed, the more valuable the data and the risk assessment. The types of "data analytics" are descriptive, predictive, and prescriptive. "It is critical not to overstate utility of the results of an assessment such as an 'impression of excessive precision.'"(Spink et al. 2019) Descriptive analytics is very valuable, but not if a customer is expecting a prediction."

There are three types of analysis or analytics:

Types of Data Analytics (Schniederjans et al. 2015)

- ***Descriptive Analytics:*** This is beyond a list of events or historical past probabilities. This term is defined as: "A simple statistical technique that describes what is contained in a data set or database." "To identify possible trends in large data sets or databases," e.g., descriptive statistics such as averages or standard of deviation, charts, graphs, sorting methods, or lists (Schniederjans et al. 2015)."
- ***Predictive Analytics:*** Apply statistical modeling to not only interpolate the history from the past but consider dependent and independent variables to predict future occurrences. This term is defined as: "Advanced statistical, information software or operations research methods to identify predictive variables and build predictive models to identify trends and relationships not readily observed in a descriptive analysis" (Schniederjans et al. 2015). "To build predictive models designed to identify and predict future trends" [e.g., ANOVA and multiple regression analysis].
- ***Prescriptive Analytics:*** Build upon predictive analytics assessment of future events to decide and apply resources that mitigate consequences, e.g., linear programming and decision theory (Schniederjans et al. 2015).

If there is not a lot of information or trust in the result, this can still help by offering a "risk-informed" decision. If there is a lot of information that is trusted, then a business decision may be able to "risk-based" automated decision.