Quality and Safety System for Specialty Feed Ingredients

FEED FRAUD PREVENTION AND DEFENCE MODULE

Audit Guidance for Certification Bodies

VERSION 1.0
12/2020

1. Introduction 2
2. Scope 2
3. Audit Duration 2
4. Resource Requirements 3
5. Audit planning 3
6. Feed fraud prevention and defence activities 3
7. Maintaining certification 12
8. Classification of non-conformities and recommendations 12
9. Assessment of suppliers and assured sources 12
10. Certificate 12
11. Other 13

1. Introduction

This audit guidance provides support for the audit of the FAMI-QS Feed Fraud Prevention and Defence module. In 2018, FAMI-QS carried out the challenging task to incorporate the requirements for feed fraud prevention and defence under its third-party certification system, by creating an additional mandatory add-on module for FAMI-QS Certification System Version 6. The module applies to trade and production.

The Feed Fraud Prevention and Defence module is not a stand-alone document and will be used exclusively in conjunction with the FAMI-QS Code of Practice Version 6.0. Implementing and adhering to the module is mandatory for all feed business organisations choosing to get certified against FAMI-QS Version 6. The goal of the module is to ensure that FAMI-QS Certified Feed Business Operators will implement an auditable system that demonstrates their ability to manage and effectively mitigate the risk of feed fraud and terrorism. This means that it is not product-specific, but process-specific. Fraud and terror activities can occur either due to external or internal factors.

The objective of the system is to protect the FAMI-QS Certified Organisation from possible fraud or terror activities and demonstrate to the feed chain their commitment to prevent fraud and terror.

Certification bodies should use this guidance in conjunction with the requirements of the Rules for Certification Bodies current version as released by the FAMI-QS Organisation. Any certification body audits against the Feed Fraud Prevention and Defence module should always be part of audit activities (initial, surveillance or re-certification audits), performed to establish compliance to the FAMI-QS Code current version or future versions thereof. All Rules for Certification Bodies current version apply therefore to the audit activities for the Feed Fraud Prevention and Defence module. Chapter 6 *'Feed fraud prevention and defence audit activities'* provides specific guidance for the auditors to prepare and execute the audits against the requirements of the Feed Fraud Prevention and Defence module.

2. Scope

The Feed Fraud Prevention and Defence module requires operators seeking certification to FAMI-QS to apply the scope as defined for the FAMI-QS 6.0 certification. The certification body should place particular focus on the specific requirements on defining the scope for feed fraud prevention and defence as defined in sections 6.1.2. and 7.1.2 of the Feed Fraud Prevention and Defence module. Due to the nature of the topic, the FAMI-QS Certified Organisation shall review the suitability of their current assessment on an annual basis in the framework of their actions for continuous improvement. The annual review does not mean that an update of assessments is required.

3. Audit Duration

For the initial assessment of the implementation of the FAMI-QS Feed Fraud Prevention and Defence module, the certification body shall allocate (as a minimum) 0.5 man-days as an add-on to the auditing time that has been already allocated. Certification bodies should carefully plan the calculation of audit time. Specific conditions such as geography, location dimensions (e.g., size of the facility) that require additional audit efforts in relation to the FAMI-QS Feed Fraud Prevention and Defence module can lead to additional audit time being allocated. Such should also include consideration on additional audit time for a multi-site certification based on the activities of the organisation.

For the next subsequent audit, 0.25 man-days shall be allocated for the review of the vulnerability and threat assessments.

4. Resource Requirements

The Certification body should ensure sufficient and competent personnel for managing and supporting the provision of the feed fraud prevention and defence audit activities according to the FAMI-QS Rules for Certification Bodies current version including an update of the competence criteria.

In addition, the certification body shall ensure that the competent personnel:

1) have successfully completed an internal training course on feed fraud prevention and defence provided by the certification body (subject to FAMI-QS' approval) or by FAMI-QS.
2) are trained on all aspects of this audit guidance

Sufficient documentation of training activities shall be kept.

5. Audit planning

The certification body assesses the feed safety management system of the organisation in compliance with the FAMI-QS Code Version 6.0 and therefore the Feed Fraud Prevention and Defence module, based on initial, surveillance and recertification audits. The audit programme shall be adapted accordingly to include the audit against the requirements of the FAMI-QS Feed Fraud Prevention and Defence module. The module will be audited through a desk review and (remote or onsite) audit. For initial certification, this shall be part of the Stage 1 audit.

Multisite organisations[1]: certain aspects relating to fraud and defence shall be checked on the local sites. These local sites may not have a complete vulnerability and threat assessment, and therefore only specific (fraud) vulnerabilities relating to the local operation will be assessed, given that all other aspects are managed centrally. Confidentiality considerations, documentation of the remote audit process deployed and any documents supporting the assessment findings shall be maintained. Special attention shall be given to the feed defence assessments for which permission may be required.

