PAS 96:2026

Food defence – Protection and prevention from deliberate acts – Guide

Department for Environment, Food & Rural Affairs

Food Standards Agency

bsi

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

Published by BSI Standards Limited 2026

ISBN 978 0 539 29065 3

ICS 67.020, 67.050

Publication history
First published March 2008
Second edition March 2010
Third edition October 2014
Fourth edition November 2017
Fifth (current) edition May 2026

Contents

List of figures

List of tables

Foreword

This PAS was jointly sponsored by the Department for Environment, Food & Rural Affairs (Defra) and the Food Standards Agency (FSA). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on 31 May 2026.

Acknowledgement is given to Leanne Singleton, Food Sure, as the technical author, and the following organizations that were involved in the development of this PAS as members of the Steering Group:

- Agrico UK Limited
- Associated British Foods, plc
- British Frozen Food Federation (BFFF)
- Campden BRI
- Cargill
- Chilled Foods Association (CFA)
- Dairy UK
- Department for Environment, Food & Rural Affairs (Defra)
- Fera Science
- Food and Drink Security Association (FDSA)
- Food Standards Agency (FSA)
- Food Standards Scotland (FSS)
- Food Sure
- Heineken
- McDonalds Europe
- National Cyber Security Centre (NCSC)
- National Farmers Union (NFU)
- National Restaurants Association
- PepsiCo
- Suntory
- Tesco
- University College London (UCL)

Acknowledgement is also given to co-opted members of the Steering Group, together with the members of a wider review panel who were consulted in the development of this PAS.

The PAS process enables a standard to be rapidly developed in order to fulfil an immediate stakeholder need. A PAS can be considered for further development as a British Standard or constitute part of the UK input into the development of a European or international standard.

Supersession

This PAS supersedes PAS 96:2017, which is withdrawn.

Information about this document

This is a full revision of the document, and introduces the following principal changes.

- The document recognizes current UK Government guidance on the rise of cyber incidents.
- The evolving threat environment post Covid-19 (which exposed global supply network fragility and vulnerabilities in international food trade) is addressed.
- The potential impact of climate change on threats to food and supply networks due to disruptions in primary production leading to ingredient scarcity is recognized.
- The effect of food sector developments is anticipated, driven by policies such as "go-green", "carbon neutral", "net-zero" and food waste reduction.

This update also aligns definitions and incorporates global food community learnings.

- Updated vocabulary to match current industry terms, (e.g. "attackers" now referred to as "threat actors").
- Examples of intentional adulteration and food fraud added in an annex;
- Expansion of the Threat Assessment Critical Control Points (TACCP) approach, aligned with the Plan-Do-Check-Act cycle.
- Prioritize food protection, including food defence, while distinguishing it from food fraud/ economically motivated adulteration (EMA) where food protection focuses on intentional harm by threat actors, whereas food fraud involves deliberate deception for economic advantage.
- Addition of other food protection approaches.

The document format has been restructured with prompts for identifying threats, vulnerabilities and mitigation measures relocated to annexes to provide a dedicated set of tools to guide application of the TACCP approach.

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at knowledge.bsigroup.com, or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

Use of this document

As a guide, this PAS takes the form of guidance and advisory recommendations. It is not to be quoted as if it were a specification or a code of practice.

Presentational conventions

The guidance in this document is presented in roman (i.e. upright) type. Any recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Additional commentary, explanation and general informative material is presented in smaller italic type.

Where words have alternative spellings, the preferred spelling of the *Shorter Oxford English Dictionary* is used (e.g. "organization" rather than "organisation").

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

Compliance with a PAS cannot confer immunity from legal obligations.

0 Introduction

0.1 Rationale

This PAS provides broad guidelines to food business operators to help them identify potential threats and associated vulnerabilities in their operations and supply networks. These guidelines use a risk-based approach to prioritise risks and implement targeted mitigation measures. The risks are different across different organizations, operations, processes and products. It is therefore likely that different threat assessments will result in different mitigation measures, proportionate to the individual context.

This PAS is not an external audit tool as it provides guidance, not requirements to demonstrate conformance.

0.2 Focus

The focus of this PAS is on food protection, encompassing food defence, cyber resilience of information technology (IT) and operational technology (OT) and food authenticity (mitigation of food fraud). Food supply networks require a proactive, integrated approach to safeguard the integrity of food and drinks; from malicious contamination, terrorism and tampering, through to adulteration for financial gain, while also addressing broader challenges such as climate change, geopolitical tensions and economic pressures.

The Threat Assessment Critical Control Points (TACCP) approach is explained in this guide. TACCP is a risk-based methodology aligned with the FAO/WHO *General principles of food hygiene*, [1] but with a distinct focus on food defence. The TACCP process (food defence) assumes and builds on a business having an effective Hazard Analysis and Critical Control Point (HACCP) food safety system in place. Many of the precautions taken to ensure the safety of food are also likely to deter or detect deliberate acts.

TACCP encourages business operators to think like threat actors, and anticipate their motivation, capability and opportunity to carry out a deliberate act, and to then implement mitigation measures. As the threat environment continues to change, business operators are encouraged to adopt a proactive approach to food protection and ask the following questions.

a) Who might want to act against us?

b) How might they do it?

c) Where are we vulnerable?

d) How can we stop them?

Information sharing and industry collaboration are critical to proactively addressing emerging and evolving threats. Since the initial publication of this PAS in 2008, numerous intentional adulteration incidents intended to cause harm, food terrorism, have provided valuable insights into threats and their impacts on food businesses. This highlights the importance of analysing past events to better predict and prevent similar incidents in the future [2]. Much of the need to stay abreast of current threats is due to new and emerging technologies.

No process can guarantee that food or the food supply network is not targeted by criminal activity but applying this PAS can make it less likely. This PAS complements existing business risk and incident management systems. It also acknowledges that, while cybersecurity considerations are increasingly incorporated into food protection, dedicated cybersecurity plans are distinct from food defence plans due to their primary focus on protecting IT and OT.

The adoption of this PAS can help businesses to manage risk within the framework of their specific regulatory requirements and other Global Food Standards Initiative (GFSI).[1)] This guide is intended to be practical and easy to use, written in everyday language and applied in a common sense rather than legalistic manner.

[1)] Available at https://mygfsi.com/who-we-are/overview/

1 Scope

This PAS provides guidance on prevention and mitigation against deliberate acts to food and drink, and their supply networks, using the Threat Assessment Critical Control Points (TACCP) risk management approach.

This PAS covers intentional acts of:

a) malicious contamination includes intentional and criminal acts, such as those carried out for ideological motives, extortion, or espionage;

b) disruption of business operations through cybercrime; and

c) economically motivated adulteration (EMA) or food fraud, including substitution, dilution, adulteration, and counterfeiting.

This PAS does not cover food safety and unintentional incidents, such as accidental contamination or naturally occurring hazards.

***NOTE** These are addressed through effective Hazard Analysis Critical Control Point (HACCP) food safety management systems.*

This PAS applies to organizations of all sizes and at all points in the food and drink supply network, from primary production through to manufacturing, distribution, retailing and foodservice. The guidance is particularly valuable for small and medium sized enterprises (SMEs) who might not have access to specialist risk management expertise.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this PAS, the following terms and definitions apply.

3.1 adulteration

reducing the quality and safety of a food product through the inclusion of another substance, removal of a product component or manipulation of the process to alter the finished product

NOTE *In the context of food defence, adulteration is the intentional contamination or manipulation of food and drink products motivated by intention to cause harm and economic gain. These acts may involve adding, substituting or tampering with substances to deceive quality or authenticity tests or deliberate omission of a stated ingredient to render food unsafe for consumption, including potential terrorism-related threats aimed at causing wide-scale public health impact, supply network disruption or societal harm.*

[SOURCE: Food Crime Strategic Assessment 2024 [3] modified – add "and safety", "or removal of a product component" and "manipulation of the process to alter the finished product"]

3.2 authenticity

product of genuine origin and not copied or falsified

3.3 cyber security

protection of devices, services and networks – and the information on them from theft or damage

NOTE *Cybersecurity includes the physical security internal devices, services and networks to prevent site interference. For example, physically protected in a secure room with restricted access or electronically protected though unique passwords and logins.*

[SOURCE: NCSC Advice and guidance – Glossary [4]]

3.4 food defence

procedures adopted to protect of food and drink and their supply networks from malicious and ideologically motivated attack leading to contamination or supply disruption

NOTE *The term "food supply network" is preferred over "food supply chain" for longer, more complex systems. While "chain" suggests a simple, linear process (which may apply to short, straightforward networks), "network" better reflects the intricate web of multiple suppliers, processors, logistics providers, distributors, and other interconnected actors typical in global or extended supply systems.*

3.5 food fraud

deliberate and intentional substitution, addition, tampering, or misrepresentation of food, food ingredients, or food packaging; or false or misleading statements made about a product for economic gain

[SOURCE: Defining the public health threat of food fraud [5]]

3.6 food protection

integrated practice of safeguarding the global food system by encompassing the essential elements of food safety, food quality, food defence, food authenticity, workplace health and safety, physical and cyber information technology (IT)/operational technology (OT) security and the resilience of critical infrastructure

NOTE *Collectively, these key elements are leveraged to protect public health, strengthen consumer trust, ensure fair trade and potentially reduce risks across the food supply network in alignment with regulatory and food industry standards.*

3.7 food supply network

interconnected system of actors, processes, activities and infrastructure involved in producing, processing, storing, transporting, distributing and delivering food from its origin to end consumers

NOTE *An example of a food supply network is given in Annex A.*

3.8 hazard

something that can cause loss or harm which arises from a naturally occurring or accidental event or results from lack of necessary competence on the part of the people involved

3.9 Hazard Analysis Critical Control Point (HACCP)

science-based and systematic, identifies specific hazards and measures for their control to ensure the safety of food

[SOURCE: General principles of food hygiene [1]]

3.10 insider

person who has, or previously had, authorised access to or knowledge of the organization's resources, including people, processes, information, technology, and facilities

[SOURCE: National Protective Security Authority (NPSA) [6]]

3.11 insider threat

insider, or group of insiders, that either intends to or is likely to cause harm or loss to the organization

[SOURCE: National Protective Security Authority (NPSA) [6]]

3.12 mitigation measure

specific action taken to eliminate, reduce or control an adverse effect

[SOURCE: Department of Homeland Security (DHS) [7]]

3.13 personnel security

protecting organizations from the risks associated with the people it employs

NOTE *Personnel security principles help ensure the trustworthiness of an organization's own employees and contractors. These principles may also extend to the employees and contractors of suppliers as part of vendor accreditation processes (not to be confused with personal security).*

[SOURCE: NCSC Advice and guidance – Glossary [4], modified – note added]

3.14 product tampering

<food fraud> type of food fraud which includes the deliberate changing of food characteristics so that they no longer match the implicit or explicit claims associated with the product

NOTE 1 *Product tampering is the deliberate alteration of a food product or its packaging. It includes: subjecting the product to an unapproved or undeclared process, removing a required substance, adding or replacing a substance (adulteration), or other intentional mischievous acts.*

NOTE 2 *Malicious tampering refers to deliberate tampering with the intent to cause harm (e.g., sabotage or extortion). It falls under food defence rather than food fraud, which is primarily economically motivated.*

[SOURCE: BS EN 17972:2024, **3.16**, modified – note 1 to note 5 revised and combined into note 1 and note 2]

3.15 risk

possible future outcomes that can be describes in terms of their chances of occurrence, and the impact they would have if realized

[SOURCE: NCSC advice and guidance – Glossary [4], modified – "we" removed and amended to "can be described"]

3.16 seal numbers

unique alphanumeric identifier printed or embossed on tamper-evident security seals applied to containers, pallets, packaging or vehicles in food supply networks

3.17 threat

credible potential for intentional, malicious acts by individuals or groups that could result in adulteration, contamination, or disruption of food systems, leading to harm to public health, economic loss, or loss of consumer confidence

3.18 Threat Assessment Critical Control Point (TACCP)

systematic approach to identify potential threats, assess vulnerabilities and determine if mitigation measures against intentional acts aimed at harming the organization, its operations, processes or products are needed

3.19 threat environment

external, constantly evolving ecosystem of actors, threats, vulnerabilities and attack methods that can target or impact an organization, independent of its internal controls

3.20 vulnerability

weakness, or flaw, in software, a system or process

NOTE *An actor exploits these to, for example, gain unauthorised access to a computer system or the vulnerability of a process step could lead to intentional adulteration.*

[SOURCE: NCSC Advice and guidance – Glossary [4], modified – second sentence changed to a note]

4 Types of threats

4.1 General

Deliberate acts against food, drink and their supply networks can take various forms including:

a) intentional adulteration to cause harm (food defence), see **4.2**;

b) disruption of business operations (cybercrime), see **4.3**; and

c) intentional adulteration for economic gain (food fraud), see **4.4**.

For examples of reported cases for different types of threats, see Annex B.

4.2 Intentional adulteration to cause harm (food terrorism)

4.2.1 Malicious contamination

Malicious contamination might be motivated by the intent to cause localized or widespread illness or death, and in some cases, threat actors deliberately introduce contaminants, including allergens, not normally present in the product or readily accessible within the facility. However, threat actors seeking publicity or to extort money, are more likely to use contaminants capable of causing widespread harm.

4.2.2 Ideologically motivated malicious contamination

Ideologically motivated malicious contamination refers to deliberate acts to advance political, religious or extremist agendas, typically aiming to cause public harm, societal disruption, or influence events like elections. The primary goal might be to undermine confidence in the food supply network or to generate publicity for the cause.

4.2.3 Extortion

Extortion is typically motivated by the desire to obtain financial gain or cause reputational harm. Even a small number of contaminated items can effectively demonstrate a threat actor's intent, capability and opportunity, creating sufficient public concern and media attention to pressure the target. These actions are particularly attractive to threat actors when the product is a sensitive food item, such as an infant food, or when the targeted company is high profile.

4.2.4 Espionage

The primary motivation for espionage is to obtain commercial advantage by accessing intellectual property from an organization. Criminals and organized crime groups, often state sponsored or protected, might attempt to extract confidential information from executives and employees through blackmail, extortion (see **4.2.4**) or other coercive threats. Common tactics include gathering compromising information for leverage, recruiting or coercing insiders, and remotely targeting IT systems.

4.3 Disruption of business operations (cybercrime)

4.3.1 General

Cybercrime motivated by intentional disruption aims to harm, disrupt or exploit an organization's operations through targeted cyberattacks, generally for financial gain. Advances in information and communication technologies, such as Internet of Things (IoT) sensors, Global Positioning System (GPS)-guided or tracked equipment and cargo, cloud-based systems, automated processes and robotic equipment provide threat actors with opportunities to target both IT networks and operational technology (OT).

A successful cyberattack can cause significant disruption by:

a) compromising or encrypting critical systems (e.g. via ransomware), which stop production, processing, transport or automated processes, leading to production losses, supply shortages, equipment downtime or animal welfare issues;

b) theft of proprietary data, such as financial records, employee information, confidential recipes or processes, marketing strategies, and supplier/customer details enabling competitive sabotage or further harm; and

c) enabling cyber fraud against the business, its suppliers, or its customers.

NOTE *In England and Wales, for the year ending March 2022, the Office for National Statistics reported approximately 4.5 million fraud offences, of which 61% were cyber-related, and 1.6 million incidents of computer misuse [8].* Scottish Crime and Justice Survey 2023/24: Main findings *indicate there were approximately 456 000 fraud related crimes and 68,000 crimes of computer misuse [9].*

4.3.2 Cyber-enabled industrial espionage or hacking

A successful cyberattack can compromise an organization's proprietary data, such as financial records, employee information, confidential recipes or processes, marketing strategies and supplier/customer details. Another form of cybercrime is cyber-enabled industrial espionage, or hacking, which involves unauthorized access to computer systems, typically with malicious intent.

