Central Production Unit Food Safety & Quality Management System

Food Defence

Purpose

To ensure that the Central Production Unit is assessing the end-to-end supply chain and minimising the risk of purchasing or placing on the market fraudulent or adulterated food, and to ensure that all product descriptions and product claims are legal, accurate and verified.

Scope

This policy outlines the controls in place to manage food defence from the supply chain, through to potential vulnerabilities in raw materials, and the potential threats to the finished product.

Responsibilities

Responsible Person (s)	Responsibility
Site manager	To ensure this procedure is fully implemented, adhered to and content communicated to the wider Unit team and all relevant colleagues and third parties To ensure that only approved products, from approved suppliers are purchased. Where substitutions are used, they are formally approved, and records retained to ensure traceability To ensure this procedure is accurate, regularly reviewed and kept up to date, to include examples where is a change to process

Foodbuy

All products purchased should be through Foodbuy. All approved products are in line with the Compass Group UK&I Supply Chain Integrity Policy Statement to ensure safe, legal, ethical, and quality products are sourced and supplied into the Compass Group UK&I units. Compass Group UK&I are also members of Campden BRI, and The Food Industry Intelligence Network (FIIN) and receive regular communications around and food related horizon scanning and food alerts.

Purpose

A Food Defence Plan is designed to encompass all activities end-to-end across the supply chain. This will help to ensure the raw materials, and the production processes are reviewed and assessed for potential Food Fraud, Food Sabotage or Food Terrorism related incidents. The aim of the vulnerability assessment is to search for potential weaknesses within the supply chain of the products used by the Central Production Unit and identify any raw materials that may be at particular risk of adulteration or substitution allowing for appropriate controls to be implemented to minimise of reduce risk.

Definitions

The term 'Food Defence' is defined as protecting food products, raw materials, and production processes from threats. Food Defence can be broken down into three key areas that may represent a threat to raw material and the finished product

1. **Food Fraud**: A collective term used to describe the deliberate adulteration or misrepresentation of food, food ingredients or raw materials for financial gain.

2. **Food Sabotage**: The deliberate destruction, damage or disruption of food products or processes with the intention of causing reputational damage of financial loss.

3. **Food Terrorism**: An act or threat of deliberate contamination of food for human consumption with biological, chemical and physical agents or radioactive materials for the purpose of causing injury or harm to civilian populations and/or disrupting social, economic or political strategy

Raw material vulnerability assessment

The aim of the raw material vulnerability assessment is to search for potential weaknesses within the supply chain of the raw material ingredients used by the Central Production Unit to identify any raw materials that may be at particular risk of adulteration or substitution allowing for appropriate controls to be implemented to minimise or reduce potential risk.

Structuring the assessment

A tabular approach should be used to conduct the assessment due to its simplicity and helps to ensure that the system is viewed and considered in its entirety.

Defining raw materials

Due to various raw materials used at the Central Production Unit, materials should be grouped as per the example below.

Example

Meat products	*Cooked, meat products that have been sliced, diced, or processed including cooking*
Grains and pulses	*Rice, Pasta, Noodles, Bulgar Wheat, Quinoa, Cous Cous, Tinned Pulses*

The assessment should review the threat categories Fraud, Terrorism and Sabotage and considers each of these categories in relation to: -

- Historic Incidents
- Economic factors
- Geographic origin of product
- Length and complexity of the supply chain
- Storage and distribution
- Nature of raw materials
- Physical form
- Emerging concerns
- Existing controls
- Availability of raw material
- Ease of access to raw materials
- Availability of substitutes / potential adulterants

On site threats associated with the product process and threats associated with the downward product supply chain are considered in part two of the assessment.

Central Production Unit Food Safety & Quality Management System

Food Defence

Types of threats

The following threats should be considered in the raw material vulnerability assessment.

