PAS 96:2014

Guide to protecting and defending food and drink from deliberate attack
Contents

Foreword ........................................................................................................ ii
Introduction .................................................................................................. iii
1 Scope ........................................................................................................ 1
2 Terms and definitions .............................................................................. 1
3 Types of threat .......................................................................................... 4
4 Understanding the attacker ....................................................................... 7
5 Threat Assessment Critical Control Point (TACCP) ................................. 9
6 Assessment ............................................................................................... 12
7 Critical controls ....................................................................................... 15
8 Response to an incident .......................................................................... 17
9 Review of food protection arrangements .............................................. 18

Annexes
Annex A (informative) TACCP case studies ............................................. 19
Annex B (informative) Sources of information and intelligence about emerging risks to food supply ................................................................. 31
Annex C (informative) Complementary approaches to food and drink protection .............................................................................................. 32

Bibliography ............................................................................................... 33

Standards publications .............................................................................. 33

Other publications and websites ............................................................. 33

List of figures
Figure 1 – A food supply chain ................................................................. 2
Figure 2 – Outline TACCP process .......................................................... 10
Figure 3 – Risk scoring matrix ................................................................. 14
Figure A.1 – Threat identification ............................................................ 21
Figure A.2 – Threat prioritization ............................................................. 28
Figure A.3 – Vulnerability assessment ....................................................... 30
Figure B.1 – Global dissemination of information and intelligence about emerging risks to food ................................................................. 31

List of tables
Table 1 – Risk assessment scoring ............................................................ 13
Table 2 – Approaches to risk reduction ..................................................... 15
Table 3 – Tamper evidence ....................................................................... 16
Table 4 – Personnel security .................................................................... 16
Table A.1 – Threat information ................................................................. 20
Table A.2 – Threat identification .............................................................. 22
Table A.3 – Threat assessment ................................................................. 26
Table A.4 – Threat assessment report 20140422 .................................... 29
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 October 2014.

Acknowledgement is given to the following organizations that were involved in the development of this PAS as members of the steering group:

- Agrico UK Limited
- Bakkavor
- Cargill
- Department for Environment, Food & Rural Affairs (Defra)
- Food and Drink Federation (FDF)
- Food Standards Agency (FSA)
- GiST Limited
- Global Food Security Programme
- Heineken UK
- Hilton Food Group plc
- J Sainsbury plc
- Leatherhead Food Research
- McDonald’s Europe
- Raspberry Blonde
- SSAFE
- Tesco plc

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a guide to be rapidly developed in order to fulfil an immediate need in industry. 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.

It has been assumed in the preparation of this PAS that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a PAS cannot confer immunity from legal obligations.
Introduction

The food industry sees the safety of its products as its main concern. Over the years, industry and regulators have developed food safety management systems which mean that major outbreaks of food poisoning are now quite unusual in many countries. These systems typically use Hazard Analysis Critical Control Point (HACCP) principles which are accepted globally. HACCP has proven to be effective against accidental contamination.

HACCP principles however have not been routinely used to detect or mitigate deliberate attacks on a system or process. Such attacks may include deliberate contamination or fraud. Deliberate acts may have food safety implications but can harm organizations in other ways, such as damaging business reputation or extorting money.

The common factor behind all such deliberate acts is people. The people may be within a food business, may be employees of a supplier to the food business, or may be complete outsiders with no connection to the food business. The key issue being their motivation; they may aim to cause harm to human health or business reputation, or to make financial gains at the expense of the business. In any of these situations it is in the interests of the food business to protect itself from such attacks.

The purpose of PAS 96 is to guide food business managers through approaches and procedures to improve the resilience of supply chains to fraud or other forms of attack. It aims to assure the authenticity of food by minimizing the chance of an attack and mitigating the consequences of a successful attack.

PAS 96 describes Threat Assessment Critical Control Points (TACCP), a risk management methodology, which aligns with HACCP, but has a different focus that may need input from employees from different disciplines, such as HR, procurement and/or security.