4.3.3 Cyber-enabled fraud

Cyber-enabled fraud leverages technology to amplify traditional crimes, often exploiting an individual's or an employees' limited understanding of digital systems through phishing, social engineering or deceptive electronic communications to gain unauthorized access.

For further information on techniques used on cybercrime, see Annex C.

4.4 Intentional adulteration for economic gain (food fraud)

4.4.1 General

Food fraud is the intentional act of adulteration or deception for financial gain. It involves deliberate misrepresentation for monetary gain, typically involving the quality, origin, or composition of a product. Common examples include:

a) falsely claiming the origin of ingredients (e.g. geographic source, plant, animal species or breed);

b) knowingly selling food past its original use by date;

c) intentionally selling contaminated or unsafe food;

d) misrepresenting the true nature of the food (e.g. substituting one animal or plant species for another);

e) replacing a product with a cheaper alternative (e.g. farmed salmon labelled and sold as wild-caught);

f) illegal processing or handling outside legal regulations (e.g. recycling animal by-products back into the human food chain or slaughtering/preparing products without the required regulatory oversight); and

g) Importing and selling products under the same or similar brand that fail to meet the destination country's rules (e.g. foreign soft drinks with the same branding as UK versions but produced elsewhere, without paying the UK Soft Drinks Industry Levy (SDIL) or complying with local additive limits).

These acts are deliberate and aimed at financial benefit, though they can sometimes pose health risks too. From a threat actor's perspective, a successful food fraud adulteration is one that remains undetected. Detection often occurs through audits revealing unexplained purchases or quantity discrepancies, routine testing, process verification or internal checks.

4.4.2 Economically motivated adulteration (EMA)

4.4.2.1 Adulteration

The common factor in most cases of EMA is that the adulterant is neither a food safety hazard, nor readily detectable, as easy identification would undermine the fraud. Common adulterants include water, sugar, starch, or other ingredients that would normally require declaration on the label but are either undisclosed or added in undeclared proportions. High value products are particularly susceptible. Examples of adulteration for economic gain include substitution, dilution and additions.

4.4.2.2 Misrepresentation

Misrepresentation occurs when a product is deliberately presented with false or misleading claims regarding its nature, quality, origin, composition, or other attributes for economic gain.

4.4.3 Counterfeiting

Counterfeiting is the deliberate substitution of inferior foods, drinks or packaging in place of those of a reputable brand. Counterfeiting is conducted purely for financial gain; however, brand reputation can also be harmed. While petty criminals might participate in opportunistic acts, the activity is typically conducted by organized crime groups that take advantage of the scale and complexity of international supply networks. Counterfeit products might be produced in unsanitary conditions and be contaminated or unsafe for human consumption, potentially leading to further reputational damage.

Organized groups employ sophisticated technologies, ranging from high quality printing to complete packaging lines and moulding, to produce convincing replicas of labels and packaging. Additional tactics include the theft of genuine packaging materials or the unauthorized refilling and resale of single-use containers, enabling widespread fraudulent substitution throughout the food and drink sector.

4.4.4 Evolving food sector threats

4.4.4.1 Climate change causing potential supply disruption

Climate change can increase food fraud risk by disrupting crop yields, causing resource scarcity, price volatility and extended supply networks for climate-sensitive commodities (e.g. olive oil, honey, spices, coffee, cocoa and seafood). This can make substitution, addition, dilution and counterfeiting even more financially attractive. Resource shortages can also intensify social grievances and ideological motives to carry out deliberate acts.

Extreme weather events disrupt infrastructure and security controls, creating temporary vulnerabilities that threat actors could exploit. While recovery periods after extreme events can increase employee stress, reliance on temporary employees or relaxed protocols, can potentially increase opportunities for threat actors.

4.4.4.2 Efforts to meet environmental social governance (ESGs)

ESG commitments, especially carbon-neutral or net-zero claims, can inadvertently create vulnerabilities for food fraud, misuse or diversion. Pressure to meet these claims often drives companies to source from new, alternative or distant suppliers, resulting in longer, more complex supply networks with reduced visibility and oversight. This might increase risks of deliberate substitution, adulteration, or contamination.

Perceived greenwashing or unsubstantiated claims might also encourage ideologically motivated insiders or external activists to sabotage products, aiming to expose perceived hypocrisy and cause reputational damage. The increasing reliance on new digital traceability systems for verifiable ESG metrics can increase vulnerability of the entire system to cyberattack.

4.4.4.3 Donation of surplus edible foods

Donating surplus edible foods to food rescue organizations to reduce food waste, adds new supply network partners and processes which might require assessment. Potential vulnerabilities can arise from the reliance on volunteer personnel, lack of secure food storage facilities and limited oversight, especially given the lower intrinsic value placed on surplus food products. These factors might increase the risks of food fraud and contamination, or diversion of donated food into unauthorized channels or black markets.

5 Understanding threat actors

5.1 General

The success of a deliberate act targeting food or the food supply network depends on the following key factors.

a) Motivation and determination:

   Does the threat actor have the determination to persist in overcoming barriers? When barriers appear robust and success unlikely, many potential actors seek easier targets.

b) Capability:

   Does the threat actor have the necessary skills, resources and expertise? A group is generally more likely to have access to more resources and specialised capabilities than individuals.

c) Opportunity:

   Does the threat actor have reasonable access, or can they possibly gain access to carry out the act? Physical attacks require direct access to the target area, whereas cyberattacks can be launched remotely via networked computers, smart phones or other connected devices.

d) Deterrence:

   Is the likelihood of detection or the risk of potential penalties likely to discourage the threat actor?

Threat actors differ significantly in their intent, purpose and mode of operation. Acts of intentional adulteration are more likely to be detected, increasing the probability of the actor being identified and apprehended. In contrast, food fraud and cybercrime actors typically prioritize avoiding detection and minimizing attention. The characteristics of different threat actors are described in **5.2** to **5.8** and an individual or group might have traits of more than one actor type.

5.2 Cyber criminals and other malicious digital actors

Cyber criminals deliberately subvert controls on computerized information and communication systems to:

a) impair their effective operation;

b) steal or corrupt the data they hold; and/or

c) disrupt internet-based business activities.

These actors might also align with other type of threat actors. Their methods are often opportunistic rather than targeted, such as large-scale phishing campaigns sent to thousands, where even one successful response can yield significant rewards.

Motivations include criminal, political or financial gain, as well as mischievous demonstrations of technical skill in bypassing protective systems. A key attraction of cybercrime is the perceived anonymity (or deniability), which makes proving guilt difficult. Another key attraction is remote access to internet-connected systems, which allows attacks to be launched from afar. Certain jurisdictions appear to condone and might even actively encourage such actions.

The rapid increase in cybercrime, particularly the use of ransomware, has led many businesses to conclude that an attack is inevitable and to prioritize planning, system resilience and incident response accordingly.

5.3 The opportunist

Opportunist threat actors often hold influential positions within an operation, giving them the ability to evade or bypass internal controls. While they might possess some technical knowledge, their primary advantage is legitimate and ready access. They are generally deterred by the consequences of detection, particularly from unannounced customer visits, audits or random product sampling and analysis that could occur at any time. A supplier facing the risk of non-delivery might opportunistically adulterate products, hoping the act remains undetected. In some cases, the individual might rationalize the adulteration as acceptable. For example, substituting chicken for pork in a sausage while maintaining that it still qualifies as "meat" and will likely do no harm.

5.4 The extremist

Extremists are defined by an uncompromising commitment to their cause, often leading them to distort its context and disregard broader consequences. Their dedication can be limitless, with determination to advance the cause overriding most constraints or deterrence. Many extremists intend to cause harm and actively seek publicity following an incident. They have a high level of motivation and while the risk of failure is a potential deterrent, the risk of sustaining personal injury or being captured after the event is not. These threat actors are typically focussed, resourceful and innovative in devising methods to carry out deliberate acts.

Single-issue, extremist or terrorist groups might deliberately target business disruption and reputation damage while avoiding mass harm, in order to maintain public sympathy or support for their cause.

5.5 The irrational individual

Some individuals act with no rational motive. Their preoccupations and perspectives can be distorted to such an extent that they have an altered sense of reality and their actions can be difficult to predict or prevent. Such individuals can often be deterred by measures that make access to targets more difficult or that increase the likelihood of detection.

5.6 The disgruntled individual

Disgruntled individuals believe they have been treated unfairly by the organization and see direct revenge on the organization as being an acceptable response. Generally operating alone, they might include current or former employees, contractors, agency workers or supply network partners. They often have expert knowledge of the operation and suitable access.

Insiders can pose a serious threat, but usually aim to cause embarrassment, reputational damage or financial loss rather than harm the public. External threat actors are more likely to falsely claim or boast of having committed a deliberate act than actually being able to do so.

5.7 The professional criminal

Organized crime groups often perceive food fraud as a low-risk, high-reward opportunity that is relatively straightforward to execute and highly profitable, with a low probability of detection and relatively lenient penalties if convicted. The globalized nature of food trade is characterized by relatively free movement of materials across jurisdictional boundaries. This creates an environment that allows professional criminals and, in some cases, terrorist groups, to exploit supply network complexity and vulnerabilities. Additionally, the anonymity provided by the internet and the ease of remote access to electronic systems have made cybercrime increasingly attractive to professional criminals.

Professional criminals are best deterred by maintaining robust systems and sustained collaboration between food businesses, national authorities, and international law enforcement agencies.

5.8 The extortionist

The extortionist is motivated by financial gain through deliberate acts and prioritizes avoiding detection. Targets are typically high-profile organizations that face significant reputational or financial damage from adverse publicity.

Extortionists can operate alone and are often resourceful, secretive and self-interested. Some individuals might issue threats to harm a business without possessing any capability. In such cases, while the business might assess the threat as lacking credibility, it should always treat the claim seriously, report it promptly to the appropriate authorities, and respond in accordance with established incident protocols (see Clause **9**).

6 Threat Assessment Critical Control Point (TACCP)

6.1 Broad themes

TACCP forms a key element of wider risk management and the food protection framework. Its primary objectives are to:

a) reduce the likelihood (chance) of a deliberate malicious act;

b) mitigate the impact (consequences) should such an event occur;

c) safeguard the organization's reputation;

d) meet global food sector expectations and support trading partner requirements; and

e) provide customers and the public with confidence that proportionate steps are in place to protect food from intentional harm.

TACCP aligns with the Plan-Do-Check-Act (PDCA) cycle, providing a systematic method to identify and assess threats associated with specific operational vulnerabilities (see Figure 1). Recognising food defence as an ongoing process, the PDCA model facilitates regular review and continual improvement.

The risk assessment can be split into two separate processes.

1) Intentional adulteration (malicious contamination/tampering):

   This part evaluates risks from deliberate acts intended to cause harm. It focuses on vulnerabilities that could enable malicious contamination or tampering and draws on multidisciplinary expertise from security, human resources, operations, product development, logistics and distribution.

2) Food fraud/EMA:

   This part assesses risks from intentional adulteration motivated by economic gain, (e.g. substitution, dilution, addition, or misrepresentation). It relies on input from procurement and technical/quality assurance specialists to identify vulnerabilities in the supply network.

   These two risk assessment processes are often interlinked, sharing common threats and vulnerabilities in key areas such as:

   i) incoming raw materials and suppliers where substitution, dilution or malicious contamination could occur due to supply network weaknesses or insider actions;

   ii) packaging and labelling where tampering, counterfeiting, mislabelling or substitution for economic gain or malicious intent could occur;

   iii) accessible points in the production process where deliberate addition of substances could occur; and

   iv) employee access and insider threats where disgruntled employees could carry out an act of sabotage (e.g. intentional contamination for harm) or EMA (e.g. substitute or dilution for profit).

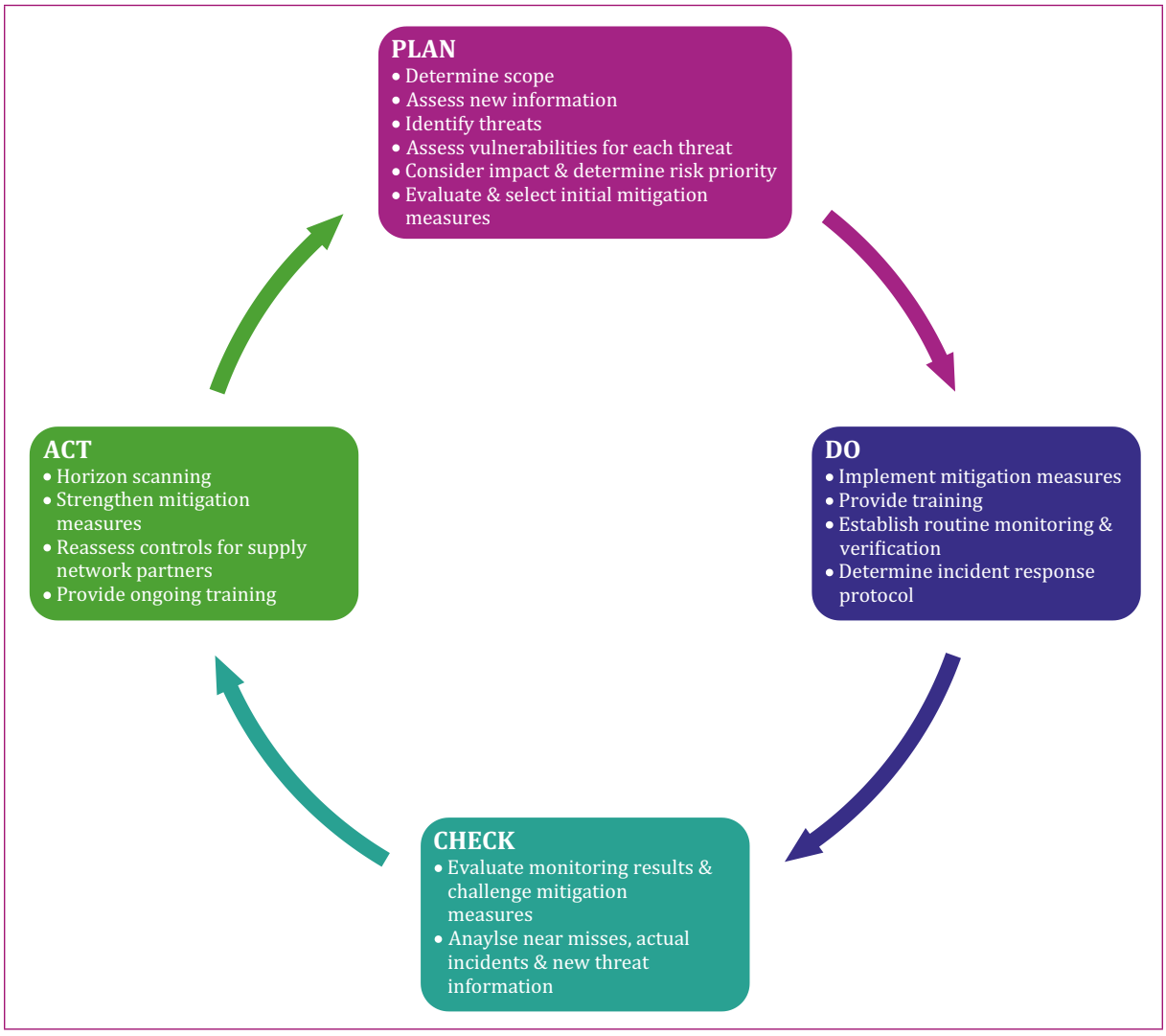
   NOTE *The outline is illustrative only and is representative of all steps that might apply to all organizations.*

6.2 The TACCP food protection team

A cross-functional TACCP team brings together individuals with diverse experience to identify potential threats, while systematically evaluating vulnerabilities that could allow those threats to succeed. A smaller core (or designated team leader) may then be responsible for conducting the detailed risk assessment, selecting appropriate mitigation measures and implementing them.

