FAMI-QS®

The Quality and Safety System for Specialty Feed Ingredients

FAMI-QS CODE OF PRACTICE

FEED FRAUD PREVENTION AND DEFENCE MODULE

VERSION 1.0
2019-09-02

Feed fraud prevention and defence module

1. Introduction

Since 2004, the FAMI-QS Code of Practice provides requirements for implementing measures necessary to ensure feed safety and quality of products manufactured by processes, as defined by FAMI-QS. The text of the Code is designed to set out general requirements and is to be used as a tool for Operators to develop their specific procedures. The Code covers requirements on Good Manufacturing Practices, the HACCP System, continuous improvements to the design, management of operations and risks with a goal of maintaining feed safety and quality.

Recent scandals in the worldwide food and feed sector have highlighted the need to strengthen fraud prevention measures across the entire supply chain. Not only is this necessary to protect the health of consumers, but corporations and regulators both know that trust is the foundation upon which efficient, functioning markets are built. In addition, there is public concern that the food or feed sector is being used for intentional acts that could harm an individual or the public for ideological purposes (acts of terror).

The principles used for managing feed safety and quality as defined in the FAMI-QS Code of Practice have not been developed to routinely detect or mitigate feed fraud or terror attacks on an operator's systems or processes. For this reason, FAMI-QS has developed the feed fraud prevention and defence module. The ultimate goal of this feed fraud prevention and defence module is to ensure operators, adhering to the FAMI-QS Code of Practice, can implement an auditable system that demonstrates the Operator's ability to manage and effectively mitigate the risk of feed fraud and terror.

Compliance with the feed fraud prevention and defence module does not exonerate the Operator from meeting statutory or regulatory requirements in:

a) The country where the Operator is based;
b) The country where the final product, coming from FAMI-QS certified process is placed.

The FAMI-QS feed fraud prevention and defence module is a public document, whose contents can be followed freely by any operator. This module is not a stand-alone auditable document, but a module that is to be used in conjunction with the FAMI-QS code. Implementing and adhering to the feed fraud prevention and defence module is mandatory for operators choosing to participate in the FAMI-QS certification process. In the next update of the FAMI-QS, code version 6.0 the requirements of this feed fraud prevention and defence module will be integrated into the code.

How to read this document

The FAMI-QS feed fraud prevention and defence module includes:

Requirements: These are mandatory measures for operators adhering to the feed fraud prevention and defence module. The requirements are highlighted in grey text boxes.

Guidance: The guidance section, following the requirements, includes background information, additional explanation and methods to support operators with implementing the requirements.

2. Scope

This chapter helps operators to identify their products, according to the definitions within the scope of this feed fraud prevention and defence module.
The FAMI-QS feed fraud prevention and defence module is an integral part of FAMI-QS code. Operators wishing to obtain initial FAMI-QS certification against the FAMI-QS code must integrate the requirements of this module into its management system. Operators already holding an existing FAMI-QS certification must integrate the requirements of this module according to the transition period requirements published by FAMI-QS.

2.1. FAMI-QS code scope and the feed fraud prevention and defence module scope

This feed fraud prevention and defence module must only be used in conjunction with the FAMI-QS Code of Practice. It is mandatory for operators choosing to participate in the FAMI-QS certification process to implement this module. Operators need to make sure application and scope of the module are aligned with the scope as defined under chapter 2 of the FAMI-QS code.

Further requirements on defining the scope for feed fraud prevention and defence are defined in sections 6.1.2. and 7.1.2

3. Terms and definitions

The following terms and definitions are used in this module and associated documents:

Agent: A means or method used to exploit a vulnerability in a system, operation, or facility.

CARVER+ Shock analysis: Offensive targeting prioritization tool that has been adapted for use in the food sector. The tool can be used to assess the vulnerabilities within a system or infrastructure to an attack.

Corrective action: Action to eliminate the cause of a nonconformity and to prevent recurrence. *(ISO 22000:2018)*

Control Measure: any action and activity that can be used to prevent or eliminate a feed / food safety hazard or reduce it to an acceptable level. *(Codex Alimentarius and adapted)*

Critical Control Point (CCP): A step at which control can be applied, which is essential to prevent or reduce a feed/food safety hazard or to reduce it to an acceptable level. *(Codex Alimentarius and adapted)*

Cyber security: Protection of devices, services and networks — and the information on them — from theft or damage. *(National Cyber Security Centre)*

Facility: Physical premises of operator.