Food terrorism

Contamination of raw materials at the supplier's site or in the raw material supply chain with a harmful biological agent or contamination of water or other services with harmful agents

Food sabotage

Malicious contamination of raw materials by a supplier's disgruntled employee to cause harm to the consumer or disruption to the business, such as the addition of glass fragments or allergenic materials such as peanuts. Sabotage of raw materials by welfare groups, focusing on businesses in the supply chain, e.g., animal welfare groups publicly announcing that they have contaminated product.

Types of perpetrators

A threat is 'a deliberate act by someone to cause harm or for financial gain. The possibility of who the "someone" might be, has to be carefully considered in the context of a food defence study. Within the scope or the study, the following perpetrators should be considered:

- **Suppliers** of raw material who have access to, and the opportunity to compromise the product either for financial gain, or to cause harm.

- **Logistical Contractors** used to move or store raw material, who are contracted either directly by the company or by their suppliers, have access to the product and the opportunity to compromise it.

- **Outsiders** are furthest from the business (have no current contact with the business, for example, extremists or extortionists). Outsiders may have little opportunity of access but may be highly motivated. They may try to increase their access to the raw material through compromising insiders via bribery or threat.

Potential perpetrators who are more remote from the target business may also have far less loyalty or connection with the business. In this regard, the perpetrator may see the business as an entity rather than a team of people with jobs and livelihoods to protect. For a threat to be carried out, the perpetrator needs to be sufficiently motivated. The types of motivation may vary, and can include: -

- **Ideological**: This is perhaps the strongest level of motivation and may lead to the perpetrator, such as a terrorist endangering their own personal safety.

- **Financial Gain**: This is likely to be the motivator for an extortionist who may be demanding large sums of money by claiming raw materials have been contaminated with a harmful substance. It is also the key driver for economically motivated adulteration and counterfeiting.

- **Welfare causes:** This would include both animal and human welfare such as anti-slavery.

- **Personal grievance or pressure:** Feeling the need for revenge as a response to action taken by the company can motivate disgruntled individuals, such as employees. Pressure of financial Targets or production volumes may motivate some individuals to do the wrong thing, such a substitution of cheaper ingredients.

Central Production Unit Food Safety & Quality Management System

Food Defence

Threat categories

There are known knowns, these are things we know we know. There are known unknowns; that is to say, we know there are some things we know we do not know, and there are also unknown unknowns, the ones we don't know what we don't know."

- **Known knowns**: There are threats which have occurred before, so history tells us that they could occur again in the future. Known threats are included in the assessment.

- **Known unknowns**: These are threats that have not occurred before. However, given what we have learnt from previous threats, it is plausible to presume that they could happen. As known unknowns could possibly happen, these are included in the assessment.

- **Unknown unknowns**: These are threats that have not occurred before and are inconceivable. Unknown unknows are not included in the assessment, because including these types of threats would cause the assessment to become unfocused and subjective.

To establish the known and plausible threats that should be included, both internal and external sourced of information should be used. Internal sources of information include information from the Supply chain and planning team, around sourcing and availability of raw materials. External sources of Information include historical data, and real time data that comes through from the Food Standards Agency, Food Standards Scotland, the Health Security Agency and other agencies across devolved nations, Vendor Assurance, FIIN and business as usual horizon scanning completed in house and in consultation with Primary Authority.

Finished goods vulnerability assessment

The aim of the finished goods vulnerability assessment is to search for potential weaknesses at site level and within the operation of the Central Production Unit that may result in adulteration, substitution or sabotage allowing for appropriate controls to be implemented to minimise of reduce risk.

Structuring the assessment

A tabular approach should be used to conduct the assessment due to its simplicity and it can help to ensure that the system is viewed and considered in its entirety.

Types of threats

The following threats should be considered in the finished goods vulnerability assessment.

Food Fraud

Food fraud is a collective term used to describe economically motivated adulteration (EMA) and counterfeiting of food for financial gain. Examples of EMA and counterfeiting relevant to the Finished Good Vulnerability study have been listed below.