***NOTE** For small businesses, forming a cross-functional team might not be feasible and it might be a job for one person.*

Figure 1 – Outline of TACCP process



The team should adapt the TACCP approach to best meet their needs, such that it addresses the following fundamental questions.

a) Who might want to act against us (see **6.3.4**)?

b) Where are we most vulnerable (see **6.3.5**)?

c) How can we reduce the risk by mitigating vulnerabilities against the threat(s) (see **6.4** to **6.6**)?

The TACCP team requires specialist knowledge to develop and maintain a food protection plan. This will likely include knowledge and expertise in the following areas:

1) security, (e.g. physical security, IT & and OT security, personnel security);
2) human resources;
3) food technology;
4) food safety and quality;
5) process engineering;
6) production and operations;
7) purchasing and procurement;
8) distribution and logistics;
9) information technology;
10) legal;
11) communications;
12) commercial/marketing; and
13) senior leadership and management.

The team may also consult with a broader group of specialists including environment, health & safety (EHS) and the business continuity team.

NOTE 1 *The team may include representatives of key suppliers and customers.*

NOTE 2 *While the HACCP team might serve as a starting point, expertise beyond food safety is often needed. The business continuity team could be a more suitable model. The TACCP team is typically an established group, able to regularly review decisions, adjust priorities and revise mitigation measures.*

As the TACCP process can cover sensitive information, team members should be knowledgeable of actual processes, trustworthy, discreet and have an awareness of the implications of the TACCP process. This might include non-disclosure agreements where appropriate.

6.3 Application of TACCP

6.3.1 Planning (Plan)

The planning stage of TACCP identifies potential threats and associated vulnerabilities relevant to the organization, its operations and products. These are evaluated to assess the overall risks to the business. The risks are then prioritised to develop an action plan with specific mitigation measures to protect against intentional contamination.

6.3.2 Determine scope

The TACCP team should first determine the scope of the food defence, (or food protection) plan. The scope can be broad, covering the entire organization, its systems, and operations, or focused, targeting individual facilities, specific processes or particular products.

6.3.3 Assess new information

The TACCP team should assess all new and emerging information including:

a) emerging threats, reports and trends related to new tactics, motivations or vulnerabilities;

b) amplification or escalation of existing threats;

c) changes to transportation, distribution or shipping;

d) changes to the wider supply network, including raw material sourcing, supplier arrangements and geopolitical events; and

e) potential impacts on product safety, integrity or brand reputation.

6.3.4 Identify threats

The TACCP team can systematically identify probable and potential threats to the organization, its operations and specific products. These threats might come from people or groups who deliberately cause harm, whether internal (insiders), external or third parties (supply network partners or contractors). Examples of these include the following.

a) Threats to the organization:

   Identify threats to the overall organization and its systems, especially electronic/IT/OT systems (see Table D.1);

b) Threats to operations:

   Identify threats that could exploit vulnerable internal process steps or that arise from outsourced activities (e.g. transport or warehousing activities) (see Table D.2); and

c) Threats to product:

   Identify threats targeting a specific product with biological, chemical, physical or radiological contaminants. This may involve considering agents/adulterants which are able to withstand processing treatments, (e.g. cleaning procedures, heat treatments, and interactions with other ingredients that could neutralize, denature or remove them) (see Table D.3).

6.3.5 Assess associated vulnerabilities for each threat

For each threat, the TACCP team should identify any associated vulnerabilities where a threat actor could succeed in causing harm. They should also take into account the risk posed by individuals or groups with access to the product or process at points of vulnerability. Vulnerabilities can arise from organizational and site changes and the introduction of new products or processes. The TACCP team might literally ask themselves, "If we were trying to undermine our business, how could we do it?".

6.3.6 Consider impact to determine risk priority

For each identified threat and its associated vulnerability, the potential impact of the threat succeeding should be assessed (see Clause **7**) and the full range of possible outcomes evaluated, including:

a) human health effects and public safety risks;

b) business, financial and reputational damage to the organization; and

c) broader effects on other parties in the supply network (e.g. from grey market diversions, contamination incidents, products recalls).

Any risk priority rating that does not align with the TACCP team's overall logic and consensus should be reviewed and revised.

6.3.7 Evaluate and select initial mitigation measure(s)

The proposed mitigation measures should be evaluated to confirm the organization has the resources, training, personnel, and systems to implement and sustain it/them reliably.

6.4 Implementation of mitigation measures (Do)

6.4.1 General

During the implementation stage of TACCP, the organization puts the selected mitigation measures into effect, delivers relevant training, establishes monitoring and verification procedures for those measures and develops an incident response plan.

6.4.2 Implement mitigation measures

Implement mitigation measures proportionate to the risk should be implemented with a focus on prevention (e.g. access controls), detection (e.g. monitoring, tamper evident seals), or reduction of impact. The selected mitigation measures should be documented and implemented, maintaining confidentiality where required.

6.4.3 Provide training

Role-specific training should be delivered to support the implementation of mitigation measures which may include food protection/ food defence awareness, recognizing suspicious behaviour, reporting and escalating suspected or actual incidents.

6.4.4 Establish routine monitoring and verification

Routine monitoring activities should be established to verify the effective implementation of the selected mitigation measures. In addition, verification procedures should be implemented to confirm the continued effectiveness of these measures in addressing identified threats and reducing or eliminating vulnerabilities.

6.4.5 Determine an incident response protocol

An incident response protocol should be developed and tested to manage a potential incident (see Clause **9**).

6.5 Check/review (Check)

6.5.1 General

In the check/review stage of TACCP, the ongoing adequacy and effectiveness of the mitigation measures are confirmed. Near-miss incidents confirmed incidents and updated threat intelligence are systematically reviewed to identify any deficiencies or gaps in the mitigation measures.

6.5.2 Evaluate monitoring results and challenge mitigation measures

Monitoring data from the mitigation measures should be reviewed to confirm their continued adequacy and effectiveness. The mitigation measures should be challenged (e.g. through audits, testing or scenario reviews) to assess their robustness and ongoing suitability.

6.5.3 Analyse near-misses, actual incidents and new threat information

Near-miss events, confirmed incidents (including security breaches, suspected tampering, or authenticity issues), and new or emerging threat intelligence should be investigated. These insights should be used to detect gaps or deficiencies in mitigation measures that can be addressed by the TACCP team.

6.6 Improvement of food protection plan (Act)

6.6.1 General

During the act stage of TACCP, the organization revises and updates the identified threats, vulnerabilities, and associated risks in response to findings from the check stage. This enables:

a) the improvement of existing mitigation measures to close identified gaps;

b) the reassessment of food protection expectations and controls for supply network partners; and

c) the provision of ongoing training to relevant personnel.

6.6.2 Horizon scanning

The TACCP team should proactively perform horizon scanning to detect early indicators of risk. This involves systematically gathering and evaluating information from credible and reliable sources to identify:

a) new and emerging threats;

b) developments or changes that may escalate the likelihood, capability or impact of existing threats; and

c) local, regional, or emerging geopolitical/economic issues that could heighten vulnerabilities.

The TACCP assessment should be revised promptly based on new threat intelligence, analysis of incidents/near-misses or changes in the operation, such that the food protection plan remains current, proportionate and effective (see **10.6**).

6.6.3 Strengthen mitigation measures

Improve, add or re-evaluate based on audit findings, actual incidents or challenge studies to determine if new mitigations measures are needed.

6.6.4 Reassess controls for supply network partners

Expectations and controls for all supply chain partners should be reviewed and updated, including suppliers, transportation carriers, contractors, service providers and distributors to maintain coordinated protection against deliberate threats.

6.6.5 Provide ongoing training

Training programmes should be updated as needed and provide routine refresher training to personnel involved in food protection activities, which maintain ongoing competence in recognizing threats, implementing controls, reporting incidents and fulfilling role responsibilities (see **10.3**).

7 Risk assessment

7.1 General

Risk arises from the interaction of a threat with an associated vulnerability. A vulnerability by itself does not automatically create risk, as there needs to be a credible threat capable of exploiting the vulnerability. Similarly, a threat without a relevant vulnerability does not represent a risk to the organization.

7.2 Evaluating threats

The TACCP team should assess each potential threat by evaluating the threat actor's specific motivation and their realistic capability to successfully carry out a deliberate act. Threats should be assessed in a manner that accurately reflects their real-world complexity. Threats can be categorized as either:

a) single/individual threats that are – standalone malicious acts or events (e.g. a lone insider deliberately introducing a contaminant at a single process step); or

b) layered/complex threats that are – sophisticated scenarios involving multiple coordinated elements, sequential steps, combined vulnerabilities or interdependent actions, (e.g. an external threat actor colluding with an insider to gain access or a threat amplified by cyber intrusion enabling physical access to a site or process).

When evaluating layered or complex threats, the team should assess:

1) the overall likelihood of a successful deliberate act;

2) the interconnections between individual steps or elements; and

3) the cumulative impact if the entire sequence succeeds rather than assessing each threat in isolation.

7.3 Identifying vulnerabilities

7.3.1 General

The TACCP team should systematically identify and evaluate vulnerabilities associated with each identified threat. For a list of question prompts to assist the TACCP team in identifying and assessing vulnerabilities, see Annex E.

7.3.2 Vulnerabilities to malicious contamination

Vulnerabilities to malicious contamination vary depending on factors such as product type, production process, type of packaging and the degree of access to the product both before and after production, prior to reaching the consumer.

7.3.3 Cyber/IT/OT vulnerabilities

Cyber vulnerabilities can arise from any connected systems, devices, or technologies used throughout the operation. If these are not kept up-to-date with security patches and updates, they can be disabled, compromised, hacked, or bypassed, significantly increasing the site's overall vulnerability to deliberate acts.

7.3.4 Food fraud vulnerabilities

A typical feature of EMA (see **4.4.2**) is the deliberate substitution of a lower-cost or inferior ingredient for a high-value component. Products with provenance or identity-preserved claims, such as organic, non-GMO or protected designations of origin, have elevated vulnerability for EMA. The actors typically have ready access to lower-value substitutes that are visually, chemically, or otherwise indistinguishable from the authentic product.

7.3.5 Food supply network vulnerabilities

Food supply networks are inherently vulnerable due to their complexity and high interdependence among the many actors present. Longer, more globalized, and less transparent supply chains amplify these risks by:

a) increasing the number of intermediaries and touchpoints;

b) reducing visibility and traceability, making it harder to monitor quality and detect issues (e.g. contamination or adulteration); and

c) heightening exposure to unforeseen events, as interdependencies can lead to multiple failures.

7.4 Risk assessment

7.4.1 General

For each identified threat, the TACCP team should:

a) assess the likelihood of occurrence, taking into account the threat actor's motivation, their opportunity, access and existing system or process vulnerabilities; and

b) evaluate the potential impact or consequences should the threat succeed.

Combining the likelihood and impact scores provides an overall threat priority risk rating. This prioritized risk rating enables the TACCP team to focus attention, resources and mitigation efforts on the threats that pose the greatest risk to the organization, its operations or its product.

7.4.2 Likelihood

The likelihood of a deliberate act can be evaluated by considering threats in terms of:

a) whether success would enable the threat actor to achieve their objective;

b) whether a threat actor would prefer other targets, which might offer higher visibility, value or vulnerability; and

c) historical incidents within the organization or in similar operations (comparable in terms of product type, process, scale or sector).

Vulnerabilities can be evaluated in terms of:

1) whether a deliberate act would likely be detected before causing significant impact;

2) whether the threat actor could gain realistic access to the product or process; and

3) whether existing mitigation measures would effectively deter the threat actor.

Likelihood can be assessed as point-in-time or over a defined period (e.g. the next 5 years).

7.4.3 Impact

The potential impact of a malicious act, should be assessed using two criteria:

a) human health and public safety consequences; and

b) business, financial and reputational consequences.

Organizations may choose to implement additional proportionate mitigation measures for threats rated as high or very high risk.

NOTE *Threat priority relies on subjective judgment; a low priority rating does not mean that the threat can be ignored or left uncontrolled.*

For an example risk assessment scoring and matrix, see Annex F.

7.5 Documenting the risk assessment

The TACCP risk assessment should be documented. This demonstrates the systematic application of the TACCP process and provides evidence of due diligence. The principles outlined in this PAS should be integrated into the organization's existing food safety and quality system, as well as other risk management and crisis management procedures.

The two fictional case studies, provided in Annex G are adaptable and may be customized to align with the specific requirements of an individual organization.

8 Mitigation measure

8.1 General

Mitigation measures are intended to reduce an organization's vulnerability to deliberate acts against its operations, processes or products. A proportionate combination of physical, process/engineering, technology, product, procedural and behaviour measures that are directly aligned with the risks identified in the TACCP assessment should be implemented. These mitigation measures, whether applied individually or in combination, should be tested and validated to confirm their effectiveness. Periodic challenge testing is recommended to expose any remaining weaknesses.

8.2 Physical access mitigation measures

The goal of physical mitigation measures is to reduce the opportunity for an intentional act to occur by limiting access only to authorized people. Only individuals with a genuine need should be allowed access to critical processes or areas. Examples of mitigation measures include:

a) perimeter security (fencing, gates, lighting);

b) access control systems (biometrics, keycards, turnstiles);

c) closed-circuit television (CCTV)/video surveillance system (VSS) coverage with real-time monitoring and recording; and

d) intrusion alarms, motion sensors and secure storage zones.

For prompts to assess the adequacy of mitigation measures to prevent access, see **H.1**.

8.3 Process/engineering mitigation measures

Process mitigation measures (already in place for food safety and quality) can also provide mitigation from intentional acts. Measures include monitoring of equipment performance, process parameters, and verification of hygiene programmes. Examples include:

a) verification of cleaning programmes;

b) environmental pathogen monitoring;

c) in-process chemical tests (e.g. pH, Brix), where unexpected variances in inline chemical test results could indicate changes to set points in automated processes have occurred;

d) temperature monitoring; and

e) camera anomaly detections.

8.4 Technology mitigation measures

Technology mitigation measures protect overall business systems and examples include:

a) secure data management;

b) strict access controls; and

c) verification processes, such as oversight of procurement purchases to flag any unusual purchase quantities or items.

8.5 Product specific mitigation measures

Existing product controls (already in place for food safety and quality) can also provide mitigation from intentional acts. These include inspection and testing of raw materials, in-process products, or finished products to detect any anomalies or contamination. Examples of product controls include:

a) foreign object detection using metal detectors, X-ray systems, or visual inspections;

b) sensory assessments evaluating appearance, odour, taste and texture;

c) microbiological testing for positive release, where batches are held until confirmed safe after pathogen or indicator analysis;

d) mass balance assessments or yield reconciliation to account for all inputs (raw materials, ingredients, additives) against outputs, identifying discrepancies that could indicate unauthorised losses or additions;

e) verification of supplier certificate of analysis (COA's) often combined with independent testing of incoming raw materials; and

f) routine laboratory analysis to detect adulteration such as added water via Brix or specific density checks, unexpected fats and oils (e.g. via fatty acid profiling), or other undeclared substances.

