



September 30, 2024

National Organic Standards Board
Handling Subcommittee
USDA-AMS-NOP

Docket: # AMS-NOP- 24-0023

RE: Risk-based Certification Discussion Document

Dear NOSB CAC Subcommittee,

Thanks for reaching out to organic stakeholders to discuss the important role of risk-based certification.

Risk-based oversight is an area of particular interest for Strengthening Organic Systems (SOS). Our business was established with the goal of supporting supply chain integrity. The timing of the launch of SOS was intentionally aligned with Strengthening Organic Enforcement (SOE). Risk-based oversight is an important tool and opportunity for fraud deterrence and prevention in the organic sector and it can lead to a more efficient use of resources and reduce the burden on low-risk operations.

Who is SOS?

Strengthening Organic Systems (SOS), LLC was founded to strengthen the resilience and overall integrity of organic systems and global organic supply chains. Our goal is to assure authenticity of organic products, protect organic businesses from organic fraud, and maintain consumer confidence in the USDA organic seal. As long-time leaders and regulatory experts in the organic space, SOS is excited to continue to support NOSB in its purpose to “assist in the development of standards for substances to be used in organic production and to advise the Secretary on any other aspects of the implementation of OFPA.”

SOS offers the following context and response to NOSB-posed questions about risk-based certification:

Importance of risk-based certification and oversight

Risk based certification, while not a new idea, can be difficult to implement within a process-based standard. SOS has a unique perspective in the SOE implementation era, having seen the certification process from both the enforcement/certifier side, and at the operation level where we work to support compliance and prevent fraud. SOS has been spending a considerable amount of time assessing opportunities to apply risk-based certification and operation level controls, including publishing a recent blog article on the topic, titled [How Risk-Based Certification Supports Fraud Prevention](#).

Certification carries a heavy administrative process burden. Operation paperwork review occurs three times at the certifier level during annual certification: 1) at application or renewal; 2) at inspection; and 3) post-inspection for a certification decision. Physical audit of an operation is performed at inspection, which is commonly the sole opportunity an operation physically interacts with their certifying agent. Organic System Plans (OSP), required by the regulation, exhibit varying degrees of length and complexity depending on the certifier and the nature of the operation. The primary expenditure for certifying agents is personnel - highly qualified individuals trained to

evaluate compliance of one of the most rigorous process-based voluntary certification categories under US Federal Law. Add this to the breadth and complexity of the organic supply chain, inclusive of all agricultural products, including food, fiber/textiles, personal care, dietary supplements, pet food, and new sectors as they develop. This complexity underscores the challenge certifiers encounter in determining the appropriate application of a risk-based approach.

While the complexity of the issues makes a structured approach like a decision tree or set instructions for risk assessment seem appealing, it is precisely this complexity that necessitates a reliance on comprehensive training, familiarity with vulnerability assessments, risk assessments and fraud prevention, and a deep understanding of risk-based certification concepts. These elements, coupled with robust organizational direction and prioritization within a well-defined schedule, are crucial for a successful risk-based certification approach.

Questions to stakeholders:

1. *How does your organization define risk?*

SOS Response:

Risk has a longstanding and germane understanding. Miriam Webster Dictionary defines risk in two definitions: 1. : *possibility of loss or injury* : *peril*. 2. : *someone or something that creates or suggests a hazard*.

SOS recommends consideration of existing risk definitions in the US agriculture and food sector as they relate to food defense, food safety, and food fraud prevention. We do not recommend creating new or unique risk definitions – and therefore we are not offering any novel or unique definitions. Our suggestions below utilize the same food fraud prevention resources that were used to build the Organic Trade Association’s Organic Fraud Prevention Guide and associated Organic Integrity Learning Center (OILC) trainings on inspecting an organic fraud prevention plan. The connection between a vulnerability and a risk is important, because the first step in identifying fraud risk is understanding fraud vulnerabilities. From there, one can carry out a risk-assessment and determine the likelihood of a fraud event occurring and its impact. The assessment outcome then informs prioritization and resource allocation.

According to [this FDA resource](#), The term “risk profile” provides an opportunity to apply an existing model to organic certification: *Risk profiles are comprehensive descriptions of a hazard, the supply and consumption chains of the foods it affects, and potential interventions. These types of risk assessments don’t include models that estimate outcomes and comparisons of interventions.*

[Dr. John Spink](#) provides expansive resources for definitions in his book titled “Food Fraud Prevention – Introduction, Implementation and Management”- which is a valuable resource for establishing a common definition with respect to fraud prevention, risk assessment, and organic compliance.

During the early stages of food fraud prevention research, it was discovered that risk and vulnerability had been formally defined as separate concepts in formal publications such as by the International Standards Organization (ISO) or the U.S. National Institute of Standards and Technology (NIST). They are related topics but explicitly and implicitly different.