Economically motivated adulteration

Decisions made on-site to avoid financial consequences, such as using a lower grade ingredient in the event of a shortage of the genuine material to avoid penalties of incomplete orders, or misrepresentation of product due to changing of labels or identity in the downstream distribution chain.

Counterfeiting

Theft of electronic artwork or recipes through cybercrime which are subsequently used to produce counterfeit product, or theft of product (finished work-in-progress, excess or waste product), from site, third party storage facilities, or waste contractors which is then sold through unapproved routes (grey market). The grey market includes genuine products sold through routes which are unauthorised, unofficial, or unintended by the manufacturer.

Perpetrators

Within the scope of the finished goods vulnerability assessment, the most likely perpetrators can include, but are not limited to:

Insiders: Current employees of permanent or temporary contracts, agency staff) are perhaps the most significant category of potential perpetrator due to their possibly high level of legitimate access to the production areas and products. The high level of legitimate access can make direct product or raw material contamination much more feasible. Insiders are also likely to have the strongest emotional connection with the business.

Suppliers and contractors: Contracted employees such as contractors and maintenance personnel may also have legitimate access to parts of the process. A lack of effective on-site controls may enable these trusted and familiar individuals to have easy access to sensitive parts of the operation required to allow for food tampering or adulteration.

Outsiders: Have no current contact with the business, for example extremists or extortionists are furthest from the business. Outsiders may have little opportunity to access but may be highly motivated. They may try to increase their access through compromising insiders via bribery or threat.

Process flow decision tree

The vulnerability assessment process flow diagrams detailed in Appendix II and Appendix III summarises the process for determining each step and aligning them to threats and vulnerabilities within the operational process.

Assessing impact and vulnerability

When assessing the impact and vulnerability the same method applies for both the raw material and the finished good vulnerability assessment.

Impact Assessment

To ensure the risk is assessed objectively and consistently a scoring system has been applied. The scoring system is higher for the consumer than for the business, as the consumer is the primary concern. Any loss or harm to the business is generally a consequence of the effect that the threat has on the consumer, resulting in loss of sales or financial impact due to fines, withdrawals, recalls etc. The terms and consumer reactions repulsion and upset have been included in the impact on the consumer. Food defence is not restricted to food safety and therefore consumer repulsion and upset is a risk and reputational factor, therefore has been included. Within the scoring system, the scores for consumer impact and business impact are added together. The addition of the numbers ensures that the impact to the consumer has a greater weighting as consumer protection is paramount.

Table 1: Consumer vulnerability assessment

Consumer		Business	
Definition	**Score**	**Definition**	**Score**
Death	9	Closure	4
Hospitalisation	8	Major financial loss	3
Minor harm	7	Minor financial loss	2
Reputational / disgust	6	Disruption	1
Upset	5	None	0
None	0		

Vulnerability assessment

Threat and vulnerability are two separate entities; However, they are fundamentally linked. A threat can exist but, if there is no weakness to that threat, then there is no vulnerability. Vulnerability is a measure of how susceptible the business is to the threat having an impact.

Table 2: Motivation vulnerability assessment

Motivation		Likelihood of detection	
Definition	**Score**	**Definition**	**Score**
Ideological	4	It will not be detected	4
Financial gain	3	It is unlikely to be detected	3
Welfare causes	2	It is likely to be detected	2
Personal grievance or pressure	1	It is highly likely to be detected	1
None	0	It will be detected	0

Once the overall scores for impact and vulnerability have been calculated, the two scores are then multiplied together to give a risk score for that threat. The reason for multiplying these figures is to allow situations where the motivation and the likelihood of detection score are deemed to be zero, to mitigate the impact score, giving a result of zero. This is because no matter how high the impact of the threat, if there is no vulnerability, there is no risk.