8.6 Tamper detection mitigation measures

Raw material storage containers, distribution vehicles and most packaged foods can be made tamper evident. These measures help ensure that if someone gains unauthorized access and commits a deliberate act, the tampering is likely to be noticed readily, giving time to prevent harm and identify or recall affected products. Examples of mitigation measures include:

a) tamper-evident seals, locks and packaging; and

b) use of detection equipment (e.g. X-ray, metal detectors or other screening techniques designed to identify intentional contaminants).

For prompts to assess the adequacy of mitigation measures for tamper detection, see **H.2**.

8.7 Procedural and behavioural mitigation measures for personnel security

Personnel security measures can be used to mitigate the insider threat to an organization and allow food businesses to evaluate the trustworthiness of supply network partners. Examples of these mitigation measures include:

a) employee vetting, (background checks), induction training, and ongoing refresher food defence awareness training;

b) pre-screening, verifying identification, granting appropriate access and providing supervisions for contractors, visitors and agency or temporary employees;

c) developing protocols for challenging and reporting unknown or suspicious people; and

d) segregation of duties and restricting access to critical areas or process steps.

For prompts to assess the adequacy of mitigation measures for personnel security, see **H.3**.

9 Response to food terrorism incident

9.1 General

While implementing mitigation measures can significantly strengthen food protection, it cannot completely eliminate the risk of a deliberate act occurring. A robust cross functional food protection emergency response and business continuity plans remain essential to effectively manage and recover from any incident that does occur.

9.2 Planning for an emergency response

An effective emergency response plan for a deliberate act should be integrated into the business' overall crisis management protocol. Its key objectives are to:

a) minimize physical and financial harm to consumers, customers, employees and others;

b) collaborate with investigatory and enforcement authorities;

c) maintain or regain public confidence in the organization;

d) reduce financial, reputational and personal impacts from the incident;

e) prevent recurrence;

f) help identify those responsible; and

g) protect long-term consumer trust in food.

These response plans work best when they are developed and tested in advance, before any deliberate act occurs against the organization or its food supply network.

Food businesses should regularly test their crisis and emergency response plans through exercises or simulated scenarios. These drills should simulate possible incidents which require a coordinated, multi-disciplinary response to check preparedness and improve response capabilities (see **I.7**).

9.3 Management of an incident

If intentional adulteration is suspected, the affected products should be immediately quarantined and assessed to determine if the need to withdraw from sale or recall from customers. This requires clear and effective lines of communication to those with responsibility and authority.[2] Follow existing crisis management and emergency response protocols.

If criminal activity is suspected, specialist police or law enforcement agencies should be notified as soon as possible to preserve evidence (see **J.3** for the relevant UK agencies). The site and any potential evidence should be secured, such as photos, samples and CCTV/VSS footage to support the investigation.

Proactive communication with the media can help avoid unnecessary alarm and limit reputational damage during an incident, and social media can be monitored to detect misinformation early. The organization should also have a rapid, coordinated response plan in place with clear responsibilities assigned to counter false information while managing the incident.

9.4 Management of a cyber incident

Engaging a specialist cyber security contractor, prior to an incident can substantially increase the cyber resilience of a business. The cyber specialist can develop a customized incident response plan, conduct regularly cyber preparedness exercises and will already be familiar with the business systems should an incident occur.

Responding quickly and appropriately can greatly reduce the damage caused by a cyber incident and also the time it takes to recover.

The UK's National Cyber Security Centre provides a free Early Warning Service,[3] which helps organizations investigate cyber incidents on their network by notifying them of malicious activity which has been detected in international feeds.

9.5 Maintaining business continuity following a food terrorism incident

Business continuity management principles[4] enhance resilience by enabling rapid response and recovery from a deliberate act, and examples include:

a) transferring production to verified alternate suppliers;

b) activating backup sites or co-packers;

c) utilising electronic backups or independent manual systems;

d) rerouting product via secondary transport or storage providers;

e) a review of the food protection plan to evaluate the need for updates or enhancements; and

f) incorporating lessons learned from the incident to strengthen mitigation strategies, ensuring ongoing improvement and adaptation to emerging risks.

NOTE *Further information on business continuity management is provided in BS 65000.*

[2] Available at https://www.npsa.gov.uk/protected-procurement-business-leaders.
[3] Available at https://www.ncsc.gov.uk/section/active-cyber-defence/early-warning.
[4] Further information is available in BS 65000.

10 Review of food protection measures

10.1 General

Food protection measures should be reviewed when there are changes which could affect the suitability of the existing mitigation measures. This could be done following a suspected or actual incident, or when there has been a breach of site security or cyber/IT/OT. A review could also be prompted when the mitigation measures are found to be ineffective.

10.2 Review of food protection arrangements

The TACCP team should review the food protection arrangements regularly, and in accordance with the organization's other corporate policies and procedures. Regulatory requirements or external standards (e.g. certification schemes) might also require a formal review to be conducted periodically.

Specific prompts that might trigger a review include:

a) new or emerging threat information, including new types of biological, chemical, physical and radiological adulterants;

b) incidents impacting other businesses or similar products;

c) an actual product tampering event or a near miss event;

d) geopolitical changes, wars and conflicts;

e) changes in suppliers or raw materials (ingredients or packaging);

f) changes to bulk raw material receival, storage or other vulnerable process steps;

g) changes to equipment, processes or layout;

h) changes in key personnel or the areas in which they are working;

i) facility expansions, renovations or new access points;

j) repeated deviations from food safety critical limits or monitoring failures;

k) new regulatory or customer requirements relating to food protection;

l) to address deficiencies found through a challenge test of mitigation measures; or

m) following internal verification activities and external audits.

The TACCP team should also be actively involved and consulted during any significant organizational changes to products, processes, equipment or structure. Involving the TACCP team early helps identify and address potential new threats or vulnerabilities as part of the change management process.

10.3 Maintaining confidentiality of food protection arrangements

Due to their commercially sensitive and confidential nature, TACCP reports and all associated review documents should be handled with the highest level of security. Access should be restricted to trusted personnel on a strict "need-to-know" basis only. Disclosure to enforcement or regulatory authorities is permitted when legally required. Unauthorised disclosure could cause serious commercial damage, reputational harm or compromise food protection measures.

A business may publish a generic overview for internal use and/or to present to external auditors, who should respect the sensitive nature of the TACCP process. Such an overview should also avoid detail which could be of value to a threat actor.

10.4 Horizon scanning and new information

The TACCP team should actively monitor reputable and official sources for updates on national threat levels, intelligence reports and any emerging risks that could affect food safety or supply chains.

This includes regularly checking trusted websites such as government agencies, international organizations, trade associations, and other reliable sources of information.

Ongoing horizon scanning can help the TACCP team stay informed about changes to the threat environment, new attack methods, or incidents elsewhere in the industry. This allows timely updates to the TACCP plan, reassessment of risks, and adjustment of mitigation measures to maintain effective food protection.

10.5 Training

Robust, ongoing food defence training should be provided to all personnel within food businesses. Organizations should assess the need for refresher training and deliver it at appropriate intervals to maintain current knowledge. Training builds understanding and skills, enabling a food business to think about "what if'" scenarios so the business can plan and improve its current mitigation measures. This reduces the risk of deliberate acts occurring and builds a stronger food protection culture.

10.6 Food protection culture

A strong food protection culture[5)] helps build robust protective security measures and it reduces risks from insiders within a business as well as from external threats. A strong culture can be created, strengthened and sustained by demonstrating shared values across the organization, which can lead to significant improvements in how employees think about food defence as well as other compliance systems in their daily work.

10.7 Continual improvement

Successful implementation of TACCP requires a proactive and dynamic approach. The threat environment is constantly evolving, with new vulnerabilities emerging and threat actors becoming increasingly sophisticated.

Food businesses, working in collaboration with regulators and supply partners, should continually strengthen their mitigation measures, detection systems and horizon-scanning activities. This ongoing effort is essential to the PDCA cycle, enabling effectively deterrence, detection, and response to emerging threats across the entire food supply network. By applying the threat assessment to differentiate between food terrorism and food authenticity (EMA), the resulting mitigation measures often align with and build upon foundational quality and food safety systems. These elements are closely interconnected within the broader concept of food protection. For information on complementary approaches to food protection, see Annex J.

5) Available at https://www.npsa.gov.uk/security-best-practices/security-culture/security-culture-tool.

Annex A (informative)
Food supply network

A.1 General

The food supply network is global, interconnected and time sensitive. Figure A.1 illustrates an example of a food supply network, highlighting the complexity and interconnectedness of products, inputs, and the various actors involved

A single ingredient can travel through multiple organizations and countries before reaching the consumer, which is why protecting every link in the network is essential to food protection.

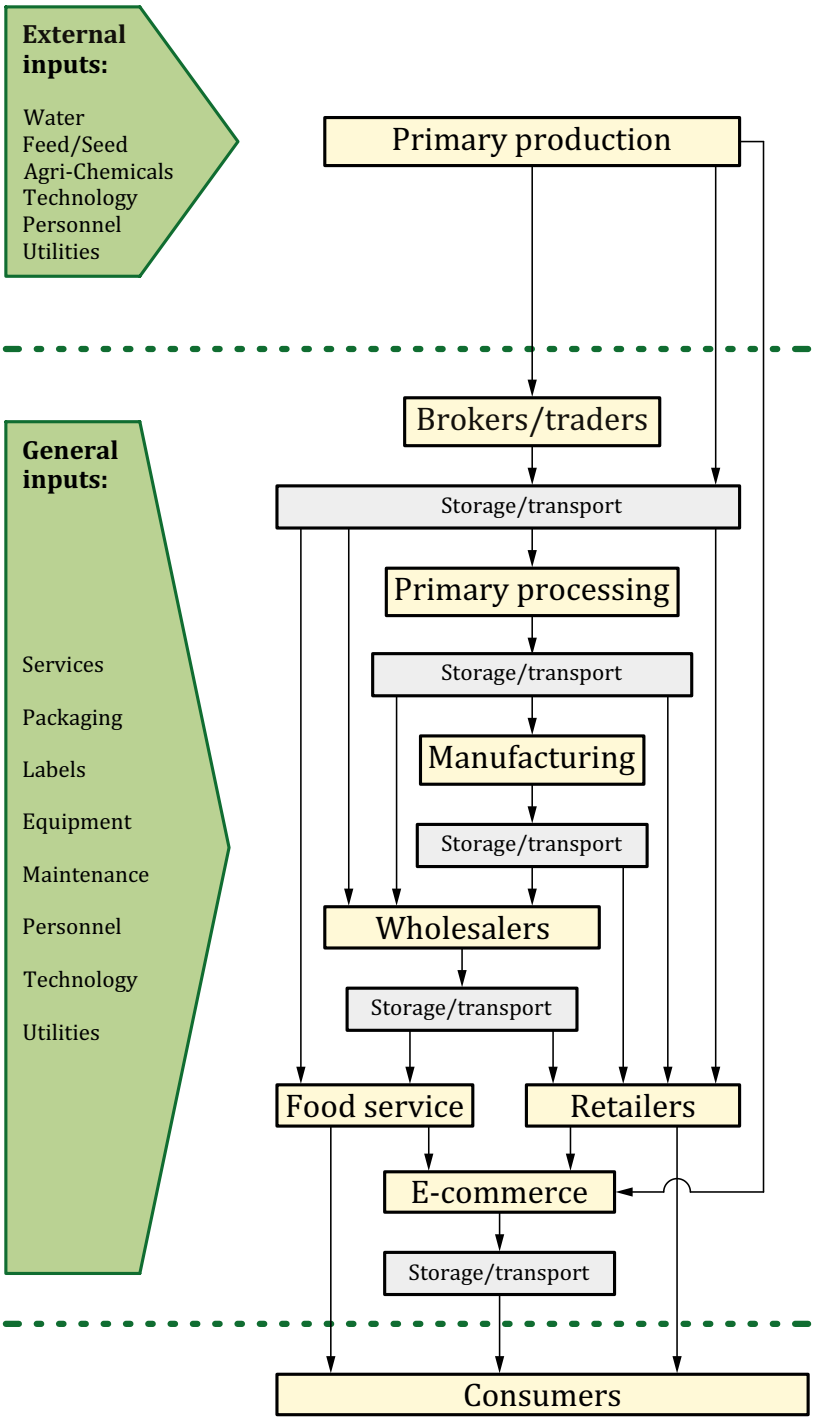
Having a secure food supply network is critical to food protection for the following reasons.

a) There are multiple points of vulnerability for long and complex food supply networks; from primary production (farms), primary processing (abattoirs), ingredient suppliers, manufacturers, logistics (storage, transport and distribution), through to retail and food service. Each step in the supply network can provide potential access points for motivated threat actors who each may target different parts of the network for maximum leverage.

b) Supply networks can have an amplification effect where deliberate contamination early in the network (e.g. in raw materials) on one single ingredient can potentially find its way into multiple different food products.

c) The food network is a critical infrastructure sector. A successful attack and subsequent disruption can simultaneously threaten public health, consumer confidence, brand reputation, national economies and in extreme cases, social stability and the rule of law.

Figure A.1 – Example of food supply network



Annex B (informative)
Examples of cases reported

COMMENTARY ON ANNEX B

This annex provides examples of reported cases involving various types of threats, to illustrate the nature and diversity of threats across different food businesses.

B.1 Intentional adulteration

B.1.1 Malicious contamination

The following are reported examples of malicious contamination.

a) In 2014 an employee at a facility in Japan was arrested for contaminating frozen foods with malathion (an organophosphate insecticide), causing over 2,800 illnesses.[6)]

b) In 2018, an incident in Australia led to extensive public concern and a dramatic drop in retail sales when retail customers found sewing needles inserted into fresh strawberries.[7)]

c) In 2022, an employee in Worcestershire, UK was found to have knowingly and maliciously contaminated hummus and salad dressings destined for a quick service restaurant (QSR) with plastic bags, rubber gloves and metal ring pulls. The contamination and product tampering occurred in the post-production storage area.[8)]

B.1.2 Ideologically motivated threatening acts of malicious contamination

In 2017, anarchist group Green-Black Commando, published online threats to contaminate food products in Greece. They claimed to have injected hydrochloric acid into soft drinks, milk, sausages and sauces from multinational companies. Similar threats also occurred in 2013 and 2016, aimed at forcing product withdrawals and significant revenue losses see *European Union Terrorism Situation and Trend Report 2018* [10].

B.1.3 Extortion

In 2020, a person in the UK was found guilty of extortion and contaminating infant food with metal shards being sold at a large retailer.[9)]

B.1.4 Espionage

In 2022, a person pleaded guilty to participating in a plot to steal a proprietary algorithm from an agribusiness company. The software enabled farmers to increase agricultural productivity.[10)]

6) Available at https://www.bbc.com/news/world-asia-25901568.
7) Available at https://www.foodstandards.gov.au/publications/Strawberry-tampering-incident.
8) Available at https://www.bbc.com/news/uk-england-hereford-worcester-66997510.
9) Available at https://www.bbc.com/news/uk-england-lincolnshire-53849726.
10) Available at https://www.justice.gov/archives/opa/pr/chinese-national-pleads-guilty-economic-espionage-conspiracy.