Flow chart: A diagram that shows step-by-step progression through a procedure or system especially using connecting lines and a set of conventional symbols. *(Merriam-Webster)*

Feed defence: Feed defence is the effort to protect feed from acts of intentional adulteration. *(Food and Drug Administration)*

Feed fraud: Feed fraud is a collective term used to encompass the intentional substitution, addition, tampering, or misrepresentation of feed, feed ingredients, or feed packaging; or false or misleading statements made about a product, for economic gain. (Spink, Moyer)

HACCP (Hazard Analysis and Critical Control Point) Programme: A system that identifies, evaluates, and controls hazards, which are significant for feed safety.

Incoming material: A general term used to denote raw materials delivered at the beginning of the production chain, including components or packaging materials

Likelihood: The state or fact of a feed fraud or defence risk being likely to occur.

Mitigation activities:, any activity that can be used to prevent or eliminate a feed/food fraud or defence risk or reduce it to an acceptable level.

Must: Compliance with a requirement that is mandatory for this module (obligation to follow the exact requirement as stated by this module).

Node: A point at which subsidiary parts originate or centre.

Non conformity: Non-fulfilment of a requirement. *(ISO 22000:2018)*

Operator: The natural or legal persons responsible for ensuring that the requirements of food/feed law are met within the feed business under their control. *(Regulation178/2002/EC and adapted)*

Process: Set of interrelated or interacting activities that transforms inputs to outputs. *(ISO 22000:2018)*

Product (final): Output that is a result of a process, and that will undergo no further processing or transformation by the organization**.** A product that undergoes further processing or transformation by another organization is a final product in the context of the first organization and a raw material or an ingredient in the context of the second organization (ISO 22000:2018). Any operators releasing raw materials or ingredients to the market without further processing should consider these as final products and treat as such according to the requirements of this module.

Raw material: Any material which enters the manufacturing process of the products covered by the FAMI-QS scope, including components or packaging materials, see '*Incoming Material*'.

Requirement: Need or expectation that is stated, generally implied or obligatory. *(ISO 22000:2018)*

Risk: A function of the probability of an adverse health effect and the severity of that effect, consequential to a hazard. *(Regulation 178/2002/EC)*

Risk appetite: the amount and type of risk that an organisation is willing to pursue or retain. *(A Risk Practitioners Guide to ISO 31000: 2018)*

Risk assessment: Means a scientifically based process consisting of four steps: hazard identification, hazard characterisation, exposure assessment and risk characterisation. *(Regulation 178/2002/EC)*

Subsystem: Part or activity within the Operator's overall production system.

TACCP: the combined activities of threat assessment and analysis and critical control points definition

Threat assessment: Activities to understand the exposure to threats (as an act of terror) in order to define and implement activities to reduce or mitigate the threats.

Traffic flow control: Activity to influence the flow of goods, people, vehicles, etc. with the objective to mitigate or reduce to an acceptable level the feed defence threats.

VACCP: the combine activities of vulnerability assessment and analysis and critical control points definition.

Vulnerability assessment: Activities to understand the exposure to vulnerabilities (as an act of feed fraud) in order to define and implement activities to reduce or mitigate the vulnerabilities.

4. Leadership

4.1. Leadership commitment

Top management must demonstrate leadership and commitment with respect to feed fraud prevention and defence management system. The Operator must ensure that leadership and commitment to feed fraud prevention and defence are integrated with leadership and commitment to the feed safety and quality management system as required in section 5.1 of the FAMI-QS code.

4.2. Responsibilities

Top Management must ensure that the responsibilities and authorisations for relevant roles within the feed fraud prevention and defence management system are assigned, communicated and understood within the organisation. The Operator must ensure that responsibilities and authorisations for relevant roles within the feed fraud prevention and defence management system are integrated with those responsibilities and authorisations for relevant roles within the feed safety and quality management system as required in section 5.2 of the FAMI-QS code. For feed fraud and defense management, responsibilities and authorisations may extend beyond the existing roles.

5. Feed fraud prevention and defence

FAMI-QS Code 6.0 refers in section 4.6 to: "Top management must ensure that a Feed Safety and Quality Policy is established, implemented and maintained. This Feed Safety and Quality Policy must include a policy to take the necessary actions for Feed Fraud Prevention". With this module, FAMI-QS introduces more detailed requirements to take actions to prevent feed fraud and feed terror threats (feed defence) and provides guidance on how to develop and maintain a system of feed fraud prevention to address identified risks. In addition, similar requirements and guidance is used to develop a system to prevent acts of terror (a feed defence system).