Scoring methodology example

Consumer Impact + Business Impact = Impact Score 8 + 3 = 11

Motivation x Likelihood of Detection = Vulnerability Score 1 x 3 = 3

Impact Score x Vulnerability Score = Risk Score 11 x 3 = 33

Scoring significance

A significant threat is a threat to which the consumer and subsequently the business is unacceptably vulnerable. A cut-off score of 33 has been applied by taking the minimum score for what would be a totally unacceptable impact on the consumer and the business, and similarly for motivation and likelihood of detection. The score which would cause significant impact to the business is **3** and above. Any Motivation by a person intending to cause harm to the consumer is totally unacceptable and therefore the score which would cause a significant motivation is **1** or above. When the deliberate act of a threat, or the threat itself is unlikely to be detected it would cause significant concern, therefore **3** and above is classed as significant.

Establishing Protection Measures

Any threat identified with a score of above **33** is put through the decision tree process as detailed in Appendix II and Appendix III, to establish a suitable protection measure for the threat as defined below.

Threat Management Technique	Process Overview
Risk Register	Highlights where risks in the business are, but no protection measure currently available.
VTP (Vulnerable Threat Point)	Identification of a weakness or gap in the business. Vulnerability has been identified but does not necessarily mean the threat is constantly there.
Supplier Management Procedures	Protection measures for Raw Material Vulnerability included in the Supplier Management Procedures.
Manage as, or Amend Site PRP's	Protection measures for Finished Good Vulnerability included in the site Prerequisite Programs.
Existing CCP	Protection Measure managed through an existing site CCP.

Review and maintaining the Food Defence plan

The site-specific Food Defence plan and assessment must be kept under constant review in line with changing economic circumstance and market intelligence. The assessment is updated in line with new raw materials and menu changes, changes in supplier specification, changes in supply chain, logistics, change in material availability, emergence of new risks, industry developments and scientific information. At a minimum the assessment is formally reviewed annually.

Document control

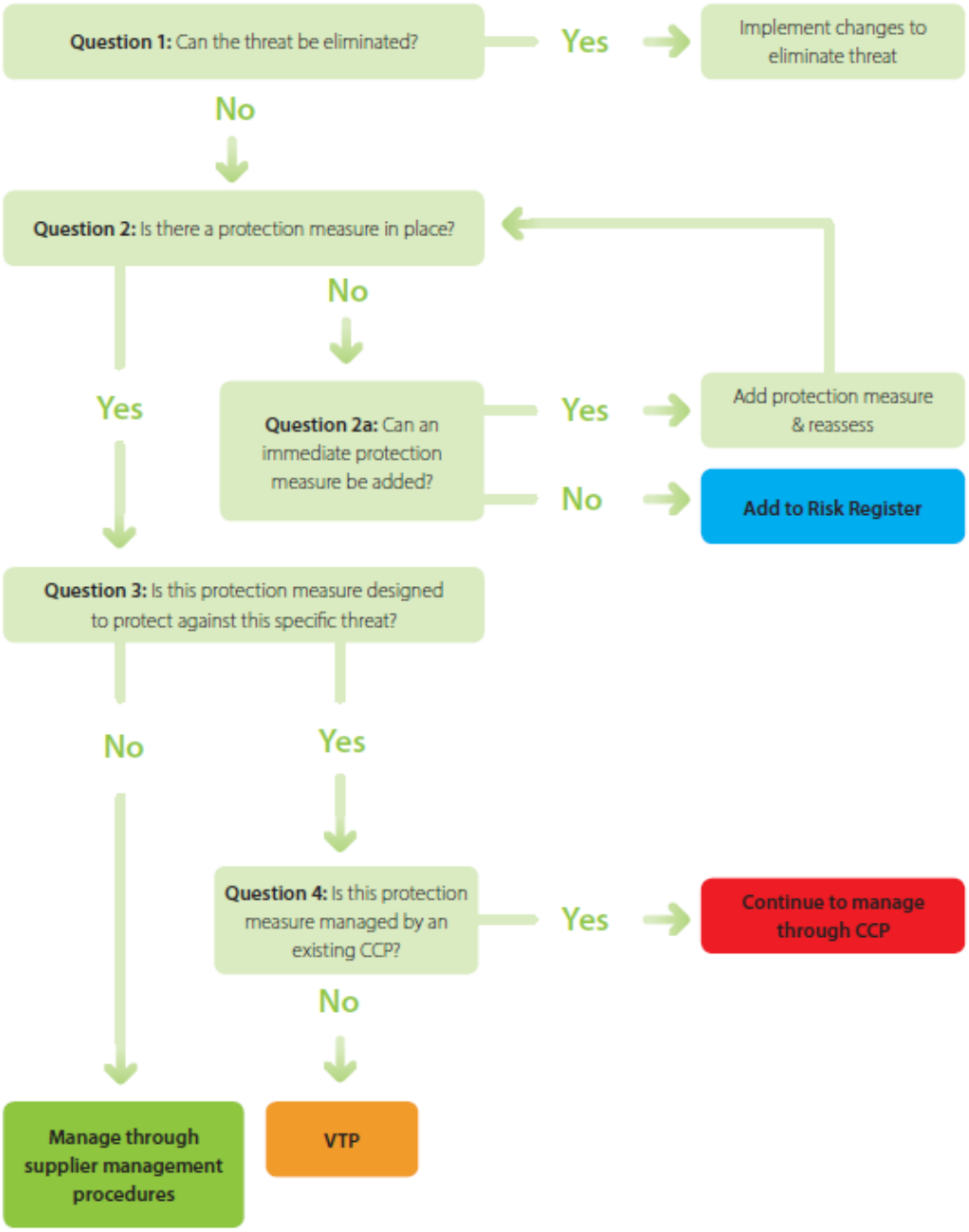
Document name:	**Food defence**
Document reference:	**CPU.FS.POL.002.01**
Date of 1st Issue:	**19 August 2024**
Author:	**Food Safety**
Version number:	**1**