B.2 Intentional disruption to business through cybercrime

B.2.1 Cyber-enabled industrial espionage or hacking

The following are reported cases of cyber enabled industrial espionage or hacking.

a) In 2023, a disgruntled former employee allegedly used residual remote access via a work app on his personal phone to illegally log into the chemical dosing system at a poultry processing plant. As a technician for the cleaning services provider, the threat actor had prior knowledge of the OT-controlled systems. Over multiple days he manipulated levels of peracetic acid and sodium hydroxide sanitisers, while disabling safety alarms and redirecting notifications to conceal his actions.

b) In 2024 a former employee hacked servers for an amusement park, falsifying allergen information to falsely mark certain items as peanut free, altering prices and redirecting QR codes to a boycott website.[11)]

B.2.2 Cyber enabled fraud

In 2022 food manufacturers and suppliers in the USA were warned about business email compromise (BEC) scams where criminals were impersonating legitimate companies to fraudulently obtain large shipments of food ingredients (whole milk powder and non-fat dry milk) without paying. Four fraudulent entities placed orders worth nearly US$ 600 000 for powdered milk; goods were picked up, but no payment followed. Scammers then spoofed a real food company's email to secure credit and pick up a first shipment worth over US$ 100 000; the supplier halted the second upon non-payment and discovered the fraud after contacting the legitimate company.[12)]

B.2.3 Distributed denial of service, (DDoS)

In 2020, a German online food delivery service reported cybercriminals had conducted a DDoS attack against its website, resulting in orders not being processed. The actors requested payment through cryptocurrency to stop the attack.[13)]

B.2.4 Ransomware attacks

In 2021, the world's largest meat processor paid a £7.8m ransom after a cyber-attack on its system shut down operations, including abattoirs and feedlots in the USA, Australia and Canada. Cattle slaughter was halted at US facilities, causing disruption in a food supply network already strained by Covid 19 impacts.[14)]

B.2.5 Misinformation and disinformation

In 2016, Nigerian customs seized 2.5 t of rice, initially calling it plastic; this was later retracted after tests found high bacteria levels, but no plastic.[15)]

11) Available at https://edition.cnn.com/2024/10/30/business/fired-disney-employee-allegedly-hacked-into-company-system-to-change-allergy-info-on-menus.
12) Available at https://industrialcyber.co/critical-infrastructure/us-agencies-warn-of-hackers-using-bec-tactics-to-steal-large-shipments-of-food-products-ingredients/#:~:text=In%20February%2C%20four%20different%20fraudulent,legitimate%20domain%20names%20were%20used.
13) Available at https://www.bleepingcomputer.com/news/security/food-delivery-service-in-germany-under-ddos-attack/.
14) Available at https://www.bbc.com/news/business-57423008.
15) Available at https://www.bbc.com/news/blogs-trending-40484135.

B.3 Food fraud

B.3.1 Substitution resulting in public health harm

In 2024, six people died from methanol poisoning with another eight hospitalised after consuming alcoholic drinks contaminated with methanol in Laos. The methanol was likely to have been introduced through illicitly produced or deliberately adulterated local spirits. The incident prompted travel warnings from multiple countries (e.g. USA, UK, Australia), and ongoing legal proceedings.[16)]

B.3.2 Substitution for economic gain

In 2017, Italian authorities disrupted an organized crime ring which was exporting fraudulent olive oil to the USA. Similarly, Brazilian officials reported that a very high proportion of olive oils tested did not meet the quality standards required by their labelling.[17)]

B.3.3 EMA with food safety consequences

The following are reported examples of adulteration.

a) In 2024, Delhi police in India seized 15 t of fraudulent spices from two factories, arresting three individuals involved in the production and supply of adulterated spices.[18)]

b) In 2016, the Kenyan Dairy Board claimed that milk vendors were putting lives at risk by adding preservatives (hydrogen peroxide) in an attempt to extend the shelf life of milk.[19)]

c) In 2008 in China, melamine was used as a nitrogen source to fraudulently increase the protein content of milk, resulting in more than 50 000 infants hospitalized and six deaths after having consumed contaminated infant formula.[20)]

B.3.4 Counterfeiting

The following are reported examples of counterfeiting.

a) In 2021, Operation OPSON IX [26] reported the seizure of 1 613 t of illicit alcohol, much of it violating intellectual property rights, with a total value around US$ 20 317 547.

b) In 2018 an investigation uncovered a fraud in Italy involving the reuse of authentic empty wine bottles and wooden box packaging. Empty bottles were collected from restaurants, refilled with cheap wines bought online or from discount stores, and sealed with corks and counterfeit capsules. Packaging films and fake guarantee seals concealed the tampering. Counterfeiters contacted buyers via a major e-commerce platform, offering prices below market rates. The wines were sold as genuine in Italy and abroad, creating a completely uncontrolled market with no traceability [11].

16) Available at https://theconversation.com/six-people-have-died-in-laos-from-drinking-tainted-alcohol-what-you-need-to-know-about-methanol-244437.
17) Available at https://www.oliveoiltimes.com/business/italy-arrests-33-accused-olive-oil-fraud/55364.
18) Available at https://economictimes.indiatimes.com/industry/cons-products/food/delhi-spice-scam-15-tonnes-of-adulterated-masalas-seized-3-arrested/articleshow/109870561.cms?from=mdr.
19) Available at https://nation.africa/kenya/counties/nakuru/Agency-arrests-Nakuru-traders-selling--poisoned--milk/1183314-3148894-j28vi3/index.html.
20) Available at https://www.who.int/emergencies/disease-outbreak-news/item/2008_09_29a-en.

Annex C (informative)
Techniques used to exploit cyber vulnerability

C.1 Distributed Denial of Service (DDoS)

A business can be impacted by a Distributed Denial of Service, (DDoS), which occurs when multiple sources overload a website or network to degrade its performance or render it inaccessible. This can cause disruption and financial loss, especially for businesses reliant on online platforms. The growing presence of the Internet of Things (IoT) increases vulnerability, as every-day connected devices might be compromised and exploited by threat actors.

C.2 Ransomware attacks

Ransomware attacks use malicious software that prevents an individual or organization from accessing their computer systems or data, leaving the target "locked out" and unable to continue operating. Generally, the threat actor will then request a "ransom" payment in cryptocurrency before the system or data is restored. These types of attack have become a favoured technique of organized criminals who operate globally and are often based in countries where governments tolerate their existence on the proviso that they themselves are not targeted [12].

C.3 Misinformation and disinformation

The rise in misinformation and disinformation which has coincided with the growth of social media, has the potential to undermine public confidence in the authenticity, safety and reliability of food. The rise in food-related fake news, misleading information and the rapid rate at which it can spread online, can significantly influence consumer perceptions and behaviour [13].

C.4 Cyber-enabled fraud

While identity theft is typically associated with individuals, organizations can be subject to corporate identity theft (or impersonation). In these schemes, attackers can steal a business' identity to commit procurement fraud where they fraudulently order goods in the company's name, divert them to the attacker's location, and leave the supplier unpaid, resulting in the legitimate business facing liability, disputes, and potential litigation.

C.5 Systems susceptible to cyberattack

Systems that are susceptible to a cyberattack include:

a) information technology systems for email, enterprise resource planning (ERP), e-commerce and cloud platforms;

b) operational systems for supervisory control and data acquisition (SCADA), programmable logic controllers (PLCs) sensors and cold chain temperature monitors;

c) IoT devices including cameras and barcode scanners; and

d) security systems such as access control systems, networked CCTV/VSS, intrusion alarms or other electronic monitoring technologies.

C.6 AI enabled systems

With the rapid advancement and uptake of artificial intelligence (AI) technology throughout society, AI enabled systems might increasingly be utilised within the food industry. As this technology shift continues to evolve and spread, new vulnerabilities and threats might also emerge. These in turn might require increased vigilance and the implementation of appropriate mitigation measures.

Annex D (informative)
Assessing the threat environment

The first step in mitigating risk is assessing the threat environment to the organization, its operation, sensitive products, or a combination of these. Reviewing the responses to these questions can give an understanding of the factors that can contribute to the risk of a potential threat.

The TACCP team could ask the following questions in Table D.1 to Table D.3 to identify potential threats.

NOTE *This is not an exhaustive list of questions that might be asked to assess a threat.*

Table D.1 – Assessing the threat environment for an organization

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Are we operating under foreign ownership by nations involved in international conflict or controversy?				
2	Do we have a reputation for connections to customers or suppliers in geopolitically unstable regions?				
3	Is our product or its brand well known and/or highly recognizable?				
4	Are any of our products or brands considered controversial by certain groups?				
5	Do we have a high-profile or celebrity senior executive or owner?				
6	Do we, or our customers, supply high-profile individuals, organizations or events?				
7	Does social media activity indicate our organization being a potential target?				

Table D.2 – Assessing the threat likelihood for an operation

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Are our premises located in a politically, environmentally or socially sensitive area?				
2	Do our premises share access or critical services with controversial neighbouring entities?				
3	Are utility services supplying our premises easily accessible to unauthorized people?				
4	Are engineering workshops, maintenance areas, tools storage areas and similar locations kept secure (e.g. locked when not in use, and with restricted to authorized personnel only)?				
5	Is there restricted or adequately controlled access to hazardous items that could be misused to contaminate, tamper with, or disrupt the production process (e.g. chemicals, lubricants, cleaning agents, tools, spare parts, waste or other hazardous materials)?				
6	Do we have robust screening procedures for new recruits, including agency and casual employees?				
7	Do any employees show signs of dissatisfaction or have any reason to feel disgruntled?				
8	Have key roles been occupied by the same employee for many years with little supervision?				

Table D.2 – Assessing the threat likelihood for an operation *(continued)*

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
9	Do we have effective, confidential reporting and handling procedures for concerns about disgruntled employees or insider threats?				
10	Are our internal verification and audit arrangements truly independent (e.g. internal auditors should have no operational responsibility for the area, process or site being audited)?				
11	Are our SCADA and other control systems, used for real-time monitoring and management of manufacturing, infrastructure, or facility-based process shared with organizations that could be targeted?				

Table D.3 – Assessing threats for a product

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Is the product or its brand well known and/or highly recognizable?				
2	Is the product considered economically high value?				
3	Is this product known to be a regular target of food fraud?				
4	Has there been recent significant cost increases affecting this product?				
5	Is this product used as an ingredient in a wide range of popular foods?				
6	Does this product contain high risk ingredients (e.g. potentially hazardous foods that support the growth of pathogens)?				
7	Does the product contain ingredients or other material sourced from other countries?				
8	Does the product hold specific religious, cultural, ethical or moral significance for certain consumer groups?				

Annex E (informative)
Identifying vulnerabilities

E.1 Identifying vulnerabilities

The next step in mitigating risk is identifying vulnerabilities that could enable a threat to succeed. Reviewing the responses to the questions in Tables E.1 to Table E.5 can help the TACCP team identify vulnerabilities that might allow a threat to be carried out.

NOTE *This is not exhaustive of all questions that might be asked to assess a vulnerability.*

Table E.1 – Malicious contamination vulnerabilities

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Could a contaminant be brought into our facility?				
2	Could a contaminant be added at any point to the water source used in our facility?				
3	Is the integrity of ingredient packaging suitable to reduce the likelihood of malicious contamination (e.g. do storage containers and transportation units have tamper-evident seals)?				
4	Does the production process involve liquid receiving, storage, handling and loading steps where large volumes make contaminants hard to detect and liquid transfer enables rapid distribution?[A)]				

Table E.1 – Malicious contamination vulnerabilities *(continued)*

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
5	Are there open and exposed production steps, such as mixing and blending, that allow insider access, where contaminants could be added and then blended into the product and be difficult to detect?[A)]				
6	Is there secondary ingredient preparation involving small volumes but with potentially high potency (e.g. allergens or toxins)?[A)]				
7	Are there fast moving, unattended, high-volume production lines that are difficult to monitor continuously?[A)]				
8	Would routine quality or food safety monitoring detect a contamination or adulteration in the product?				
9	Are personnel security procedures in place and enforced?				
10	Is employee boredom, low morale, discipline, turn-over or recruitment a problem?				
11	Do any employees hold a grudge against the organization?				
12	When employees are under investigation for misconduct, are they temporarily suspended or removed from roles involving direct handling, oversight or access to food production areas?				

Table E.1 – Malicious contamination vulnerabilities *(continued)*

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
13	Is there opportunity for access to our facility by sympathizers of single-issue groups?				
14	Have business competitors been accused of espionage or sabotage?				

[A)] FDA Mitigation Strategies Guide: Available at https://www.fda.gov/media/105742/download.

Table E.2 – Cyber vulnerabilities

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Have our senior leaders implemented a cyber strategy that clearly defines accountability and responsibility for cybersecurity?				
2	Does our organization have an effective approach to managing cyber risks?				
3	Does our OT follow secure design principles?				
4	Are our employees likely to recognize and report suspicious electronic communications (e.g. emails, SMS)?				
5	Are our employees trained on common cyberattack techniques (e.g. phishing, ransomware) and equipped to recognize them and respond appropriately?				

Table E.2 – Cyber vulnerabilities *(continued)*

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
6	Are our employees sufficiently trained in data handling/security (e.g. not leaving laptops unlocked)?				
7	Is all data appropriately protected in transit, at rest, and at end of life, commensurate with the assessed risks?				
8	Are our operators promptly and securely notified of changes to production or operational configurations (e.g. product formulations)?				
9	Are passwords or other authentication methods used?				
10	Do our procedures for employee onboarding, internal transfers or termination, address all device and access privileges and accounts security?				
11	Are our local Wi-Fi connections encrypted and inaccessible to external users?				
12	Are our internet-enabled processes secure (e.g. can process parameters be changed without proper authorization, or can cloud-based records be accessed or corrupted)?				
13	Are our backup data and storage processes effective in protecting business-critical information?				

Table E.2 – Cyber vulnerabilities *(continued)*

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
14	Is all externally sourced data (from email, internet or removable media) examined for malware before being imported?				
15	Does remote access to our company systems require multi-factor authentication and is the extent of access limited?				
16	Are our critical computerized systems tested regularly and are routine offline backups conducted?				
17	Are business continuity and disaster recovery plans for IT and production systems in place, routinely tested and deemed effective?				
18	Are the identities of suppliers and customers verified before conducting online transactions?				
19	Is our business currently operating at a pinch point (e.g. under abnormal stress on processes, systems or employees) which could increase vulnerability or a cyber-attack?				

Table E.3 – Food fraud vulnerabilities

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Do we have sufficient documented or verifiable trust in our suppliers, and also their suppliers (e.g. through verification activities and audits, or indicators such as food safety incidents, recalls and regulatory non-compliances)?				
2	Do our suppliers think that we monitor their operation and routinely test their products?				
3	Which of our suppliers are not routinely audited?				
4	Are materials supplied through remote, obscure, or indirect channels such as brokers or intermediaries?				
5	Do our key suppliers implement robust personnel security practices?				
6	Are our employees and those of our suppliers, encouraged to report concerns (e.g. confidential reporting or whistleblowing)?				
7	Are certificates of certification or accreditation and certificates of analysis issued by independent parties?				
8	Are product samples retained, especially for items with a short shelf life?				

Table E.3 – Food fraud vulnerabilities *(continued)*

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
9	Have there been significant increases in material costs?				
10	Has pressure on suppliers' trading margins increased?				
11	Have there been unexpected increases or decreases in demand?				
12	Are low-cost substitute materials available?				
13	Are major raw materials becoming difficult to source and are alternatives plentiful (e.g. due to repeated crop failures or overproduction)?				
14	How do our suppliers dispose of excessive waste materials?				
15	Are our packaging suppliers handling waste or out of specification branded packaging appropriately?				

Table E.4 – Supply network vulnerabilities

#	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Is our current supply network structure complex?				
2	Do we have short supply networks with few participants, intermediaries and touchpoints, or are they long, more fragmented and involving multiple layers?				
3	To what extent does the length and complexity of our supply networks create additional opportunities for intentional interference or malicious acts?				
4	What is our current level of visibility and transparency across our entire supply network?				
5	How effective are our oversight mechanisms, including traceability systems, supplier auditing, verification processes and on-going monitoring?				

Table E.5 – Other vulnerabilities

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Does our business have any critical pinch points, single points of failure or bottlenecks in its supply chain or production processes (e.g. sole supplier, centralized distribution, etc.)?				