5.1. Understanding feed fraud and feed terror risks

Feed fraud and feed terror risks differ from feed quality and feed safety risks in that the action is intentional and the motivation is either economic gain or harm (see figure below). Regular feed safety and quality management systems do not sufficiently incorporate assessments and controls for intentional actions.
Acts of fraud or terror might have an impact on feed quality or feed safety, or a public health effect, or provide economic gains. As a result, these acts might be difficult to distinguish from fraud. However, for risk management purposes it is important that there is an intention that precedes either economic gain or harm. As a clear separation is not always possible, there might be overlaps in some cases. Figure 1 below provides clarification.

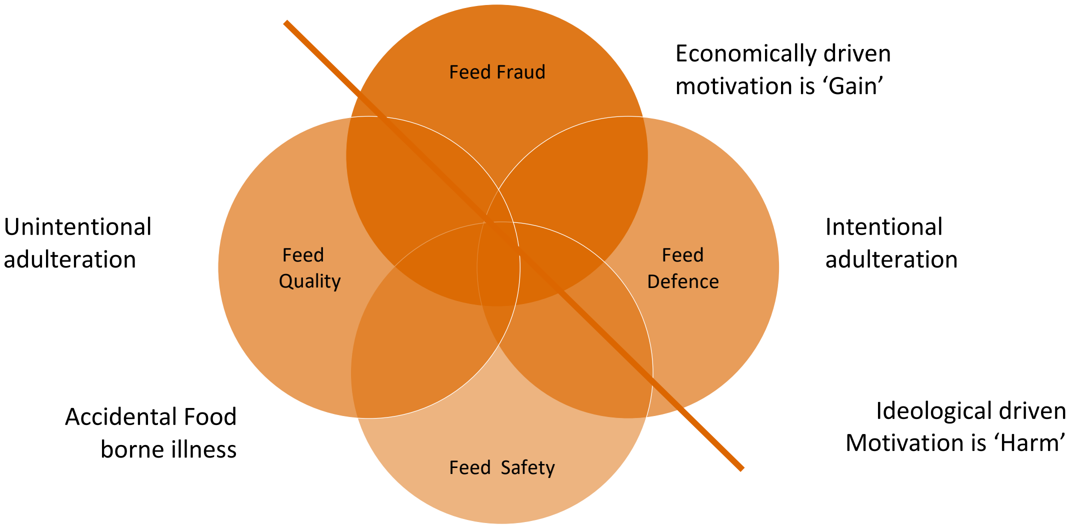

Feed Fraud
Economically driven motivation is 'Gain'
Unintentional adulteration
Feed Quality
Feed Defence
Intentional adulteration
Accidental Food borne illness
Feed Safety
Ideological driven Motivation is 'Harm'

Figure 1. Adapated by : Food risk types (adopted from GFSI Position Paper on Food Fraud 2014)

Forms of feed fraud

In essence, feed fraud is the intentional deception using feed for economic gain, which includes substitution, addition, dilution, tampering or misrepresentation of feed, feed ingredients or feed packaging; and includes false or misleading statements made about a product. These forms can be defined, amongst others as:

- Substitution: Replacement of a high value product (-component) for a low value product (-component) or dilution of a product.
- Addition: Adding non-permitted and unknown (or undeclared) substances to enlarge the quantity of the product;
- Counterfeiting: Concealment of lower quality of a product by intentional false labelling;
- Misrepresentation: the action or offence of giving a false or misleading account of the nature of something (e.g. a product).

Forms of feed terror (adopted from PAS 96:2017)

In essence, feed terror is the intentional deception using feed for ideological gain, which includes (amongst others):

- Malicious contamination: the act of deliberately contaminating feed by the use of microbiological, chemical or physical agents
- Extortion: the practice of obtaining money, property, or services from an individual or institution, through pressure.

6. Feed fraud prevention system

Feed safety management systems generally focus on the unintentional contamination of feed by known ingredients, pathogens, mishandling, or processing. Feed fraud, however, is an intentional act perpetrated for economic gain. The perpetrators' fraudulent ingredients and/or modifications are specifically engineered to evade the purchasers' quality assurance and quality control systems. Only perpetrators know which adulterant-substance has been manipulated and how. Moreover, the adulterants introduced by feed fraud are often unconventional substances that are not anticipated by feed safety management systems, and only become known after they have entered the supply chain. While the vast majority of reported feed fraud cases do not result in a threat to human health, acts of feed fraud can create a vulnerability when dangerous adulterant substances have been added or the product has been mishandled and, hence, become dangerous when consumed.