It explains the TACCP process, outlines steps that can deter an attacker or give early detection of an attack, and uses fictitious case studies (see Annex A) to show its application. Broadly, TACCP places food business managers in the position of an attacker to anticipate their motivation, capability and opportunity to carry out an attack, and devising protection. It also provides other sources of information and intelligence that may help identify emerging threats (see Annex B).

The TACCP process assumes and builds on a business' existing effective operation of HACCP, as many precautions taken to assure the safety of food, are likely to also deter or detect deliberate acts. It also complements existing business risk management and incident management processes.

The focus of this PAS is on protecting the integrity and wholesomeness of food and food supply. Any intending attacker, whether from within a food business or its supply chain, or external to both, is likely to attempt to elude or avoid routine management processes. It should help food businesses mitigate each of these threats, but the approach may also be used for other business threats.

No process can guarantee that food and food supply are not the target of criminal activity, but the use of PAS 96 can make it less likely. It is intended to be a practical and easily used guide and so is written in everyday language and should be used in a commonsense rather than legalistic way.

---

1) Further information and guidance regarding HACCP can be found in the CODEX Alimentarius publication, General Principles of Food Hygiene [1].
1 Scope

This PAS provides guidance on the avoidance and mitigation of threats to food and food supply. It describes a risk management methodology, Threat Assessment Critical Control Points (TACCP), which can be adapted by food businesses of all sizes and at all points in food supply chains.

It is intended to be of use to all organizations, but may be of particular use to managers of small and medium sized food enterprises who may not have easy access to specialist advice.

2 Terms and definitions

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

2.1 cyber security
procedures used to protect electronic systems from sources of threat

NOTE Examples of these threats are from malware and hackers intent on misusing IT systems, corrupting them or putting them out of use.

2.2 food defence
procedures adopted to assure the security of food and drink and their supply chains from malicious and ideologically motivated attack leading to contamination or supply disruption

NOTE The term food security refers to the confidence with which communities see food being available to them in the future. Except in the limited sense that a successful attack may affect the availability of food, food security is not used and is outside the scope of this PAS.

2.3 food fraud
committed when food is deliberately placed on the market, for financial gain, with the intention of deceiving the consumer

NOTE 1 Although there are many kinds of food fraud the two main types are:
- the sale of food which is unfit and potentially harmful, such as:
  - recycling of animal by-products back into the food chain;
  - packing and selling of beef and poultry with an unknown origin;
  - knowingly selling goods which are past their ‘use by’ date.
- the deliberate misdescription of food, such as:
  - products substituted with a cheaper alternative, for example, farmed salmon sold as wild, and Basmati rice adulterated with cheaper varieties;
  - making false statements about the source of ingredients, i.e. their geographic, plant or animal origin.
NOTE 2 Food fraud may also involve the sale of meat from animals that have been stolen and/or illegally slaughtered, as well as wild game animals like deer that may have been poached.

(SOURCE: FOOD STANDARDS AGENCY, http://food.gov.uk/enforcement/enforcework/foodfraud/#.USXn2v1OWwU [2])

2.4 food protection

procedures adopted to deter and detect fraudulent attacks on food

2.5 food supply

elements of what is commonly called a food supply chain

NOTE An example of a food supply chain is given in Figure 1. Figure 1 is not intended to be comprehensive.

2.6 hazard

something that can cause loss or harm which arises from a naturally occurring or accidental event or results from incompetence or ignorance of the people involved

2.7 Hazard Analysis Critical Control Point (HACCP)

system which identifies, evaluates, and controls hazards which are significant for food safety

(SOURCE: CODEX Alimentarius. General Principles of Food Hygiene [1])

2.8 insider

individual within or associated with an organization and with access to its assets but who may misuse that access and present a threat to its operations

Figure 1 – A food supply chain

Upstream

Agri-chemicals
Seed crops
Animal feed
Artificial insemination
Materials

Farming

Water

Product assembly

Primary ingredient manufacture

Distribution

Storage

Retail

Customer

Food service

Consumer

Waste disposal

Packaging

Downstream
2.9 personnel security
procedures used to confirm an individual’s identity, qualifications, experience and right to work, and to monitor conduct as an employee or contractor

**NOTE 1** Not to be confused with ‘personal security’.

**NOTE 2** Personnel security principles are used to assure the trustworthiness of staff inside an organization, but may be applied to the staff of suppliers within processes for vendor accreditation.