Revision Record		
Issued date of revision	**Version**	**Details of revision**

Appendix I: Potential perpetrators and their motivation

Perpetrator	Characteristics	Motivation
The extortionist	Wants financial gain. Generally wants to remain anonymous. May or may not have the means to carry out the threat. More likely to target high-profile business where negative publicity would have a larger impact.	Financial gain
The opportunist	May be an insider in an influential position therefore able to evade controls. May be driven by commercial factors or pressures such as shortages of raw materials or finished product, which may cause them to act fraudulently.	Pressure (such as pressure to fulfil orders or financial pressure to cut corners)
The extremist or terrorist	Very passionate about their cause, could be religious, political, environmental, or animal rights extremists. Publicity for their cause is a key motivator. May set out to cause harm to the consumer (terrorists). Others such as environmental campaigners, may fear this will damage their cause. The perpetrators may be willing to compromise their personal safety.	Ideological
The irrational individual	The actions of this individual may have no rational motivation or explanation. They may have diagnosed mental health issues. May be deterred by standard security protocols.	No rational motivation, perceived personal grievance
The disgruntled individual	Not limited to the obvious disgruntled employee, includes any individual who feels aggrieved by the business's actions. May also be a supplier who feels mistreated, a local resident or even a customer. Generally more motivated by revenge, or a desire to humiliate the business rather than financial gain. Less likely to be focused on consumer harm.	Personal grievance
The hacker or cybercriminal	Expert in technology. May wish to disrupt business systems or steal sensitive data to use for commercial gain or place in public domain. May not have any direct impact on product, may be more of a threat to business continuity. May be motivated by the 'challenge' of hacking the system.	Financial gain, no rational motivation (this may be seen as the 'challenge' of hacking which would be classed as irrational)
The fraudster	May be large criminal network with significant resources. May see food fraud as high gain for a relatively simplistic crime. May exploit weak border controls for food.	Financial gain

Appendix II: Raw materials vulnerability decision tree



Appendix 3 – Finished goods vulnerability decision tree