In case of an initial certification audit to FAMI-QS Code 6.0, all rules for conducting Stage 1 and 2 audits as defined in the latest version of the Rules for Operators apply.

6. Feed fraud prevention and defence activities

To support the certification body in the execution of the audit planning, FAMI-QS has developed a guidance that provides suggested audit activities for each section of the Feed Fraud Prevention and Defence module. These activities focus on the setup and effective implementation of the Feed Fraud Prevention system and the Feed Defence system as outlined in chapters 6 and 7 of the module.

[1] An organization covered by a single management system comprising an identified central function (not necessarily the headquarters of the organization) at which certain processes/activities are planned and controlled, and a number of sites (permanent, temporary or virtual) at which such processes/activities are fully or partially carried out. (IAF MD1:2018). The Certification Body shall maintain a single audit programme and audit plan. Please note that we refer to multi-site application were site sampling is not possible.

#	FFPD requirement	FFPD detailed requirement	Audit objective	Suggested audit activities	Guidance for audit
6.	Feed fraud prevention system				
6.1	Feed fraud prevention system and its processes	*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	*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.*	To verify sufficient involvement of key competence and establish if a multi-disciplinary approach has been deployed for all activities relating to 6.1.2 - 6.1.5	* Discuss with responsible management the logic of the involved team (as captured in the 'team tab in the VACCP template') as well as their roles and responsibilities assigned in relation to feed fraud prevention. * Discuss how team members have been involved (e.g., workshops, brainstorms or other) in the establishment of scoping, vulnerability assessment and controls definition and implementation. In the event of a multi-site organisation, the team shall also include a representative of each local site.	Due to the nature of feed fraud vulnerabilities (intentional, economic gain) the need for competencies to be involved may be different from managing feed safety risks. Therefore, it is key that responsible management involves competencies as suggested in 6.1.1.
6.1.2	Scope the Feed fraud prevention system	*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 nutrition;* *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, function groups,*	To verify if sufficient scoping has occurred that ensures alignment with the overall certificate scope	* Discuss with responsible management the results of the defined scope as reported in the VACCP template to establish alignment/fit with the FAMI-QS Code 6.0 certificate scope. * If additional scopes (sub scopes) have been defined in the template, request evidence if vulnerability assessments have been performed for these additional scopes.	To support a more product, process or geographical oriented discussion of vulnerabilities, the operator may choose to define a more detailed scope based on the answers to the questions in the 'scoping' tab of the VACCP template. This scoping tab supports companies in focusing on the areas that matter or that are considered most vulnerable to fraud. As a result, the operator may also decide to define additional scopes. In such situation, the term sub-scopes is used. The operator should always ensure that the results of all sub-scopes cover the full FAMI-QS Code 6.0 certificate scope. Operators are not allowed to exclude certain activities

		territories/sites involved in the assessment and define a process plan.			of the overall scope in scoping the vulnerability assessment.

#	FFPD requirement	FFPD detailed requirement	Audit objective	Suggested audit activities	Guidance for audit
6.1.3	Performing Vulnerability Assessments	*The Operator must conduct a feed fraud vulnerability assessment based on the scope determined in 6.1.2. and document the results.* *The VACCP 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.*	To verify if the process of the vulnerability assessment as described in the requirements and supporting VACCP template has been performed.	* Review if all vulnerability assessment has been scored for each of the (22) vulnerabilities, including a justification for scoring * Discuss 1 or 2 example vulnerabilities and the justification for scoring 1, 2 or 3 and justification has been captured in the justification section of the 'Vulnerability assessment tab'.	*The objective of the auditor should not be to verify the contents of the vulnerability assessment as sufficient competency deployment together with a verified process should ensure that the vulnerability assessments have been performed at an adequate level. Auditors can choose to discuss one or two identified vulnerabilities to gain a better understanding of the process deployed. * Operators are advised to score all vulnerabilities even in situations where a clear control mitigating or reducing the vulnerability is already in place, especially in the early stages of fraud prevention. Most controls in place have not been established for the (sole) purpose of feed fraud prevention and changes to the controls may be managed by those not responsible for fraud prevention. In such a case, changes to the control are then noted by those responsible for fraud prevention. If not recorded, such changes may not be noticed and a potential vulnerability may arise.