2.10 threat
something that can cause loss or harm which arises from the ill-intent of people

**NOTE** Threat is not used in the sense of threatening behaviour or promise of unpleasant consequence of a failure to comply with a malicious demand.

2.11 Threat Assessment Critical Control Point (TACCP)
systematic management of risk through the evaluation of threats, identification of vulnerabilities, and implementation of controls to materials and products, purchasing, processes, premises, distribution networks and business systems by a knowledgeable and trusted team with the authority to implement changes to procedures
3 Types of threat

3.1 General

Deliberate acts against food and food supply take several forms. Clause 3 describes the characteristics of the main threats to food authenticity and safety – economically motivated adulteration (EMA) and malicious contamination, and outlines the nature of other threats.

3.2 Economically motivated adulteration (EMA)

Case 1
In 2013, allegations were reported that a food factory in Asia was labelling cooking oil as peanut, chilli and olive when it contained none of these oils.2) The motivation of EMA is financial, to gain an increased income from selling a foodstuff in a way which deceives customers and consumers. This may be by either passing off a cheaper material as a more expensive one, (see case 1). Or it may be that a less expensive ingredient is used to replace or extend the more expensive one (see cases 2 and 3).

The avoidance of loss may also be an incentive for adulteration (see case 4). Limited supply of a key material may encourage a producer to improvise to complete an order rather than declare short delivery to the customer.

The intention of EMA is not to cause illness or death, but that may be the result. This was the case in 2008 when melamine was used as a nitrogen source to fraudulently increase the measured protein content of milk, resulting in more than 50 000 babies hospitalized and six deaths after having consumed contaminated infant formula.5)

The common factor in many cases of EMA is that the adulterant is neither a food safety hazard, nor readily identified, as this would defeat the aim of the attacker. Common adulterants6) include water and sugar; ingredients that may be properly used and declared but improper use is food fraud.

EMA is likely to be more effective for an attacker, and therefore present a greater threat to a food business, upstream on the food supply chain (see Figure 1) close to manufacture of primary ingredients. A successful adulteration (from the point of view of the attacker) continues without detection. EMA may need an insider but could be revealed by audit, for example:

• from purchases which are unexplained by recipes, such as sudan dyes which have no place in spice manufacture; or
• where there are differences between quantities sold and quantities purchased, such as beef mince sold and bovine meat purchased, with horsemeat to make up the difference.

2) Further details on this case of false food labels is available from: http://www.foodnavigator-asia.com/Markets/False-food-labels-on-82-impure-oils-in-China [3].
3) For further details are available from: http://oceana.org/sites/default/files/National_Seafood_Fraud_Testing_Results_Highlights_FINAL.pdf [4].
4) For further details on this adulteration case are available from: http://news.bbc.co.uk/1/hi/world/europe/8472377.stm [5].
5) For further details on this adulteration case see the WHO and FAO publication, Toxicological aspects of melamine and cyanuric acid [6].
6) Further information on common adulterants is available from the U.S. Pharmacopeial Convention Food Fraud Database: http://www.foodfraud.org/ [7].
3.3 Malicious contamination

Case 5
In 2005, a major British bakery reported that several customers had found glass fragments and sewing needles inside the wrapper of loaves.\(^7\)

Case 6
In 1984, the Rajneeshee sect in Oregon attempted to affect the result of a local election by contaminating food in ten different salad bars, resulting in 751 people affected by salmonella food poisoning.\(^8\)

Case 7
In 2013, a major soft drinks supplier was forced to withdraw product from a key market when it was sent a bottle which had had its contents replaced with mineral acid. The attackers included a note indicating that more would be distributed to the public if the company did not comply with their demands.

Case 8
In 2007, a bakery found piles of peanuts in the factory. It withdrew product and closed for a week long deep clean to re-establish its nut-free status.

The motivation for malicious contamination may be to cause localized (see case 5) or widespread (see case 6) illness or death.

In case 6, the attacker did not want the contamination to be detected before it was consumed, therefore the contaminant had to be an effective toxin with little effect on the palatability of the food.