Three factors are important to understand the risk of fraud and how it can be controlled:

- Opportunity

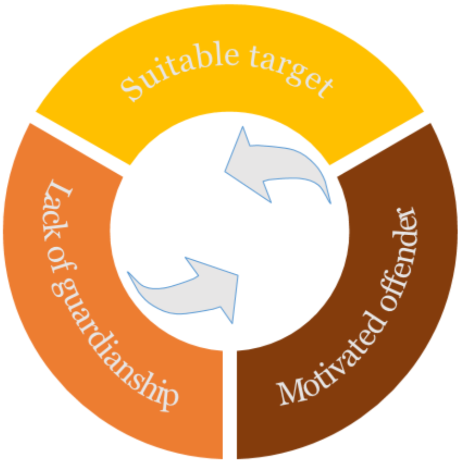
The opportunity to commit fraud, based on the content of and information related to the product, access to product or process, possibility to detect fraud and complexity of the supply chain. This includes the ability and the knowledge of how to perform the act, as well as the ability not to be caught.

- Motivation

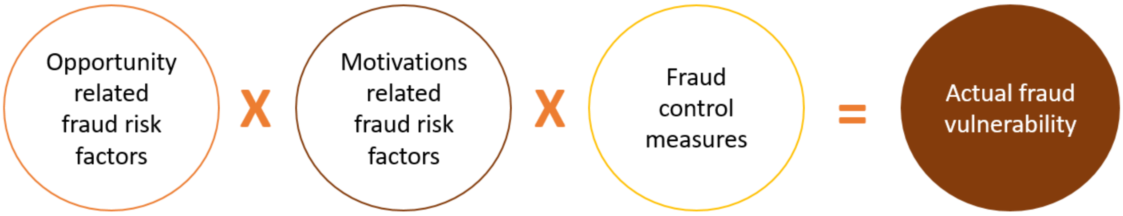
The motivation to commit fraud, based on potential benefit of fraudulent behaviour, financial pressure on operator/person or lack of supply, culture of corruption or fraud, and personal psychological motivation.

- Controls

The controls in place (or lack thereof) to prevent fraud: systems and measures in place within the company and its environment to mitigate risks.



The three factors relate to each other and influence the level of actual fraud vulnerability, see graph below:


Opportunity related fraud risk factors
X
Motivations related fraud risk factors
X
Fraud control measures
=
Actual fraud vulnerability

To determine the level of actual fraud vulnerability, operators must document and conduct an assessment, considering the opportunity, motivation and control factors. The Operator must install a feed fraud mitigation plan, which addresses the vulnerabilities as concluded from the assessment.

6.1. Feed fraud prevention system and its processes

Requirement

Operators must develop and implement a method to manage the feed fraud risk as described in sections 6.1.1 to 6.1.5.

6.1.1. Feed fraud prevention team

Requirement

The Operator must assign responsibilities for the feed fraud prevention system (vulnerability assessment and mitigation activities).
Performing a vulnerability assessment (as well as defining the Critical Control Points to mitigate them – a VACCP) must be a multi-disciplinary activity, bringing together the best available skills to address potential feed fraud risks 'vulnerabilities'). This must be done taking into account the limited complexity that smaller operators might face.

Guidance

It is suggested to have a feed fraud prevention team (VACCP team) in place with sufficient skills relating to fraud risks. As fraud risk are intentional, focus on economic gain and could be conducted internally as well as externally (by value chain partners, such as suppliers and buyers), it is important that the team ensures that knowledge of these topics is present in the team. Such (non-exhaustive) knowledge may include:

- supply chain or procurement;
- commercial or sales;
- quality and safety assurance
- operations
- finance
- internal audit

6.1.2. Scope the feed fraud prevention system

Requirement

The Operator must determine the scope of their feed fraud prevention system by conducting an initial assessment. The Operator must:

1. identify high risk business units and geographies, taking into consideration risks, economical value, reputational impact and nutritional value;
2. perform high level supply chain mapping and deliver an indication of high risk supply chains, suppliers and products;
3. develop a scope definition as input for the vulnerability assessment based on 1 and 2, determine sections, sites, product lines, business units involved in the assessment and define a process plan.

Guidance

For initial assessment, any method may be applied as long as the assessment addresses the topics identified in this section. The FAMI-QS template on feed fraud vulnerability assessment can support operators in conducting the scoping.