- **Risk:** an uncertainty of an outcome that is assessed in terms of likelihood and consequence (ISO, 2007a; NIST, 2002; CNSI, 2010; DHS, 2013). Often, the consequence is subdivided into other factors such as onset, severity, or other. Risk is based on factors such as the threat's probability and vulnerability susceptibility (NRC, 2009). In other applications, it is an unwanted outcome (DHS, 2008; Codex Alimentarius, 2014, 21 CFR 50 (A) (.3)(k), Merriam-Webster, 2004).
- **Vulnerability:** a weakness or flaw that creates opportunities for undesirable events related to the system ("system design") (ISO, 2007a; ISO 2002; ISO, 2012; DHS, 2013; NIST, 2011; CNSI, 2010; NRC, 2009; COSO 2014; Merriam-Webster, 2004).

The expansion from just risk to vulnerability was key in the early development of the food fraud standards – including the landmark fraud prevention work by the Global Food Safety Initiative (GFSI, and the related standards from BRC/BRCGS, IFS, SQF, FSSC 22000, and others). This expanded focus on vulnerability was key to enabling the early adoption of the food fraud prevention programs. It was also efficient to focus on the root causes.

The [Organic Trade Association Fraud Prevention Guide](#) is an important reference for organic fraud prevention best practices and corresponding definitions. The guide is based on Dr. Spink's fraud prevention work and the GFSI fraud prevention model and provides important definitions that distinguish a "vulnerability" from a "risk."

The Guide states: "A vulnerability is a weakness or gap in protection efforts." A "Risk" on the other hand is the "potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability. Risk is the intersection of assets, threats, and vulnerabilities".

What is the key difference? Risk assessment evaluates the probability and impact of a risk event, while vulnerability assessment focuses on identifying and addressing weaknesses that could lead to such events.

Food fraud, or in our case "organic fraud" is difficult to estimate and quantify, so we use the word 'vulnerability' rather than a 'risk.' A risk is something that has occurred and will occur again. A risk can be quantified using existing data. A vulnerability is a weakness that can be exploited. A fraud vulnerability can lead to a risk. The difference between the two and how they interrelate is important if we want to optimize a risk-based certification approach.

- **Vulnerability assessment** identifies weaknesses in the supply chain that could be exploited for fraud, such as gaps in traceability or record-keeping. This helps to pinpoint areas where preventive measures are most needed.
- **Risk assessment** evaluates the likelihood and potential impact of specific fraud risks, allowing for prioritization of resources and efforts towards the most significant threats.

By combining these two assessments, operations (and certifying agents) can develop a targeted and proactive approach to fraud prevention, addressing the most critical vulnerabilities and risks in a prioritized manner. This ensures that resources are allocated efficiently and effectively to safeguard the integrity of organic products and protect consumer confidence.

2. *Would it be valuable for the definitions listed above (Risk-based oversight, Risk management, Risk, Vulnerability) to be included at §205.2 Terms Defined?*

SOS Response:

It is appropriate to define these terms, although SOS recommends the language define “risk” more specifically as, “organic fraud risk assessment,” “organic risk-based oversight,” and “organic risk management.” We also recommend the term “Vulnerability Assessment.”

“Vulnerability Assessment” is the step aimed at reviewing and assessing various factors that create vulnerabilities in a supply chain (i.e. weak points where fraud has the greater chances to occur).

“Organic Fraud Risk Assessment” is a systematic process that evaluates an organization’s risk of fraud, including its likelihood and potential impact.

“Organic Risk-Based Oversight” is a regulatory approach that prioritizes the allocation of resources and oversight activities based on the level of risk associated with different organic operations.

“Organic Risk Management” refers to making decisions on how to prevent, reduce or minimize risks. It includes mitigation strategies, preventive measures, and implementation.

3. *Are there other definitions that would be beneficial to include at §205.2 Terms Defined besides those listed above? Is it important that all certifiers use the same risk criteria to evaluate certifier operations? Why or why not?*

SOS Response: The terms and definitions outlined in the previous question would provide adequate framework for common understanding of the concept of risk-based certification. Regarding using the same risk criteria, this is an important question and has some important nuance that needs to be acknowledged and discussed. The **process of identifying and establishing risk** *should* follow a consistent format across certifying agents. We recommend a unified approach is established for **evaluating risk** across certifying agents – with respect to their offices, clients, and areas of priority.

Alternately, **risk criteria** should be established within each certifying agent based on conditions present, including internal conditions, geographic and cultural clientele type and factors, and marketplace conditions and factors. Applying the same risk criteria to the variety of operations and certifying agents is not supported, but establishing a uniform framework for establishing risk factors is supported.