The motivation in case 7 was publicity. Public opinion would have been against the attackers if harm had been caused to members of the public, but the supplier could not take that risk.

Materials which could be used by an attacker to gain publicity, or to extort money, are more readily found than those needed to cause widespread harm. The case of allergens (see case 8) shows the harm, impact and cost that can be caused to a business with little risk to the attacker.

Contamination close to point of consumption or sale, as in case 6, (downstream in Figure 1) is more likely to cause harm to health than an attack on crops or primary ingredients.

3.4 Extortion

Case 9
In 1990, a former police officer was convicted of extortion after contaminating baby food with glass and demanding money from the multi-national manufacturer.\(^9\)

Case 10
In 2008, a man was jailed in Britain after being convicted of threatening to bomb a major supermarket and contaminate its products.\(^10\)

The motivation for extortion by either an individual or group is financial, to obtain money from the victim organization. Such activity is attractive to the criminal mind when the product, like baby food (see case 9), is sensitive or where a company is seen as rich (see case 10).

A small number of samples can be used to show the company that the attacker has the capability and is enough to cause public concern and media interest.

3.5 Espionage

Case 11
One business consultancy uses the theft of the intellectual property of a fictitious innovative snack product as an example of commercial espionage.\(^11\)

Case 12
In July 2014, Reuters reported that a woman was charged in the USA with attempting to steal patented U.S. seed technology as part of a plot to smuggle types of specialized corn for use in China.\(^12\)

\(^7\) Further details on this case of malicious contamination are available from the Food Standards Agency archive: http://webarchive.nationalarchives.gov.uk/20120206100416/http://food.gov.uk/news/newsarchive/2006/dec/kingsmill [8].
\(^8\) For further information see the American Medical Association publication, A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars [9].
\(^9\) Further details on this food tampering case are available from Q Food publication: http://www.qfood.eu/2014/03/1989-glass-in-baby-food/ [10].
\(^11\) Further information on this fictional case study is available from Murray Associates: http://www.spybusters.com/mbsc1.html [12].
\(^12\) Further information is available from: http://www.grainews.ca/daily/chinese-woman-arrested-in-plot-to-steal-u-s-corn-technology [13].
The primary motivation of espionage is for competitors seeking commercial advantage to access intellectual property. They may infiltrate using insiders to report, or may attack remotely through information technology systems. Alternatively, organizations may try to entice executives to reveal confidential information or use covert recording to capture such material, or they may simply steal the material, as case 12 suggests.

3.6 Counterfeiting

Case 13
In 2013, enforcement officers seized 9,000 bottles of fake Glen’s Vodka from an illegal factory.13)

Case 14
In 2011, 340 bottles of a famous Australian brand of wine were seized, following complaints of poor quality to the owner, which had no link with Australia.14)

The motivation for counterfeiting is financial gain, by fraudulently passing off inferior goods as established and reputable brands. Both organized and petty crime can cause companies financial loss and harm to their reputation. The former, for example, can use sophisticated printing technologies to produce product labels that are indistinguishable from the genuine ones. The latter can steal genuine packs or even refill single use containers for resale.

Organized criminals may try to mimic the food contents closely to delay detection and investigation. Petty criminals may be tempted by a ‘quick killing’ and be less concerned about the safety of the food.

3.7 Cyber crime

Case 15
In 2014, Financial Fraud Action UK advised restaurant managers to stay vigilant as fraudsters are attempting to target their customers in a new phone scam. They phone restaurants claiming there is a problem with their card payments system, the restaurant is then told to redirect any card payments to a phone number provided by the fraudster.15)

Modern information and communications technologies provide new opportunities for malpractice. In the UK for the year to February 2013, Action Fraud received 58,662 cyber-enabled frauds and 9,898 computer misuse crime reports representing 41% of all of its reports, with an average loss of £3,689.16)

In case 15 the fraudster aims to defraud both business and consumer. It is common for the attacker to try and exploit individual ignorance of the technologies involved. Identity theft is perhaps more familiar to the public, but organizations may be aware of their identity being stolen to enable procurement fraud, in which goods are ordered in their name but diverted to the fraudsters premises leaving it to carry the cost and litigation.