6.1.3. Performing vulnerability assessments

Requirement

The Operator must conduct a feed fraud vulnerability assessment based on the scope determined in 6.1.2. and document the results.

The vulnerability assessment approach must address the opportunities for feed fraud, motivations that fraudsters may have and consider the controls that may already exist in order to determine the current 'vulnerability to feed fraud' status. The approach must consider the scope of the feed fraud prevention system in order to apply the appropriate level of detail to the vulnerability assessment. Such could include considerations of:

1. addressing the vulnerabilities at product or product group level, including raw and packaging materials;
2. addressing the vulnerabilities at production process level;
3. addressing the vulnerabilities at country, regional or site-specific level.

Assessing vulnerabilities using the tools outlined in this paragraph could be supported by a system on data gathering about fraud risks. The Operator could use potential sources of information (e.g. public databases, websites, horizon scanning tools, industry working group or blogs) to support the assessment.

Guidance

The Operator performs vulnerability assessment along the lines of the following components:

Opportunities	Motivations	Controls
Availability of knowledge and technology to adulterate	Economic factors: Financial strains, level of competition; supply/demand and pricing ingredients/products, business strategy, economic health or conditions, special attributes or constituents determining value	Information system (mass balance, traceability)
Simplicity/complexity of adulteration	Cultural and behavioural factors: Personal gains or traits, ethical business culture, corruption level of country, victimization, criminal offences	Fraud monitoring system and verification of the system
Accessibility to the processing lines		Whistle blowing
Complexity and transparency of the supply chain and network		Ethical code of conduct
Detectability of feed fraud		Legal framework and enforcement
		Contractual requirements suppliers
		Integrity screening of employees, when allowed

The FAMI-QS template on feed fraud prevention will support operators in conducting the requirements of this section.

Other tools to support the vulnerability assessment are:

- PwC's/SSAFE's Food Fraud Vulnerability Assessment tool (Free): https://ffv.pwc.com/vsat/, or for an excel based version go to http://www.ssafe-food.org/our-projects/
- Food fraud database (former USP now Decernis) (subscription): https://www.foodfraud.org/

6.1.4. Analysing risks and defining risk boundaries

Requirement

The Operator must analyse the output of the vulnerability assessment, document the outcome of the analysis and decide on priorities, based on an evaluation of the level of vulnerability associated with each object of focus. The Operator must set risk boundaries, depending on the levels of vulnerability that are acceptable and unacceptable for the operation. Boundary setting must only be adopted were considered practical. For those levels of vulnerability that are deemed unacceptable, counter measures should be defined in terms of critical control points (see section 6.1.5).

Guidance

The FAMI-QS template on feed fraud prevention will support operators in conducting the requirements of this section.

6.1.5. Defining critical control points

Requirement

Using the outcome of the vulnerability assessment the Operator must define a set of preventive actions and controls to reduce the vulnerabilities to an acceptable level. This can include, but is not limited to, defining critical control points (CCP's). Based on the controls identified a mitigation plan based on CCP's must be developed.
The Operator must first perform a gap-analysis to assess if sufficient controls are already in place, and then extend the control framework.

Gap –analysis controls:

1. understand outcome of vulnerability assessment as performed under 6.1.3.;
2. review opportunities and motivations identified in light of the controls already in place;
3. identify any additional controls not in place;
4. determine (remaining) controls needed using the defined risk boundaries under 6.1.4.

Building the control framework:

1. identify control points critical to detect feed fraud (CCP's) from the vulnerability assessment, considering legal requirements and describe the control measures (mitigation measures);
2. define monitoring procedure (controls) for each CCP;
3. define anticipated corrective actions for each;
4. validate approach before implementation and verify effective implementation.

Guidance

Possible methods of control are (non-exhaustive):

1. Value chain profiling including:
    b. supplier risk profiling (understand its reputation, identify past issues with suppliers),
    c. regional risk profiling (country risks, region incidents, business culture),
    d. product risk profiling (history of incidents with products, known fraud cases),
    e. supply chain risk profiling (which is a mix of the initial three plus general supply chain complexity (e.g. number of companies between operator and the manufacturer);

Refer to the templates for further examples of controls.
The FAMI-QS template on feed fraud prevention will support operators in conducting the requirements of this section.

2. Audits/Certifications that include fraud prevention for the actual manufacturing facility.

3. Product integrity testing: such us Organoleptic and Microscopy evaluations, Near Infrared testing (NIR), Bulk Density, Powder Flow, X-ray fluorescence, Wet Chemistry Testing and Chromatography.