4. *What other resources (e.g. trainings, models, certifications/credentialing program) are currently available that would help an organization become more proficient at risk-based oversight and/or risk evaluation?*

SOS Response: Risk assessment across certifying agents must provide for unique conditions of different markets and client base. However, we would propose that there are some foundational commonalities for risk assessment. The [Cressey Fraud Triangle](#) outlines that three conditions need to be present for fraud to occur, and only one needs to be absent for fraud occurrence to be reduced or eliminated:

- **Pressure/Incentive**
 - For example, the organic market often commands premium prices, creating a financial incentive for fraudsters to misrepresent non-organic products as organic. Additionally, factors like supply shortages or increased demand can further intensify the pressure to commit fraud.
- **Opportunity**
 - For example, complex supply chains with multiple handlers and intermediaries can create opportunities for fraudsters to introduce non-organic products into the organic supply chain without detection. Weaknesses in traceability systems and inadequate oversight can also increase the chances of fraud going unnoticed.
- **Rationalization**
 - For example, fraudsters may rationalize their actions by believing that organic fraud is a victimless crime or that they are simply taking advantage of a system that is easy to manipulate.

Resources included in the discussion about the definition of Risk, including the OTA Organic Fraud Prevention Guide and Dr. John Spink’s website “Food Fraud Think Tank” are valuable resources for understanding vulnerability assessment, risk assessment, oversight, and evaluation. Food fraud provides a well-established and valuable resource pool for organic fraud prevention, including many fraud vulnerability factors that can help inform a risk-based approach to verifying compliance.

5. *What are the unintended consequences that could arise from using a risk-based oversight approach?*

SOS Response: Risk-based certification has the potential risk of deprioritizing areas of lower risk, losing the deterrent benefit of comprehensive oversight, and potentially creating new vulnerabilities. This can be combatted through a systematic approach to each season and market’s risk areas, identifying prioritization areas, and ensuring areas of lower risk are not completely ignored, while areas of higher risk are adequately monitored. In our organic seed usage comments, SOS proposed a systematic review approach for commercial availability, arguably a lower risk area for enforcement, since use of a nonorganic alternative is technically sanctioned, but verification of compliance is still important to deter lax or “in concept only” compliance. In this example, we suggest that on a 3-year cycle, commercial availability is prioritized for the certification cycle and applied to businesses where this requirement applies.

While this approach would require initial organization, including evaluation of the scope of businesses, applicable activities, and identification of frequency of prioritization, once accomplished, this would drastically reduce the administrative burden created by paperwork and comprehensive annual review.

Some examples are supplied in the table below (example provided for a crop operation):

Topic	Identified Risk for 2024 Cycle	Determined review/prioritization frequency
Seed Sourcing (commercial availability)	Low risk to certification status, priority determined for compliance verification in 2024 (accreditation)	3-year prioritization (2024 priority) Review 20% of seed documentation (or all seed if less than 5 crops) for commercial availability compliance.
Inputs - high nitrogen fertilizer- operation is operating in both conventional and certified production	High Risk	Annual review, random or targeted sampling
Buffers	Low Risk (not a 2024 priority, due to 2023 prioritization)	Verify new field buffers at initial review, select a new field to verify – cross verify to confirm all fields have been reviewed on a 5-year cycle

6. *What other ways are there to reduce burdens on low-risk operations?*

SOS Response: Burden on low-risk operations is immediately reduced when an effective risk-based system has been implemented. Low-risk operations can be identified and prioritized for reduced oversight through a combination of factors, including:

- **Historical compliance:** Operations with a consistent track record of compliance and no history of violations can be considered low-risk.
- **Nature of the operation:** Certain types of operations, such as those with simple supply chains or low-risk products, may inherently pose a lower risk.
- **Risk assessment tools:** Using standardized risk assessment tools can help certifiers objectively evaluate various risk factors and prioritize operations accordingly.
- **Data analysis:** Analyzing data on past inspections, audits, and certifications can reveal patterns and trends that can inform risk assessments.

By considering these factors, certifiers can focus their resources on higher-risk operations, while still ensuring that all operations are compliant with organic standards.

7. *How can the community provide information to NOP and/or certifiers on acute risks?*

SOS Response: There are several opportunities to identify and point out acute risks:

- A) NOP has unprecedented access to data and information post SOE. Annual training serves to provide opportunities for prioritization, which informs certifier approach for the certification cycle.
- B) Operations are developing maps of their fraud vulnerabilities and assessing risk- through their organic fraud prevention plans. Certifiers can utilize this knowledge, expand identified vulnerabilities and prioritize risks in oversight.
- C) The marketplace has knowledge of areas of acute risks, and complaint processes can be effectively leveraged to draw attention to risk areas.



In closing, SOS advocates for increasing resources and the collective knowledge and application of risk-based systems in the organic certification space. An effective risk-based system avoids creating a systematic process that encourages routine. Rather, we propose that creating disruption and risk-based prioritization, that adapts and changes based on risk- achieves a superior oversight model that ensures fresh observation and opportunity to avoid routine or assumption.

We thank NOSB for its volunteer service and everyone's commitment to work on this important topic.

Respectfully submitted,

Gwendolyn Wyard
Founding Partner

Kim Dietz
Founding Partner

Johanna Phillips
Director, Business Development
& Technical Affairs

 GwenWyard@organicSOS.com
 503-798-3294
 Corvallis, OR

 KimDietz@organicSOS.com
 530-321-8996
 Chico, CA

 JPhillips@organicSOS.com
 208-576-2641
 Eagle, ID