Annex F (informative)
Example of risk assessment methodology

F.1 Introduction

The TACCP team may elect to use a structured, risk-based approach to identify, evaluate and prioritize deliberate threats against food products, processes or supply networks.

This example (see Table F.1) uses a 5x5 matrix to score two key dimensions for the following.

a) Likelihood or the probability of the threat occurring and succeeding is evaluated on a scale of 1 to 5. With 1 being rated as unlikely to happen, through to a 5 which is rated as having a very high chance of happening).

b) Impact or the severity of consequences if the threat succeeds, is also scored from 1 (minor) through to 5 (catastrophic).

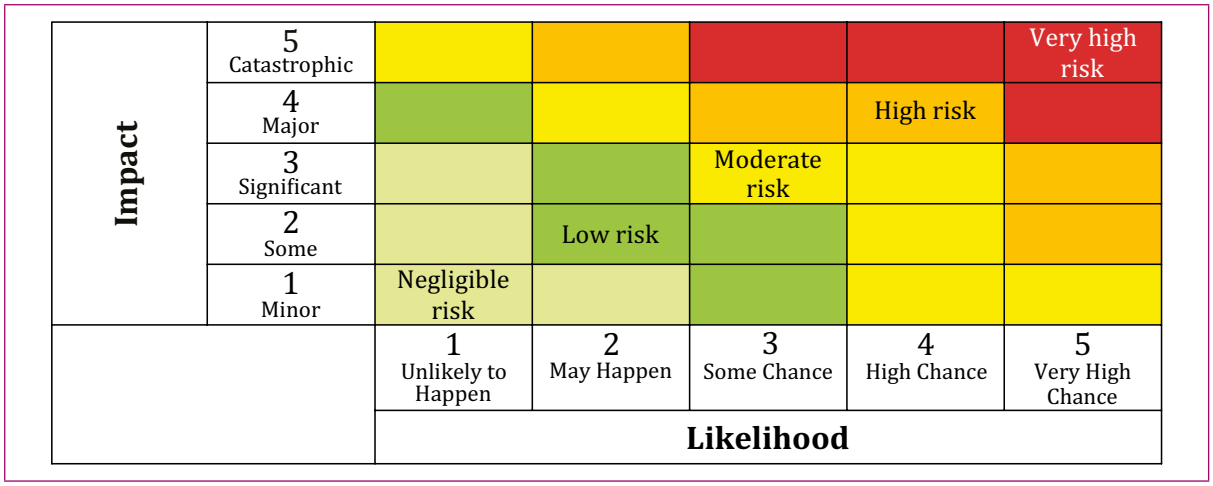
Table F.1 – Example risk assessment scoring

Likelihood of threat happening	Score	Impact		
		Descriptor	Human health/ public safety	Business/financial/ reputational
Very high chance	5	Catastrophic	Death	Business / site closure
High chance	4	Major	Illness or injury requiring medical treatment	Brand damage
Some chance	3	Significant	Generally mild symptoms, might require medical treatment	Regulatory non-compliance or recall/withdrawal
Might happen	2	Some	Mild symptoms lasting a few days	Negative media reports
Unlikely to happen	1	Minor	Mild symptoms prompt recovery	No perceived impact
***NOTE** Impacts could be assessed in human and financial terms.*				

Once the scores for likelihood and impact have been determined for each threat, these are plotted on the risk assessment matrix to provide a risk prioritization where: Risk = Likelihood × Impact, (see Figure F.1).

A higher score indicates a higher-priority threat (e.g. "very high risk" in the top-right corner of the matrix). Mitigation measures are proportionate to the priority score: the higher the score, the more comprehensive the mitigation measure.

Figure F.1 – Example of risk assessment matrix



Annex G (informative)
TACCP case studies

G.1 Introduction

The case studies in this annex are entirely fictitious and any resemblance to real organizations is purely coincidental. They show varied applications of the TACCP process, using different formats from that described in Clause **6**, to encourage users of this PAS to adopt a flexible approach.

Two examples are provided to demonstrate how different food businesses can adapt and present their TACCP threat assessments.

a) Case study 1, Burgers4Me is a national Quick Service Restaurant (QSR) fast-food chain.

b) Case study 2, Bridgeshire Cheese Company is a small family enterprise that manufactures a range of organic cheeses.

G.2 Case Study 1 – Burgers4Me

G.1.1 Overview

This case study presents an example TACCP report from the TACCP team at Burgers4Me, a national QSR chain. The company's burger range includes standard, jumbo, veggie, cheese and chilli options.

The TACCP team have identified the following:

a) threats to the company and information systems (see Table G.1); and

b) threats to the product process (see Figure G.1).

The TACCP team include the:

1) Operations Director (Team Leader) who also leads the company's Emergency Planning and Business Continuity Committee;

2) Human Resources Manager;

3) Procurement Manager;

4) Technical Manager; and

5) Regulatory Compliance Officer, who holds dedicated responsibility for security and fraud prevention.

The team also receives contributions from other managers as required for specialist topics or areas of expertise.

Table G.1 – Burgers4Me threat information

No.	Source of threat to company and information systems	Possible method of operation	Comments
A	Animal rights activists	Vandalism or sabotage	Little evidence of current activity
B	Hacktivists 1	Distributed denial of service (DDoS) attack on website	Developing company profile might provoke attack
C	Hacktivists 2	Ransomware attack	Experienced in 2020; online orders increasing
D	Company buyers	Fraud; collusion with suppliers	Established team working autonomously
E	Criminals	Counterfeiting; misappropriation of packaging	Increasing risk as brand strengthens
	Source of threats to locations	**Possible method of operation**	**Comments**
F	Supporters of local businesses	Adverse publicity; "guilty by association" with fast food	Some locations report high levels of media interest
G	Overworked company employees, disenchantment; alliance with extremists (e.g. activists or terrorists)	Petty contamination; possible serious malicious contamination	Some employee shortages requiring regular overtime
H	Single issue groups	Deliberate infiltration of premises	Some recent precedent
I	Front line employees	Theft; collusion with customers	Rigorous audit in place; outlet managers trustworthy (personnel security checks)

Table G.1 – Burgers4Me threat information *(continued)*

	Source of threats to product from:	Possible method of operation	Comments
J	Suppliers of meat	EMA – non-animal protein, or non-beef meats, replacing substandard meat or meat not intended for human consumption	Beef is specified and expected, even though not claimed in publicity
K	Front line employees	Deliberate undercooking of patty to cause harm through unsafe food	Variable rosters minimize that chance of collusion
L	Front line employees	Selling burger too long after wrapping in an attempt to cause harm through unsafe food	
M	Ideologically motivated group	Malicious contamination of food and drinks sold by the business	Official threat level unchanged
NOTE *Press reports of concerns about food authenticity are pertinent.*			

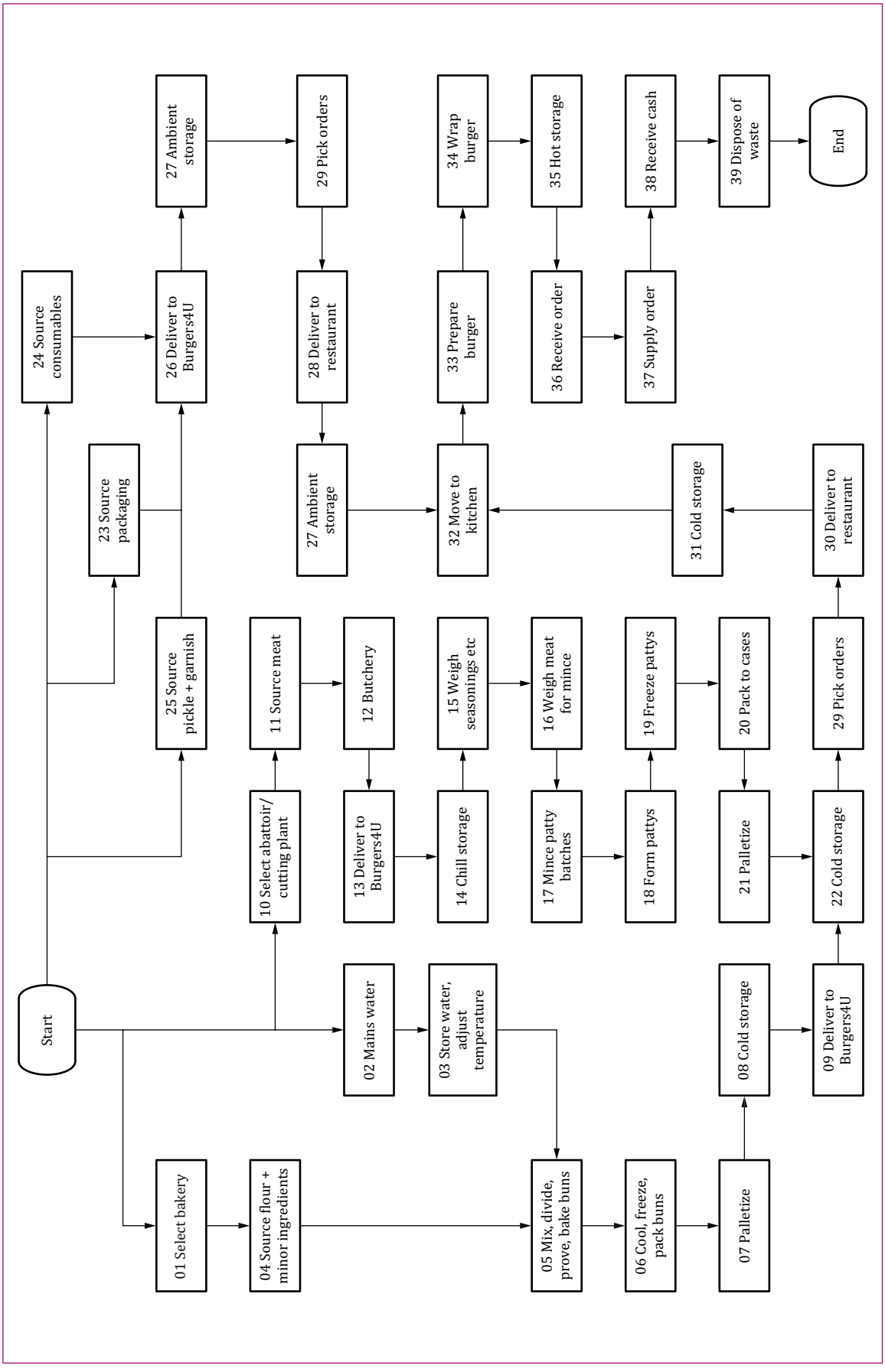


Figure G.1 – Burger4Me product process threat identification

Table G.2 – Burgers4Me threat assessment

Step	Process step	Threat	Vulnerability	Access	Mitigation	Adulterant contamination	Impact of process	Quality assurance/ Quality control (QA/ QC)	Likelihood	Impact
01A	Select bakery	Malicious contamination	Casual employees	Production employees	Contracts require personnel security protocols	—	—	—	—	—
01B	—	EMA	Collusion	Buyers	Little	—	—	—	2	3
02	Mains water	Malicious contamination	Bulk storage reservoirs	Services engineers	Effective control of access	Soluble toxins	Can inhibit yeast; and affect dough handling	Can fail sensory tests	1	1
03	Store water; adjust temperature	Malicious contamination	Batch storage reservoirs	Services engineers	Effective control of access	-—	Water might not reach required temperature to effectively clean equipment and utensils	Can contribute to poor sanitation	1	1
04	Source flour and minor ingredients	EMA	Little cost advantage to fraudster	—	—	—	—	—	—	—

Table G.2 – Burgers4Me threat assessment *(continued)*

Step	Process step	Threat	Vulnerability	Access	Mitigation	Adulterant contamination	Impact of process	Quality assurance/ Quality control (QA/ QC)	Likelihood	Impact
05	Mix, divide, prove, bake buns	Malicious contamination	Batch mixing operation	Skilled mixer operative	Trained experienced employees	Powdered toxin	Can inhibit yeast and affect dough handling	Can fail sensory tests	1	1
06	Cool, freeze, pack buns	—	—	—	—	—	—	—	—	—
07	Palletize	—	—	—	—	—	—	—	—	—
08	Cold storage	—	—	—	—	—	—	—	—	—
09	Refrigerated delivery	—	—	—	—	—	—	—	—	—
10A	Select abattoir/ boning plant									
10B		Fraudulent substitution	Poor segregation of species	Delivery drivers and process employees	Unique animal identification recorded	Meat from cheaper sources	Negligible	Random tests can detect unless collusion	2	3
11	Source meat	Fraudulent substitution	Poor segregation of species	Process managers and employees	Inspect meat on receival and confirm from approved suppliers	Meat from cheaper sources	Negligible	Random tests can detect unless collusion	4	3

Table G.2 – Burgers4Me threat assessment *(continued)*

Step	Process step	Threat	Vulnerability	Access	Mitigation	Adulterant contamination	Impact of process	Quality assurance/ Quality control (QA/ QC)	Likelihood	Impact
12	Butchery	Fraudulent substitution	Poor segregation of species	Process managers and employees	Check it meets specification for species (e.g. beef)	Meat from cheaper sources	Negligible	Random tests can detect unless collusion	2	
13	Delivery to site	Diversion of consignment	Supplier responsibility	—	—	—	—	—	—	—
14	Chilled storage	—	—	—	—	—	—	—	—	—
15	Weigh seasonings	Malicious contamination	Manual operation	Process managers and employees	Rigorous hygiene standards	Powdered toxins	Negligible	May Might fail sensory tests	1	3
16	Weigh meat for mince	Malicious contamination	Manual operation	Process managers and employees	Rigorous hygiene standards	Powdered toxins	Negligible	May Might fail sensory tests	1	3
17	Mince patty batches	Malicious contamination	Manual operation	Process managers and employees	Rigorous hygiene standards	Powdered toxins	Negligible	May Might fail sensory tests	1	3
18	Form patties	Malicious contamination	Manual operation	Process managers and employees	Rigorous hygiene standards	Powdered toxins	Negligible	May fail sensory tests	1	3

Table G.2 – Burgers4Me threat assessment *(continued)*

Step	Process step	Threat	Vulnerability	Access	Mitigation	Adulterant contamination	Impact of process	Quality assurance/ Quality control (QA/ QC)	Likelihood	Impact
19	Freeze patties	—	—	—	—	—	—	—	—	—
20	Pack to cases	—	—	—	—	—	—	—	—	—
21	Palletize	—	—	—	—	—	—	—	—	—
22	Cold storage	—	—	—	—	—	—	—	—	—
23	Source packaging	Misappropriation and counterfeiting								
24	Source consumables	—	—	—	—	—	—	—	—	—
25	Source pickle and garnish	Unauthorized ingredient substitution	—	—	Established brands, reliable contracts	—				
	—	—	—	—						
26	Ambient delivery to site	—	—	—	—	—	—	—	—	—
27	Ambient storage	—	—	—	—	—	—	—	—	—
28	Deliver to restaurant	—	—	—	—	—	—	—	—	—
29	Pick orders	—	—	—	—	—	—	—	—	—
30	Deliver to restaurant	—	—	—	—	—	—	—	—	—
31	Cold storage	—	—	—	—	—	—	—	—	—

Table G.2 – Burgers4Me threat assessment *(continued)*

Step	Process step	Threat	Vulnerability	Access	Mitigation	Adulterant contamination	Impact of process	Quality assurance/ Quality control (QA/ QC)	Likelihood	Impact
32	Move to kitchen	Malicious contamination	Out of hours; unsupervised	Night store-employees	Tamper evident cases	'Spiked' patties	Little	None	1	3
33	Prepare burger	Deliberate undercooking/ and malicious contamination	Lone worker	Restaurant employees	Rigorous food safety protocols	—	—	None	1	2
34	Wrap burger	—	—	—	—	—	—	—	—	—
35	Hot hold	—	—	—	—	—	—	—	—	—
36	Receive order	Ransomware	Online ordering	Hacktivists	NCSC cybersecurity protocols	—	—	—	2	3
37	Supply order	Deliberate breach of food safety and sale of burgers past holding period	Restaurant manager under wastage pressure	—	Personnel security procedures					
38	Receive cash	Theft	Restaurant employees	Counter employees	Automated cash tills; and rigorous audit	—	—	—	4	1
39	Dispose of waste	Misappropriation							39	Dispose of waste

NOTE *The symbol "'—" indicates "not applicable" or "not significant".*

G.1.2 Burgers4Me TACCP assessment outcomes

The TACCP review identified 20 threats. Of these, 13 already have effective mitigation measures in place, and none require urgent action. The TACCP review also identified the following:

a) Growth in online orders through third-party agents has made ransomware the main cybersecurity threat to Burgers4Me. Tenders have been invited from cybersecurity consultants to review current protections and improve incident response and recovery.

b) Fraud when selected abattoirs or boning plants remains a key ongoing risk for species substitution and the use of non-meat proteins. The Technical Manager oversees mitigation measures, including a combination of remote and on-site supplier audits.

c) As Burgers4Me is known for quality and trust, the risk of counterfeit packaging has increased. A new packaging supplier has been approved with adequate safeguards, but regular monitoring will continue.

d) While the Burgers4Me website is mainly for marketing, (not primary sales), IT and internal audit resources are sufficient to manage cybersecurity risks, especially DDoS attacks.

e) The Technical Manager monitors official and industry sources for new risks, and in consultation with the TACCP Team Leader, they decide if the team needs to meet ahead of its regular six-monthly review.