7. Feed defence system

FAMI-QS Code 6.0 refers in section 7.1 Establishment to "The Operator must assess if feed safety hazards may be expected to occur by potential acts of sabotage, vandalism or terrorism and must put in place adequate protective measures". This chapter specifically outlines the requirements to perform such an assessment and provides guidance on how to develop and maintain a system of feed defence to address these (terror) risks.

Managing risks related to feed terror requires operators to understand the threat of attacks (intentional acts) with ideological gain. This requires a systematic approach, focusing on the likeliness of such acts to occur as well as understanding its impact. From this understanding, a systematic approach to reducing the threats can be introduced to control the risks related to feed terror. These activities form the basis of "Threat Assessment Critical Control Point", a method that aligns with HACCP (as described in the FAMI-QS code) and VACCP (as described in chapter 6 of this module). By performing a threat assessment and determining the most vulnerable points in the infrastructure, the Operator can then focus available resources on protecting the most vulnerable points.

Several recognized methods support the scoping of the feed defence system such as BSI "PAS 96:2017 Guide to protecting and defending food and drink from deliberate attack" and FDA's "Carver + Shock Primer"
More information available on:

- https://www.bsigroup.com/en-GB/PAS-96/;
- https://www.fda.gov/food/fooddefence/fooddefenceprograms/ucm376791.htm

7.1. Defence system and its processes

Requirement

Operators must develop and implement a method to manage the feed defence risk as described in 7.1.1 to 7.1.5

7.1.1. Feed defence team

Requirement

Performing a threat assessment (as well as defining the critical control points to mitigate them) (TACCP) must be a multi-disciplinary activity, bringing together the best available skills to address potential terror risks 'threats'. This must be done taking into account the limited complexity that smaller operators might face.

Guidance

Expertise that can be included in the feed defence team, comprises of, but is not limited to:

- IT and site security;
- human resources;
- feed technology and science;
- toxicology, epidemiology, and microbiology;
- medicine (human and veterinarian) and radiology;
- packaging (and labelling) specialists;
- process engineering;
- production and operations;
- purchasing and procurement;
- distribution and logistics;
- information technology;
- communications;
- commercial/marketing
- regulatory.

7.1.2. Scope of the feed defence system

Requirement

The Operator must determine the scope of their feed defence system by conducting an initial assessment.

Guidance

Any method for assessment may be applied as long as the assessment addresses the topics identified in the guidance. Several recognized methods support the scoping of the feed defence system such as BSI "PAS 96:2017 Guide to protecting and defending food and drink from deliberate attack" and FDA's "Carver + Shock Primer"

Key questions in determining the scope of the defence system include

- What is the complexity of the feed supply chain and which step in the supply chain will be assessed (e.g. full supply chain vs. product processing in a specific facility)? It is important that the scoping aligns with the scoping of the feed fraud prevention system as defined in 6.1.2. (premises threat);
- What feed defence concerns are addressed (injury, illness or even mass mortality)?
- What type of attacker and attack is being protected from (from disgruntled employees to international terrorist organizations (attacker threat))?
- What agent(s) might be used to commit an attack (Product threat)?

The FAMI-QS template on threat assessment will support operators in conducting the requirements of this section.

7.1.3. Performing threat assessments

Requirement

The Operator must describe the supply chain subject to the threat assessment and choose the objects of focus based on the scoping defined under 7.1.2. The Operator must ensure that no parts of the scoping are excluded from the threat assessment. The Operator is, however, also encouraged to provide a clear rationale on the level of detail applied to the objects of focus.
Performing a threat assessment must be based on a systematic and risk based methods with the objective to reduce the likelihood of an attack and/or reduce the consequences of attack. The approach must consider the scope of the feed defence system in order to apply the appropriate level of detail to the threat assessment. Such could include considerations of:

1. addressing the threats at product or product group level;
2. addressing the threats at production process level;
3. addressing the threats at country, regional or site-specific level.

Assessing threats using the tools outlined in this paragraph must be supported by a system on data gathering about fraud risks. The Operator can use potential sources of information (e.g. public databases, websites, horizon scanning tools, industry working group or blogs) to support the assessment.

Guidance

A graphical presentation, in the form of a flow chart, can help to identify and choose objects of focus. For such a flow chart, operators break down their production system (considering the facilities, installations and buildings where they operate) into subsystems (e.g. ingredients mixing subsystem, packaging subsystem). These subsystems can then, if desired, be broken down into more detailed component parts (e.g. raw materials, receiving area, processing area, etc.) and nodes (i.e. equipment pieces). The Operator is encouraged to include external providers in the threat assessment.