#	FFPD requirement	FFPD detailed requirement	Audit objective	Suggested audit activities	Guidance for audit
6.1.4.	Analysing risks and defining risk boundaries	*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).*	To verify if the operator has a transparent process in place to analyse each vulnerability and decide on treatment.	* Discuss if the company has discussed the risk appetite and which risk appetite level has been chosen (using the slider). * Discuss 1 or 2 example vulnerabilities selected for treatment and the rationale for selection. * Review which vulnerabilities in the assessment have been treated (treatment column is yes) and select one or two to establish if a clear rationale for treatment has been applied. Assess if decisions of treatment are coherent with the chosen risk appetite (e.g., a low-risk appetite but not treating a lot of vulnerabilities with a score of 3 is not consistent).	* The overall risk level outcome is the result of the average scores of each of the vulnerabilities assessed per category (opportunity/motivation/control) and provides an average 'need for treatment'. Based on the operator's risk appetite, this 'need for treatment' may be changed to a higher or lower need to treat risks. This provides operators with a rationale to either treat or accept certain vulnerabilities and guide internal discussion on treatment of vulnerabilities identified in 6.1.3. * Part of the vulnerability analysis is to decide which of the vulnerabilities in the assessment tab will be treated. Auditors can choose to discuss one or two vulnerabilities that have been identified as vulnerabilities to be treated. Also, consider discussing one or two vulnerabilities that have not been treated.

#	FFPD requirement	FFPD detailed requirement	Audit objective	Suggested audit activities	Guidance for audit
6.1.5.	Defining Critical Control Points	*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 diagnose whether sufficient controls are in place, and then build 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 reported;* *3. identify any additional controls not reported;* *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.*	To verify if the operator has identified and implemented sufficient controls for the vulnerabilities that require treatment according to the analysis.	* Review if all identified vulnerabilities have been addressed. * Discuss 1 or 2 example controls and why they should mitigate or reduce the vulnerability. * Add the selected controls to the overall audit programme to test the implementation of controls. Request supporting evidence of controls implementation, testing and, where applicable corrective actions. * Consider interviewing staff members involved in the execution or testing of controls to test awareness of activities and knowledge of vulnerabilities to feed fraud.	* All vulnerabilities that have been marked with 'Yes' are in the 'Control template ' tab. * The objective is not to verify the content of the controls defined as sufficient competency deployment together with a verified process should ensure that the vulnerability controls have been implemented at an adequate level. * Operators are allowed to reference to existing or new controls (CCP's) that are defined in other (operator-owned) quality manuals or systems. These manuals as a minimum should contain a description of the controls as required in sections 2-5 of the 'Control template' tab.

#	FFPD requirement	FFPD detailed requirement	Audit objective	Suggested audit activities	Guidance for audit
7.	Feed defence system				
7.1.	Defence system and its processes	*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	*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.*	To verify sufficient involvement of key competence and establish if a multi-disciplinary approach has been deployed for all activities relating to 7.1.2 - 7.1.5.	* Discuss with responsible management the logic of the involved team (as captured in the 'team tab in the TACCP template') as well as their roles and responsibilities assigned in relation to feed defence prevention. * Discuss how team members have been involved (e.g., workshops, brainstorms or other) in the establishment of scoping, threat assessment and controls definition and implementation.	Due to the nature of feed terror threats (intentional, ideological gain), the need for competencies to be involved may be different from managing feed safety risks. Therefore, it is key that responsible management involves competencies as suggested in 7.1.2.
7.1.2.	Scope of the Feed defence system	*The Operator must determine the scope of their feed defence system by conducting an initial assessment.*	To verify if sufficient scoping has occurred that ensures alignment with the overall certificate scope.	* Discuss with responsible management the results of the defined scope as reported in the TACCP template to establish alignment/fit with the FAMI-QS Code 6.0 certificate scope. * If additional scopes (sub-scopes) have been defined in the template, request evidence if threat assessments have been performed for these additional scopes.	To support a more product, process or geographical oriented discussion of threats, the operator may choose to define a more detailed scope based on the answers to the questions in the 'scoping tab of the TACCP template'. This scoping tab supports companies to focus on the areas that matter or are considered most vulnerable to terror. As a result, the operator may also decide to define additional scopes. In such a situation, the term sub-scopes is used. The operator should always ensure that the results of all sub-scopes cover the full FAMI-QS Code 6.0 certificate scope. Operators are not allowed to exclude certain activities of the overall scope in scoping the threat assessment.