13) Further information on this example of counterfeiting is available from: http://thecounterfeitreport.com/product/322/ [14].
15) Further information about this restaurant fraud is available from: http://www.financialfraudaction.org.uk/cms/assets/1/scam%20alert%20-%20restaurants%20fraud%20link%20doc.pdf [16].
4 Understanding the attacker

4.1 General
The success of a deliberate attack on food or food supply depends on several things:

a) Does the attacker have the motivation and drive to overcome the obvious, and less obvious blocks to their actions? If the blocks seem massive and success seems unlikely, many would-be attackers would seek an easier target.

b) Does the attacker have the capability to carry out the attack? A group is more likely to find the resources and learn the skills needed.

c) Does the attacker have the opportunity to carry out the attack? A physical attack needs physical access to the target, but a cyber-attack may only need access to a computer.

d) Would the attacker be deterred by the chance of detection and/or any potential penalties?

4.2 The extortionist
The extortionist wants to gain financially from an attack but does not want to be caught, and concentrates on avoiding detection. Their target is more likely to be a high profile business with lots to lose from negative publicity. They may work alone and be resourceful, secretive and self-interested. Some individuals may claim to be able to take action against a business while lacking the capability to carry it out; the business may judge the claim as not credible but still report and respond seriously.

4.3 The opportunist
The opportunist may hold an influential position within an operation to be able to evade internal controls. They may have some technical knowledge but their main asset is access. They are likely to be discouraged by the chance of detection, so unannounced visits by customers or auditors, or ad hoc sampling for analysis may deter their actions.

A supplier who cannot risk failure to deliver to a customer may take the chance that occasional adulteration would not be detected. Success on one occasion may make it easier to attempt a repeat. This opportunist may persuade themselves that the adulteration is legitimate, for example, chicken in a pork sausage would still be meat.

4.4 The extremist
The extremist takes their cause or campaign so seriously that they distort its context and overlook wider issues. The dedication to their cause may have no limits and their determination to progress it can be great.

Extremists may want to cause harm and are likely to enjoy publicity after the event. It may not matter, and may be a benefit, if they themselves are harmed. The risk of failure is a deterrent, but the risk of capture after the event is not. They are typically resourceful and innovative in devising ways to attack.

Some single issue groups may want to disrupt business operations and reputation but fear that mass harm to the public would damage their cause and lead them to lose support.

4.5 The irrational individual
Some individuals have no rational motive for their actions. Their priorities and preoccupations have become distorted so they are unable to take a balanced view of the world. Some may have clinically diagnosed mental health issues.

This individual may be readily deterred by simple steps which prevent them from gaining access to their target or make detection easy.

4.6 The disgruntled individual
The disgruntled individual believes that an organization has been unfair to them and seeks revenge. For example, they may be an aggrieved employee or former employee, supplier or customer. They may have expert knowledge of the operation and access to it.

This attacker is likely to be an individual rather than part of a group. If an insider, they could be dangerous, but are more likely to want to cause embarrassment and financial loss rather than harm to the public. If not an insider, this individual is more likely to claim or boast of having done something than actually being able to do it.
4.7 The hacktivist and other cyber criminals

A hacktivist or other cyber criminal aims to subvert controls on computerized information and communications systems in order to stop them working effectively, to steal or to corrupt data which they hold, and/or to disrupt internet business. Their motivation may be criminal, but may also be to demonstrate their expertise and ability to beat any protective system devised to stop them.

This type of attacker has information and communications technology expertise that can cause commercial harm and may pose an increasing threat to food safety as internet activity increases.

4.8 The professional criminal

Organized crime may see food fraud as a relatively simple crime, with big gains in prospect, little chance of apprehension, and modest penalties if convicted. The global trade in food in which food materials move, often with little notice, across enforcement area borders appears to encourage the professional criminal.

They may be deterred by close collaboration between food operations and national and international police authorities.
5 Threat Assessment Critical Control Point (TACCP)

5.1 Broad themes

TACCP should be used by food businesses as part of their broader risk management processes, or as a way of starting to assess risks systematically.