7.1.4. Analysing risks and defining risk boundaries

Requirement

The Operator must analyse the output of the threat assessment, document the outcome of the analysis and decide on priorities, based on an evaluation of the level of threat associated with each object of focus. The Operator must set risk boundaries, depending on the levels of threat that are acceptable and unacceptable for the operation. Boundary setting must only be adopted where considered practical. For those threats, that are deemed unacceptable, counter measures should be defined in terms of critical control points (see section 7.1.5).

Guidance

FAMI-QS template on feed defence will support operators in in conducting the requirements of this section.

7.1.5. Defining critical control points

Requirement

The Operator must decide on and implement necessary controls and countermeasures that minimize the attractiveness of the identified priority targets.

Guidance

The FAMI-QS template on feed defence will support operators in in conducting the requirements of this section.

Building the control framework:

- identify priorities from the threat and risk assessment, considering regulatory requirements and describe the control measures (mitigation measures);
- where applicable, set critical control limits for the controls;
- define monitoring procedures for each control;
- define anticipated corrective actions for each control;
- validate approach before implementation and verify effective implementation.

Note: it is suggested to apply control limits where practical and based on operator insights. A control limit could be, for example, the (acceptable) number of suppliers that have not signed the code of conduct or the type of suppliers, or the percentage of specification testing allowed. Operators are encouraged to define control limits based on the risk perceived.

Countermeasures/controls can include, but are not limited to:

- physical access control;
- traffic flow control (of people, goods, vehicles, etc.);
- cyber security;
- inventory control;
- tamper detection;
- assuring personnel security.

8. Planning

8.1. Actions to address vulnerabilities and threats

The Operator must monitor and review the information about the external and internal vulnerabilities and threats related to feed fraud prevention and defence. The Operator must determine the vulnerabilities and threats that need to be addressed, and must plan actions to address these risks and opportunities. The planning activities for feed fraud prevention and defence must be aligned with the planning activities for quality and food safety as addressed in the FAMI-QS code chapter 6.1.

The actions must be proportionate to the context of the Operator and the requirements of interested parties. The actions must include the development and implementation of feed fraud prevention and feed defence system plan and reviews.

8.2. Feed fraud prevention and defence objectives and planning to achieve them

The Operator must establish feed fraud prevention and defence objectives at relevant functions and for relevant processes, throughout the organisation. The objectives for feed fraud prevention and defence must be aligned with the planning activities for quality and food safety as addressed in the FAMI-QS code chapter 6.2.

Documented information related to the monitoring efforts must be retained.

8.3. Planning of changes

Where the Operator determines the need for change in the feed fraud prevention and defence management system, the change must be carried out in a planned and systematic manner, according to written procedures. Changes must be approved by authorised personnel. Any changes regarding feed fraud prevention and defence should be aligned with the planning activities for quality and food safety as addressed in the FAMI-QS code chapter 6.3.

9. Documentation

The Operator must have a documented feed fraud prevention and defence management system that reflects all aspects of this module. Records must contain all relevant data to permit investigation of any nonconformity or deviation(s) from planned procedure(s).

All activities related to feed fraud prevention and feed defence must be recorded without delay after they have been performed and must be aligned with the documentation requirements of the FAMI-QS Code chapter 4.4. Any requirements for documentation under the FAMI-QS code must be extended to the Operator's feed fraud prevention and defence management system and must include:

a) documentation of the vulnerability and threat assessments and analysis performed as well as identified controls required under chapter 6 and 7;
b) procedures on how the feed fraud prevention and defence management system is established, maintained and reviewed;
c) documented information determined by the Operator as being necessary for the effectiveness of the feed fraud prevention and defence management system;
d) documentation on feed fraud prevention and defence management policies (as part of overall quality and feed safety procedures).

10. Operation

10.1. Operational planning and control including external provision and purchasing

Requirement

The Operator must plan, implement and control the processes needed to meet requirements, and to implement the actions determined in the feed fraud prevention and defence management system as defined in chapter 6 and 7. These activities must include the control of externally provided products and services, including contracted manufacturers. The operational activities for feed fraud prevention and defence must be aligned with the operational activities for quality and food safety as addressed in the FAMI-QS code chapter 8.1, 8.5 and 8.6.