G.3 Case study 2: Bridgeshire Cheese

G.3.1 Overview

The case study presents an example threat assessment report for the Bridgeshire Cheese Company (BCC), a family farm owned and operated organic cheese producer. BCC sells its products to speciality retailers and food service businesses. The cheese is made primarily from milk produced on their own farm, with additional milk sourced externally when needed.

The TACCP assessment was conducted by the business owners. They used external resources to help identify threats and to recommend mitigation measures that either reduce the likelihood of a threat occurring or improve the ability to detect if it does occur. Figure G.2 shows the vulnerability assessment flowchart used in the process, and Table G.3 provides details of the threat assessment.

Figure G.2 – Bridgeshire Cheese vulnerability assessment

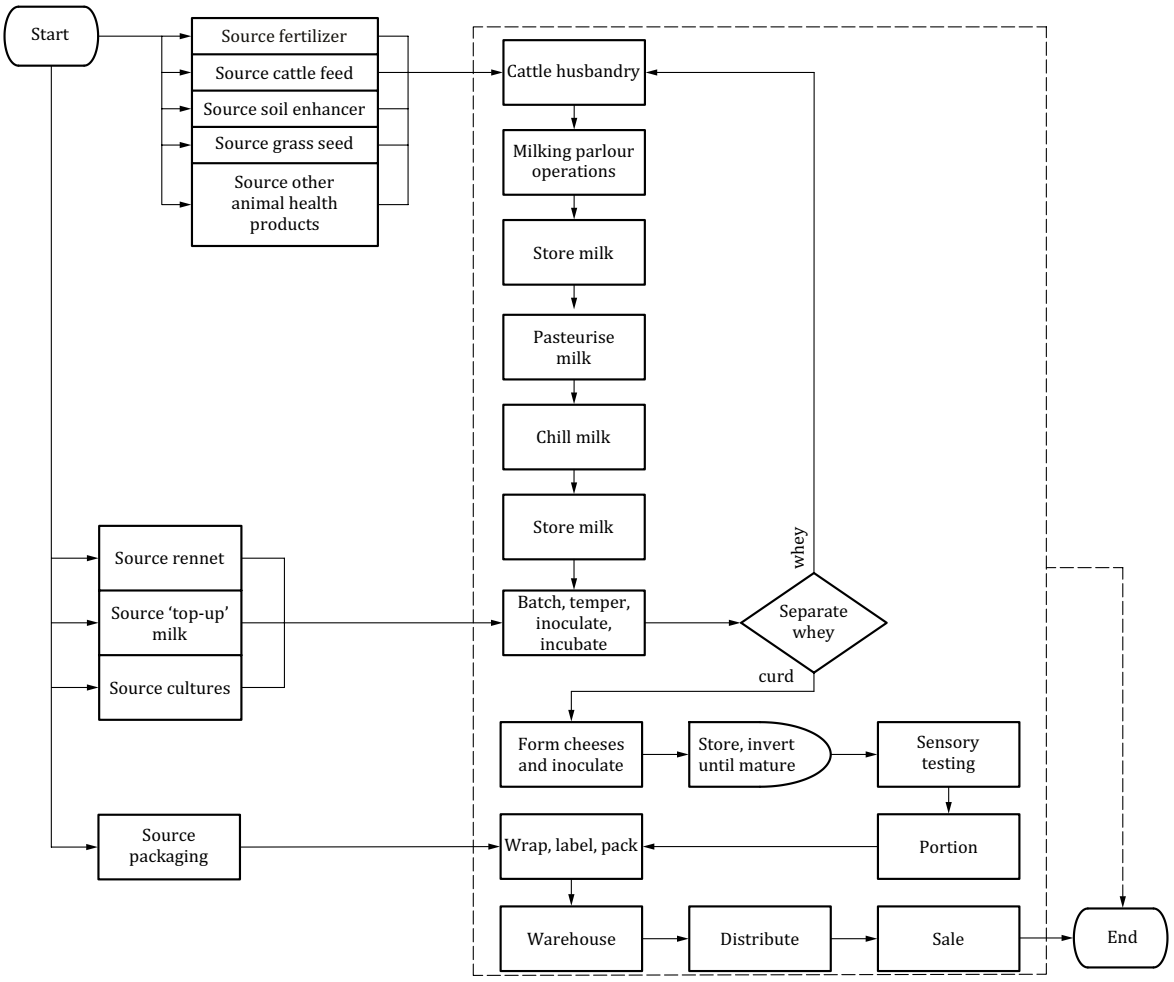


Table G.3 – Bridgeshire Cheese threat assessment

Threat No.	Threat/vulnerability	Consequence	From/threat actor	Impact	Likelihood	Score	Protective measures
1	EMA – Non-organic supply from "top-up" milk	Loss of organic status for product	Suppliers	5	2	10	All raw materials sourced from certified suppliers. Require certificate of conformance for all ad hoc milk purchases.
2	Widespread livestock disease due to right of way through farm used to move known sick or infected livestock in breach of biosecurity controls	Loss of herd, loss of insurance cover	Farmers from neighbouring properties	3	2	6	Biosecurity aligned with best practice.
3	Malicious contamination	Unsafe product	Operators	5	1	5	All products metal detected prior to release. Production area monitored by CCTV daily. Personal hygiene protocols prevent unauthorized items in production areas. Internal audits assess compliance to personal hygiene protocols twice per year. All employees are family members or long-term trusted partners. Sensory assessment of all batches completed prior to release.

Table G.3 – Bridgeshire Cheese threat assessment *(continued)*

Threat No.	Threat/vulnerability	Consequence	From/threat actor	Impact	Likelihood	Score	Protective measures
4	Trials of unauthorized GM crops on perimeter land	Loss of organic status	Farmer from neighbouring properties	5	2	10	1. Regular communication with adjacent farmers regarding activities that might compromise organic status.
5	Diversion of product during transport to grey markets	Value of goods, loss of reputation for reliability	Opportunist criminals	2	3	6	Use of approved contracted transport providers. GPS tracking of vehicles. Security seal applied to trailer at dispatch. Records of traceability maintained.
6	Remote cyberattack on Cloud controlled production processes	Tampering with food safety controls in "Off the peg'" SCADA system to reduce pasteurization time/ temperature	Cyber criminals	5	1	5	1. Maintain separate QC analysis of product. 2. Follow NCSC cyber security advice. 3. Software supplier has proven fire-walls and malware protection.
7	EMA – dilution of milk	Product dilution	Farmer	3	1	3	Use of approved supplementary milk suppliers. Routine testing to detect added water. Product traceability maintained.

Table G.3 – Bridgeshire Cheese threat assessment *(continued)*

Threat No.	Threat/vulnerability	Consequence	From/threat actor	Impact	Likelihood	Score	Protective measures
8	Deliberate mislabelling	Unauthorized extended shelf life, loss of traceability	Operators	3	1	3	1. Automated coding and labelling systems. 2. "Buddy system" for packing and labelling activities. 3. ndependent verification checks completed for each production run.
9	Deliberate use of unsafe or expired product	Consumer harm	Sales and engineering	3	1	3	1. Traceability maintained. 2. Regular stock checks. 3. Waste management protocols.
10	Deliberate by-passing of food safety parameters for pasteurization of raw milk	Under asteurized product	Operators	5	1	5	1. Routine product testing for pasteurization of each batch.

G.3.2

The TACCP assessment identified threats to the BCC operations, it found:

a) all 10 threats were assessed to be under proportionate and effective control;

b) a cyberattack on the SCADA monitoring and control system could cause serious disruption, however BCC is considered an unlikely target and current protective measures are up to date; and

c) a loss of organic certification would seriously harm the business, but reasonable precautions are already in place.

Annex H (informative) Mitigation measures

H.1 Mitigation measures to control access to an operation

Food protection requires mitigation measures to be implemented to reduce the risk of a malicious act. The TACCP team is encouraged to consider the adequacy of their current mitigation measures, using Table H.1 to Table H.5 to determine if they need to be strengthened, or to identify when new mitigation measures are needed.

NOTE *These prompts are not intended to be exhaustive of all mitigation measures which might be relevant or proportionate to reduce a risk.*

Table H.1 – Restricting access to premises

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Are our premises zoned to restrict access to authorized personnel only?				
2	Is access restricted to individuals with a legitimate business need to be in that particular area?				
3	Is visitor access by appointment only?				
4	Are the designated car parking areas positioned in such a way as to restrict or prevent unauthorized access to sensitive zones of the facility (e.g. loading docks and production areas)?				
5	Is the perimeter fencing at our site in a suitable condition and an effective deterrent?				
6	Is there a perimeter alarm system in place?				

Table H.1 – Restricting access to premises *(continued)*

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
7	Is there VSS monitoring and recording of perimeter vulnerabilities?				
8	Do our changing facilities effectively allow personal clothing and belongings to be kept separate from work wear?				
9	Are all external doors at our facility secured and access controlled?				
10	Are doors such as fire doors alarmed or security sealed and regularly checked to detect tampering or misuse?				
11	Is there restricted or controlled access to utility services?				
12	Does the organization undertake regular physical penetration tests to evaluate site security?				

Table H.2 – Restricting access to products in production or process equipment

#	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Is there ease of access to open or exposed ingredients, work in process (WIP) or finished products?				
2	Is there ease of access to process equipment, ingredient addition points or food safety devices?				

Table H.3 – Restricting access to products in transit

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Are access points to food transport vehicles monitored?				
2	Are approach roads equipped with traffic-calming devices to slow transit of vehicles?				
3	Are all deliveries scheduled?				
4	Are vehicular documentation and authorization checked before admittance on site?				
5	Are missed deliverables investigated?				

Table H.4 – Restricting access to electronic systems

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Are there electronic chip & PIN access controls?[A)]				
2	Is critical computer hardware, IT and OT infrastructure including servers, networked devices and process control equipment, located in a physically secure or restricted area with restricted access?				
3	Are automatic session timeouts (idle logout) configured on computers and networked systems, requiring users to re-enter credentials after a period of inactivity?				

Table H.4 – Restricting access to electronic systems *(continued)*

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
4	Is there CCTV/VSS monitoring and recording of all sensitive areas, processing and storage areas?				
5	Are there routine monitoring and implementation of best practice cybersecurity measures?				
6	Is there routine cyber awareness training for employees?				
7	Is there routine challenge testing by external personnel to determine ease of access to premises, products and process equipment?				
[A)] Further information is available from https://www.ncsc.gov.uk/information/top-tips-for-staff.					

Table H.5 – Other considerations

#	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Is there secure handling of mail and posted items including product samples, ingredients or customer returns?				
2	Are there restrictions on portable electronic devices in sensitive areas?				

H.2 Tamper detection mitigation measures

Tamper detection is an important and cost-effective food protection measure for the TACCP team to take into account because it can deter many would-be threat actors. Even if prevention fails, evidence of tampering can allow the business to stop contaminated product from reaching consumers and trigger an immediate incident response.

The TACCP team is encouraged to take into account the relevance and proportionality of their mitigation measures to prevent product tampering as listed in Table H.6.

Table H.6 – Tamper detection mitigation measures

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Are there numbered seals on bulk storage silos, tanks or Intermediate Bulk Containers (IBC's)?				
2	Are labels and packaging materials stored securely with restricted access?				
3	Are effective tamper evident seals applied to retail packs?				
4	Are there numbered seals on hazardous materials?				
5	Is there close stock control of key materials?				
6	Is there effective verification and recording of seal numbers on delivery vehicles and shipping containers?				
7	Are seal numbers confirmed as issued by the supplier on arrival of delivery vehicles and containers?				
8	Is there use of continuous seal logs?				
9	Are there investigation processes for seal discrepancies?				

H.3 Mitigation measures for personnel security

The TACCP team is encouraged to consider the adequacy of personnel security measures as listed in Table H.7 to Table H.10.

Table H.7 – Pre-employment checks

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Is proof of identity required and verified prior to employment for all employees including contractors?				
2	Is there proof and verification of qualifications for all employees including contractors?				
3	Are there more rigorous screening and verification checks conducted for those in sensitive roles?				

Table H.8 – On-going personnel security

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Are employees in sensitive roles motivated and monitored?				
2	Is there a procedure in place for confidential reporting (whistleblowing or speak up) for employees to report suspicious or concerning behaviour by other people on site?				
3	Are temporary employees and contract workers fully supervised?				
4	Are individuals able to work alone?				
5	Is there a proactive food protection culture?				

Table H.9 – Contractor, agency workers and visitor security

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Are visitors always accompanied throughout the premises?				
2	Is there positive identification of all employees and visitors?				
3	Do employees or contractors wear branded uniforms to make impersonating an authorized person more difficult?				
4	Are there robust contractor management procedures?				

Table H.10 – End of contract arrangements/termination

No.	Prompt	Assessed/ addressed	Does not apply	No action needed	Needs attention
1	Is notification of contract termination sent to the relevant personnel for awareness?				
2	Are access cards, ID cards and keys recovered at termination?				
3	Are all computer accounts closed, network login access revoked and all electronic devices recovered?				
4	Are all branded uniforms returned when personnel leave the business?				
5	Is there reporting of unauthorized access by cyber systems?				
6	Is it standard procedure to have a termination interview to assess security implications?				