#	FFPD requirement	FFPD detailed requirement	Audit objective	Suggested audit activities	Guidance for audit
7.1.3.	Performing Threat Assessments	*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 risks associated with attack. 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.*	To verify if the process of threat assessment as described in the requirements and supporting TACCP template has been performed.	* Review if all threat assessment has been scored for each of the threats, including a justification for scoring and **potentially not applicable.** * Discuss 1 or 2 example threats and the justification for scoring and that the justification has been captured in the justification section of the 'Threat assessment tab'.	The objective of the auditor should not be to verify the contents of the threat assessment as sufficient competency deployment together with a verified process should ensure that the threat assessments have been performed at an adequate knowledge level. Auditors can choose to discuss one or two identified threats to gain a better understanding of the process deployed. * Operators are advised to score all threats even in situations where a clear control mitigating or reducing the threat is already in place, especially in the early stages of terror prevention. Most controls in place have not been established for the (sole) purpose of feed defence and changes to the controls may be managed by those not responsible for feed defence prevention. In such a case, changes to the control are then noted by those responsible for feed defence prevention. If not recorded such changes may not be noticed and a potential vulnerability may arise.

#	FFPD requirement	FFPD detailed requirement	Audit objective	Suggested audit activities	Guidance for audit
7.1.4.	Analysing risks and defining risk boundaries	*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).*	To verify if the operator has a transparent process in place to assess each threat and decide on treatment.	* Review which threats in the assessment have been treated (treatment column is yes). * Select one or two to establish if a clear rationale for treatment has been applied and that the rationale has been captured in the justification section of the 'Threat assessment tab'.	* Part of the threat results is to decide which of the threat in the assessment tab will be treated. Auditors can choose to discuss one or two threats that have been identified as threats to be treated. Also, consider discussing one or two threats that have not been treated. * The threats displayed in the 'threat results tab' are shown per threat category. Note that the risk boundaries (the areas where the chart moves from red to yellow and from yellow to green) are deliberately not clearly set to ensure the Operator discusses which areas they consider high, medium or low risk. The Operator should be able to provide input on how this has guided the discussions on which risks to treat and which not to treat. This should show in the justification section of the 'Threat Assessment tab'.
7.1.5.	Defining Critical Control Points	*The Operator must decide on and implement necessary controls and countermeasures that minimize the attractiveness of the identified priority targets.*	To verify if the operator has identified and implemented sufficient controls for the identified threats that require treatment according to the analysis.	* Review if all identified threats have been addressed. * Discuss 1 or 2 example controls and why they should mitigate or reduce the threat. * Add the selected controls to the overall audit programme to test the implementation of controls. Request supporting evidence of controls implementation, testing and, where applicable, corrective actions. * Consider interviewing staff members involved in the execution or testing of controls to test awareness of activities and knowledge of threats of feed terror.	* All threats that have been marked with 'Yes' are in the 'Control template ' tab. * The objective is not to verify the content of the controls defined as sufficient competency deployment together with a verified process should ensure that the threat controls have been implemented at an adequate level. * Operators are allowed to reference to existing or new controls (CCP's) that are defined in other (operator-owned) quality manuals or systems. These manuals as a minimum should contain a description of the controls as required in sections 2-5 of the 'Control template' tab.

7. Maintaining certification

Certification bodies shall integrate the audit activities required for the Feed Fraud Prevention and Defence module in all audit activities relating to maintaining certification, including surveillance and re-certification. Special and unannounced audits, as defined in the latest version of the Rules for Operators, shall not include audit activities for the Feed Fraud Prevention and Defence module.

8. Classification of non-conformities and recommendations

Certification bodies shall classify any non-conformities and recommendations on the Feed Fraud Prevention and Defence requirements according to the definitions of non-conformities and recommendations defined in the latest version of the Rules for Operators.

9. Assessment of suppliers and assured sources

Certification bodies shall assess the Feed Fraud Prevention and Defence requirements for suppliers and assured sources according to the audit guidelines for suppliers and assured sources, as defined in the latest version of the Rules for Operators.

10. Certificate

Once the certification body confirms that the requirements of the module are fulfilled, the certification body shall re-issue the certificate with the highlighted statement for the remaining validity period of the certificate (if the update occurs at the time of surveillance or in between). An update of the certificate (selection of the checkbox 'Fraud and Defence') is also required in the ViaSyst platform.

Operator's Name
has implemented and maintains a Feed Safety and Quality Management System including Good Manufacturing Practice (GMP) in compliance with:
FAMI-QS Code (Version x, YYYY-MM-DD)

on the following site(s)(1) XXX

FAMI-QS Site Registration: FAM-xxxx/xx

for Activity(2) of Specialty Feed Ingredients
From Process (3)

Feed Chain Category(4) DI, K, FI, FII

The Operator implements measures for feed fraud/feed defence according to the FAMI-QS Feed Fraud Prevention and Defence Module Version 1.

This certificate is valid until: YYYY-MM-DD

11. Other

All other principles of transparency, surveillance, sanctions, notification of changes and the use of logo also apply to the audit activities against the Feed Fraud Prevention and Defence module.