10.2. Type and extent of control of external provision – contract manufacturers

Requirement

Specifically for the control of externally provided products and services, the Operator must identify externally provided processes, products, and services, which may be subject to heightened fraud and terror risk and ensure that they conform to specified requirements and are covered by the Operator's vulnerability and threat assessments as defined in chapters 6 and 7.

If the contracted manufacturer is not FAMI-QS certified according to this module, the Operator must evaluate the risk associated to the Operator's product and perform an audit, in order to ensure that the contracted manufacturer meets the requirements as outlined in this document. This audit can be aligned with any audits already planned for non-FAMI-QS certified suppliers of products our services as outlined in paragraph 8.5 of the FAMI-QS code. The audit must be performed by an appropriately trained and competent auditor. A report must be written and accessible.

During the Operator's certification and surveillance audits, the certification body must check the audit report of the contracted manufacturer, and, if deemed necessary, also audit the external contracted manufacturer. Note: Adequate training of auditors normally includes knowledge of the FAMI-QS code, feed fraud prevention and defence module, auditing techniques and the scope of the external provider (process, product or service).

10.3. Selection and management of suppliers

Requirement

In line with the purchasing of materials-requirements of the FAMI-QS code section 8.6, operators must manage suppliers in such a way that suppliers have the capability to meet specified feed fraud prevention and defence requirements.

The FAMI-QS code section 8.6.1. requires operators to define a process for the selection, approval and monitoring of suppliers, including selection and evaluation according to operators' requirements. There is also a requirement to maintain a list of internally approved suppliers, including the purchased raw material and their status as assured or non-assured, and subject these suppliers to periodical review. The Operator must extend the requirements to the feed fraud prevention and defence management system. As a result the Operators must, using the results of the vulnerability and threat assessments, consider appropriate controls to select and manage of its suppliers effectively. Such could include (non-exhaustive) product testing, supplier audits, requiring certifications that effectively mitigate fraud and terror risks.

10.4. Verification of incoming materials

Requirement

Operators must extend the verification of incoming materials according to the FAMI-QS code section 8.6.2 to the feed fraud prevention and defence management system.
If incoming materials are rejected and thus not incorporated because of noncompliance with the specification or for any reason related to product quality and safety, their disposal, destination or return to supplier must be recorded.

11. Performance evaluation

Requirement

To ensure the effectiveness of the Operator’s feed fraud prevention and defence management system, the Operator should monitor its control measures defined in section 6.1.5 and 7.1.5. The monitoring activities must be aligned with the requirements of the FAMI-QS chapter 9 and include monitoring, evaluation and management

Guidance:

Various sources (see chapter 13) have identified methods and tools that can help the Operator to monitor the feed fraud prevention and defence management system:

- internal and external audits;
- inspections by stakeholders;
- risk simulations;
- register of suspicious situations and malicious behaviour;
- benchmarking;
- routine watch of official and industry publications, which give an early warning of changes that, may become new threats or change the priority of existing threats.

12. Improvement

Requirement

To ensure the continuous improvement of the Operator's feed fraud prevention and defence management system, the Operator must address non-conformities resulting from evaluation and continuously improve the suitability, adequacy and effectiveness of its system. The improvement activities must be aligned with the requirements of the FAMI-QS code 6.0 chapter 10.

Guidance:

The Operator is encouraged to revise the feed fraud prevention and defence management system:

- in a systematic way (minimum annually), based on the effectiveness of the controls put in place;
- in case internal or external circumstances have changed;
- following risk simulations;
- following any alert, or proper attack.

13. Sources

Afnor Groupe. *“Guide méthodologique food defence.”* 2015

BSI. *“PAS 96:2017 Guide to protecting and defending food and drink from deliberate attack.”* November 2017

European Parliament. “*Regulation 178/2002/EC.”* 2002

Fami-QS. *“Fami-QS Code of Practice.”* July 2018

FDA. *“Food Defense.”* https://www.fda.gov/food/fooddefense

FDA. *“Carver + Shock Primer.”* September 2009

IRM. “*A Risk Practitioners Guide to ISO 31000: 2018.”* 2018

ISO 22000:2018. *“Food safety management systems — Requirements for any organization in the food chain.”* 2018

Ministère de l’Agriculture, de l’Agroalimentaire et de la Forêt. *“Guide des recommandations pour la protection de la chaîne alimentaire contre les risques d’actions malveillantes, criminelles ou terroristes.”* January 2014

National Cyber Security Centre. *“Cyber security.”* https://www.ncsc.gov.uk/home

Spink, J., Moyer, D.C.. *“Defining the Public Health Threat of Food Fraud.”* 2011