TACCP aims to:
• reduce the likelihood (chance) of a deliberate attack;
• reduce the consequences (impact) of an attack;
• protect organizational reputation;
• reassure customers, press and the public that proportionate steps are in place to protect food;
• satisfy international expectations and support the work of trading partners; and
• demonstrate that reasonable precautions are taken and due diligence is exercised in protecting food.

by, in broad terms:
• identifying specific threats to the company’s business;
• assessing the likelihood of an attack by considering the motivation of the prospective attacker, the vulnerability of the process, the opportunity and the capability they have of carrying out the attack;
• assessing the potential impact by considering the consequences of a successful attack;
• judging the priority to be given to different threats by comparing their likelihood and impact;
• deciding upon proportionate controls needed to discourage the attacker and give early notification of an attack; and
• maintaining information and intelligence systems to enable revision of priorities.

Food sector professionals want to minimize the chances of loss of life, ill health, financial loss and damage to business reputation that an attack could cause.

TACCP cannot stop individuals or organizations claiming that they have contaminated food, but it can help judge whether that claim is likely to be true. Any such claim, if judged to be credible, and any actual incident should be treated as a crisis. The organization needs to take steps to keep operations running and inform those involved.

5.2 TACCP process

In most cases TACCP should be a team activity, as that is the best way to bring skills, especially people management skills, together. For many small businesses the team approach is not practicable and it may be the job of one person. The TACCP team can and should modify the TACCP process to best meet its needs and adapt it to other threats as necessary to deal with four underlining questions:

a) Who might want to attack us?
b) How might they do it?
c) Where are we vulnerable?
d) How can we stop them?

The following flowchart (see Figure 2) and description of the TACCP process focuses on deliberate adulteration and contamination.
A standing TACCP team should be formed, which could include individuals with the following expertise:

- security;
- human resources;
- food technology;
- process engineering;
- production and operations;
- purchasing and supply;
- distribution;
- communications; and
- commercial/marketing.

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

**NOTE 2** For a small organization, one person may have to cover all of these roles.

**NOTE 3** While the HACCP team might provide a suitable starting point, the Business Continuity team might be a better model. The TACCP team is typically an established and permanent group able to continually review its decisions.

Since the TACCP process may cover sensitive material and could be of assistance to a prospective attacker, all team members should not only be knowledgeable of actual processes, but also trustworthy, discreet and aware of the implications of the process.

The TACCP team should:

1) evaluate all new information which has come to its attention;
2) identify individuals and/or groups which may be a threat to the organization and assess their motivation, capability and determination;
3) identify individuals and/or groups which may be a threat to the specific operation (e.g. premises, factory, site);
4) select a product which is representative of a particular process;
5) identify individuals and/or groups that may want to target the specific product;

**NOTE 4** For example, a suitable product would be typical of a particular production line and could be one which is more vulnerable.
6) draw a process flow chart for the product from but not limited by, ‘farm to fork’ including, for example, domestic preparation. The whole flow chart should be visible at one time. Particular attention should be paid to less transparent parts of the supply chain which might merit a subsidiary chart;

7) from an examination of each step of the process identify the vulnerable points where an attacker might hope for success and the people who would have access;

8) identify possible threats appropriate to the product at each step and assess the impact that the process may have in mitigating the threats;

   **NOTE 5** Model adulterants include low-cost alternative ingredients to premium components; model contaminants could include highly toxic agents, toxic industrial chemicals, readily available noxious materials and inappropriate substances like allergens or ethnically unwholesome foodstuffs.

   **NOTE 6** For example, cleaning may remove the contaminant, heat treatment may destroy it, and other food components may neutralize it.

9) select the points in the process where the threat would have the most effect, and where they might best be detected;

10) assess the likelihood of routine control procedures detecting such a threat;

   **NOTE 7** For example, routine laboratory analysis could detect added water or unusual fats and oils; effective management of buying would challenge unusual purchase orders.

11) score the likelihood of the threat happening, score the impact it would have, and chart the results to show the priority it should be given (see 6.3), and revise if this risk assessment seems wrong;

   **NOTE 8** Some lateral thinking may be needed. The TACCP team might ask, “If we were trying to undermine our business, what would be the best way?” It may consider how an attacker selects attack materials:
   • availability;
   • cost;
   • toxicity;
   • physical form; and/or
   • safety in use, for example pesticides on farms and aggressive flavour materials in factories may be convenient contaminants.