Annex I (informative)
Complementary approaches to food protection

I.1 Food Standard Agency

The Food Standards Agency's National Food Crime Unit (NFCU) has developed a Food Fraud Resilience Self-Assessment Tool to provide support, guidance, and advice to food businesses on food fraud.[21)]

I.2 Scottish Food Crime and Investigations Unit (SFCIU)

The SFCIU has developed a Food Crime Risk Profiling Tool to assist food business operators in assessing their vulnerability to food crime and identifying measures to mitigate these risks.[22)]

I.3 Food Crime Strategic Assessment (FCSA)

The FCSA is a joint assessment produced by the Food Standards Agency's National Food Crime Unit (NFCU) and Food Standards Scotland's Scottish Food Crime and Incidents Unit (SFCIU). This guide uses a risk-based framework to evaluate threats, covering seven types of food crime including document fraud, theft, waste diversion, unlawful processing, substitution, misrepresentation and adulteration.[23)]

I.4 SSAFE

The SSAFE Food Fraud Vulnerability Tool[24)] captures both opportunity and motivational indicators for fraudulent activity against the current control measures in place within a food business. It can be used by organisations across the food supply network irrespective of size, geographical location or type of food business. It is not designed to detect fraud incidents, but by addressing the identified vulnerabilities, unknown fraudulent activities may be identified and provide companies with the opportunity to stop them from occurring by exploring mitigation plans.

I.5 UK Food and Drink Federation

The UK FDF's Guide*, Food authenticity: Five steps to help protect your business from food fraud* [14] follows on from FDF's guide, *Risks under the radar – Anticipating supply chain risks for the UK food and drink sector* [15] and provides information on; mapping a business supply chain, identifying impacts, risks and opportunities, assessing and prioritizing the findings, creating a plan of action and implementing, tracking, reviewing and communicating.

21) Available at https://www.food.gov.uk/food-fraud-resilience-self-assessment-tool.
22) Available at https://www.foodstandards.gov.scot/business-guidance/running-a-food-business/food-crime-and-your-business/food-crime/food-crime-risk-profiling-tool.
23) Available at https://www.food.gov.uk/our-work/food-crime-strategic-assessment-2024.
24) Available at https://www.ssafe-food.org/resources/food-fraud-vulnerability-assessment-tool.

I.6 UK Government's Prepare website

The Prepare website provides an official online resource launched by the UK Government (primarily England), to help individuals, households, and communities prepare for emergencies and build personal and community resilience. The site encourages proactive preparation to make it easier to cope if an emergency occurs, and it links to regional variations (e.g. Ready Scotland for Scotland or NI Direct for Northern Ireland).[25)]

I.7 US Food and Drug Administration (FDA) resources supporting the FSAM IA Rule

For organizations in the USA, or exporting to the US, the Food Safety Modernization Act, (FSMA), IA Rule requires a Food Defence Plan. The Food Defence Plan Builder and the Food Defence Mitigation Strategies Database are voluntary FDA-developed online tools that support the development of a Food Defence Plan.

The mitigation database serves as a reference library of practical mitigation strategies to help food facilities reduce vulnerabilities due to intentional adulteration. It can assist food businesses in identifying and selecting mitigation measures for actionable process steps (high-risk points identified in vulnerability assessments). This database includes a list of mitigation strategies tied to common high-risk activities, e.g. bulk liquid handling, ingredient staging, and provides examples covering physical, operational and personnel-based mitigation measures.[26)]

The FDA also provides scenarios based on intentional and unintentional food contamination events to test emergency response plans, protocols and procedures.[27)]

25) Available at https://www.ssafe-food.org/resources/food-fraud-vulnerability-assessment-tool.
26) Available at https://www.fda.gov/food/food-defense-tools/mitigation-strategies-database.
27) Available at https://www.fda.gov/food/food-defense-tools/food-related-emergency-exercise-bundle-free-b.

Annex J (informative)
Sources of information and intelligence

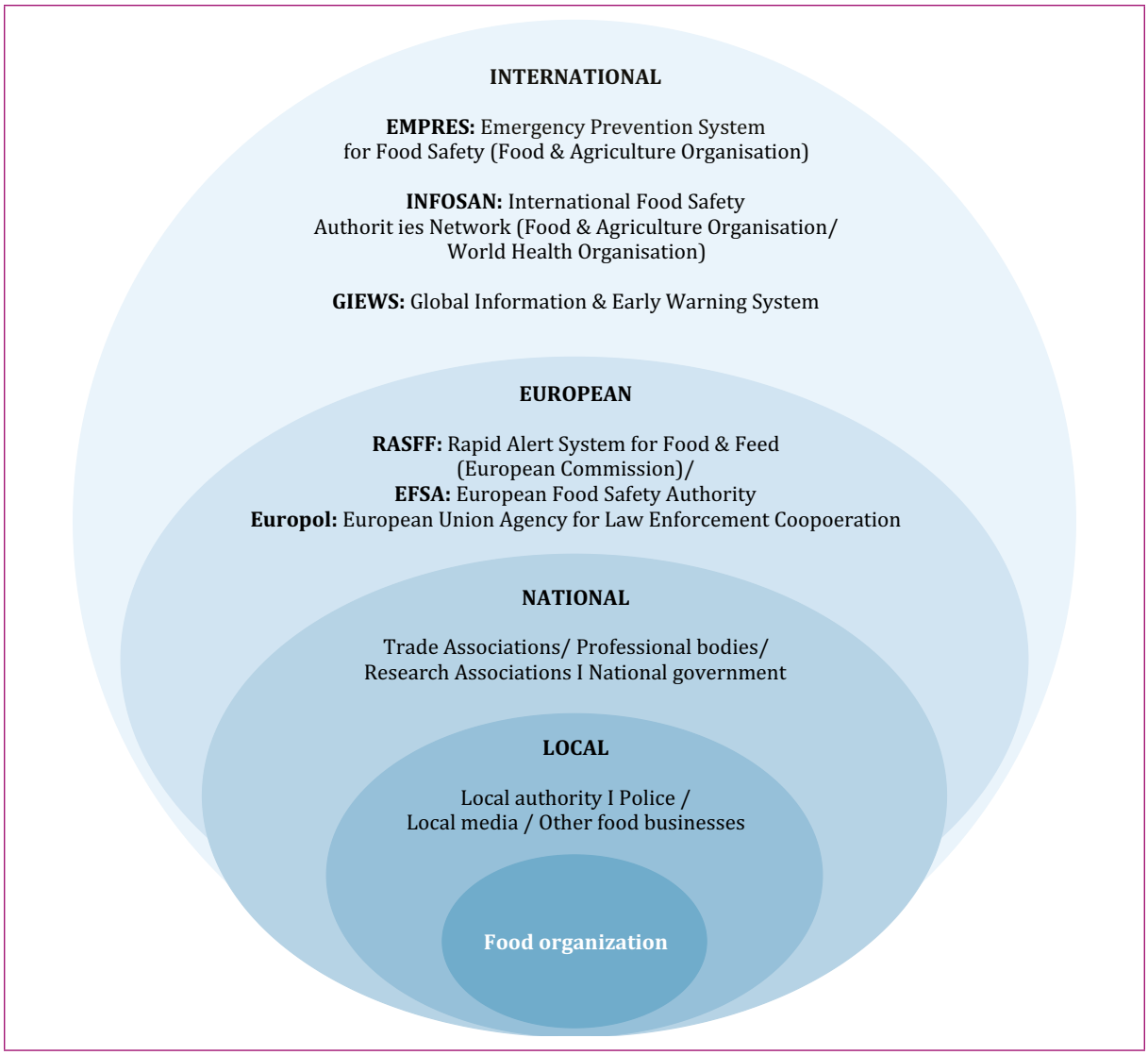
J.1 General

There are many organizations sharing information and working together on identifying new and emerging risks and coordinating control measures to reduce their impact. Global information is shared with national food safety organizations, such as national food safety organizations such as the UK's Food Standards Agency (FSA) and Food Standards Scotland (FSS). National authorities then pass the information onto food businesses, usually through trade associations and industry networks.

J.2 Information and intelligence levels

Figure J.1 shows how information and intelligence about emerging food risks flow from global sources down to the food organization. It can be used to update TACCP assessments.

Figure J.1 – Dissemination of information and intelligence on emerging risks to food



Information sharing can include the following:

a) Food organizations:

Food organizations receive information from local authorities who cascade information to food businesses, typically through trade associations.

b) Local:

Information to local authorities is provided from national organizations and Government Authorities.

c) National:

National food safety organizations such as the UK's Food Standards Agency (FSA) and Food Standards Scotland (FSS). Additional resources are from:

1) Food Industry Intelligence Network (FIIN);[28] and the
2) Food Authenticity Network (FAN).[29]

NOTE *Paid subscription services which provide helpful information include:*

- *HorizonScan;[30] and*
- *Food Fraud Database.[31]*

d) European:

EU organizations that provide information relevant to food protection include:

1) Europol;[32]
2) EFSA;[33]
3) Rapid Alert System for Food and Feed (RASFF);[34] and
4) other European government bodies and food industry associations often provide sector-specific food defence guidance, best practices, training and confidential industry alert systems. Check their respective websites for details.

e) International:

1) World Health Organization[35] (WHO), through the International Food Safety Authorities Network[36] (INFOSAN); and
2) Food and Agriculture Organization of the United Nations[37] (FAO) through the Emergency Prevention System[38] (EMPRES) and the Global Information and Early Warning System (GIEWS).

28) Available at https://www.fiin.co.uk/.
29) Available at https://www.foodauthenticity.global/.
30) Available at https://horizonscan.fera.co.uk/.
31) Available at https://www.foodchainid.com/products/food-fraud-database/.
32) Available at https://www.europol.europa.eu/.
33) Available at https://www.efsa.europa.eu/en.
34) Available at https://food.ec.europa.eu/food-safety/rasff_en.
35) Available at https://www.who.int/.
36) Available at https://www.fao.org/food-safety/emergencies/infosan/en/.
37) Available at https://www.fao.org/home/en.
38) Available at https://empres-i.apps.fao.org/general.

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 65000:2022, *Organizational resilience – Code of practice*

BS EN 17972:2024, *Food authenticity – Food authenticity and fraud – Concepts, terms and definitions*

Other publications

[1] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS (FAO) and WORLD HEALTH ORGANIZATION (WHO). General Principles of Food Hygiene. Codex Alimentarius Code of Practice, No. CXC 1-1969. Codex Alimentarius Commission. Rome 2023.

[2] TEXAS DIVISION OF EMERGENCY MANAGEMENT. Domestic Preparedness. *Looking back to look ahead to protect the food supply*. October 2022.[39)]

[3] FOOD STANDARDS AGENCY AND FOOD STANDARDS SCOTLAND. Food Crime Strategic Assessment 2024.[40)]

[4] THE NATIONAL CYBER SECURITY CENTRE (NCSC). NCSC Advice and guidance – Glossary.[41)]

[5] SPINK, J. and MOYER, D.C. Journal of Food Science. *Defining the Public Health Threat of Food Fraud.* John Wiley and Sons, 2011.

[6] NATIONAL PROTECTIVE SECURITY AUTHORITY (NPSA). National Protective Security Authority NPSA. May 2023.[42)]

[7] MANAGEMENT DIRECTORATE DEPARTMENT OF HOMELAND SECURITY. Instruction Manual 262-12-001-01, DHS Lexicon Terms and Definitions, 2017 Edition – Revision 2. Issue Date – October 16, 2017.

[8] OFFICE FOR NATIONAL STATISTICS (ONS). Nature of fraud and computer misuse in England and Wales: year ending March 2022. September 2022.[43)]

[9] SCOTTISH GOVERNMENT. Scottish Crime and Justice Survey 2023/24: Main findings June 2025.[44)]

[10] EUROPOL. European Union Terrorism Situation and Trend Report 2018 (TESAT 2018). 2018.[45)]

39) Available at https://www.domesticpreparedness.com/cbrne/preparedness-looking-back-to-look-ahead-to-protect-the-food-supply-2/.
40) Available at https://www.food.gov.uk/sites/default/files/media/document/FSA-Food%20Crime%20Strategy%202024.pdf.
41) Available at https://www.ncsc.gov.uk/section/advice-guidance/glossary.
42) Available at https://www.npsa.gov.uk/resources/npsa-insider-risk-definition.
43) Available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022.
44) Available at https://www.gov.scot/publications/scottish-crime-and-justice-survey-2023-24-main-findings/pages/fraud-and-computer-misuse/.
45) Available at https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2018_1.pdf.

[11] EUROPOL. Operation OPSON IX. 2021.[46)]

[12] THE NATIONAL CYBER SECURITY CENTRE, (NCSC). Ransomware: What you need to know about ransomware.[47)]

[13] SCIENCE DIRECT. Food-related fake news, misleading information, established misconceptions, and food choice. Stergios Melios, Afroditi A. Asimakopoulou, Ciara M. Greene, Emily Crofton, Simona Grasso. June 2025.[48)]

[14] FOOD AND DRINK FEDERATION. Guidance. Food Authenticity: Five steps to help protect your business from food fraud. 2024.[49)]

[15] FOOD AND DRINK FEDERATION. Risks under the radar – Anticipating supply chain risks for the UK food and drink sector.[50)]

46) Available at https://www.europol.europa.eu/cms/sites/default/files/documents/opson_ix_report_2021_0.pdf.
47) Available at https://www.ncsc.gov.uk/ransomware/home.
48) Available at https://www.sciencedirect.com/science/article/pii/S2214799325000396?ref=pdf_download&fr=RR-2&rr=99621f4d5a34d5e0.
49) Available at https://www.fdf.org.uk/fdf/resources/publications/guidance/food-authenticity/.
50) Available at https://www.fdf.org.uk/globalassets/resources/publications/risks-under-radar-april2020.pdf.

THIS PAGE DELIBERATELY LEFT BLANK

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards-based solutions.

Standards are carefully developed by subject matter experts, structured in a reliable format, and refined through an open consultation process.

Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting bsigroup.com/standards or contacting our Customer Relations team or Knowledge Centre.

Buying BSI publications

You can buy BSI publications, including British adoptions of European and international standards, at knowledge.bsigroup.com.

If you need international standards that are not adopted as British Standards, and/or national standards of other countries, copies can be ordered from our Customer Relations team.

Copyright in BSI publications

Storing and using BSI publications

BSI publications purchased in digital format:

- A user may download one single electronic copy of a BSI publication using Digital Rights Management (DRM). It may be stored and viewed on a maximum of three devices, provided that it is accessible by the sole named user only and that only one copy is accessed at any one time.
- A single printed copy may be printed for personal or internal company use only.

BSI publications purchased in printed format:

- A BSI publication purchased in printed format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than one copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see Subscriptions).

Reproducing extracts

For permission to reproduce content from BSI publications, contact our Licensing team.

Subscriptions

A BSI Knowledge subscription is an online platform that is available to your whole organization and provides unlimited access to a curated library of British, European, American and international standards and other standards-related publications. It includes tools that help teams manage updates, track changes, receive alerts, improve compliance and collaborate more efficiently across departments and locations. You can find out more at pages.bsigroup.com/subscription.

You can keep in touch with standards developments and receive substantial discounts on their purchase price, both in single-copy and subscription format, by becoming a BSI Subscribing Member.

You can find out more about becoming a BSI Subscribing Member and the benefits of membership at knowledge.bsigroup.com/membership.

Updates

British Standards and other publications are updated by amendment, correction or full revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication, please contact our Knowledge Centre.

Get involved with standards

Standards enable everything, and we welcome the knowledge and experience of anyone interested in developing them. You can help develop standards at www.bsigroup.com/en-GB/about-bsi/get-involved-with-standards/.

New to standards?

For a first step toward understanding and engaging with standards, helping you turn knowledge into action, download our free Beginner's Guide to Standards at www.bsigroup.com/en-GB/insights-and-media/insights/brochures/a-beginners-guide-to-standards/.

Useful contacts

Customer Relations
Tel: +44 345 086 9001
Email: cservices@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group

The Acre,
90 Long Acre, London,
WC2E 9RA, UK

BSI, The Acre, 90 Long Acre, London,
WC2E 9RA, United Kingdom

www.bsigroup.com