12) where the priority is high, identify who has unsupervised access to the product or process and whether they are trustworthy, and if that trust can be justified;

13) identify, record confidentially, agree and implement proportionate preventative action (critical controls). The TACCP team should have a confidential reporting and recording procedure that allows management action on decisions but does not expose weaknesses to those without a need to know (see case studies in Annex A);

14) determine the review and revise arrangements for the TACCP evaluation; and

   **NOTE 9** Review of the TACCP evaluation should take place after any alert or annually, and at points where new threats emerge or when there are changes in good practice.

15) maintain a routine watch of official and industry publications which give an early warning of changes that may become new threats or change the priority of existing threats, including more local issues as they develop.

   **NOTE 10** An outline of some information and intelligence systems is given in Annex B.
6 Assessment

**NOTE** The following lists are not intended to be exhaustive of all questions that may be asked to assess a threat.

### 6.1 Assessing threats

The product, the premises and the organization can be the target of an attack from a range of groups and individuals (see Clause 4), and each element should be assessed separately. The TACCP team should consider suppliers under financial stress, alienated employees and former employees, single issue groups, commercial competitors, media organizations, terrorist organizations, criminals and local pressure groups.

Commonly, a short supply chain involving fewer people may be less risky than a longer supply chain.

The TACCP team could ask the following questions to assess a threat.

**For the product:**
- Have there been significant cost increases which have affected this product?
- Does this product have particular religious, ethical or moral significance for some people?
- Could this product be used as an ingredient in a wide range of popular foods?
- Does the product contain ingredients or other material sourced from overseas?

**For the premises:**
- Are the premises located in a politically or socially sensitive area?
- Do the premises share access or key services with controversial neighbours?
- Are new recruits, especially agency and seasonal staff, appropriately screened?
- Are services to the premises adequately protected?
- Are external utilities adequately protected?
- Are hazardous materials, which could be valuable to hostile groups, stored on site?
- Are large numbers of people (including the general public) using the location?
- Do any employees have reason to feel disgruntled or show signs of dissatisfaction?

**For the organization:**
- Are internal audit arrangements independent?
- Have key roles been occupied by staff for many years with little supervision?

### 6.2 Assessing vulnerabilities

**NOTE** In this section EMA and malicious contamination are used as examples of approaches to vulnerability assessment.

#### 6.2.1 General

Individual organizations have different business needs and operate in different contexts. The TACCP team can judge which approach and questions are appropriate and proportionate to the threats they identify.

#### 6.2.2 Economically motivated adulteration (EMA)

A typical feature of EMA (see 3.2) is the substitution of a low cost item in place of a relatively high cost component/ingredient. The TACCP team needs to be alert to the availability of such alternatives. An example where this may happen is when added value is claimed, (e.g. organic, non-gm, locally grown, free range or with protected designations of origin). The attacker is likely to have ready access to lower value equivalents, which are almost indistinguishable.

**NOTE** Further guidance on sources of information and intelligence on the likelihood of food fraud is provided in Annex B.
The TACCP team needs to be confident that its own operations and those of its suppliers are in trustworthy hands. This can be achieved using advice on personnel security.\(^{17}\)

Questions which the TACCP team could ask include:

- Are low cost substitute materials available?
- Have there been significant material cost increases?
- Has pressure increased on suppliers’ trading margins?
- Do you trust your suppliers’ managers, and their suppliers’ managers?
- Do key suppliers use personnel security practices?
- Do suppliers think that we monitor their operation and analyze their products?
- Which suppliers are not routinely audited?
- Are we supplied through remote, obscure chains?
- Are major materials becoming less available (e.g. from crop failure) or alternatives plentiful (e.g. from overproduction)?
- Have there been unexpected increases or decreases in demand?
- How do suppliers dispose of excessive amounts of waste materials?
- Are we aware of shortcuts to the process which could affect us?
- Are our staff and those of suppliers encouraged to report concerns (whistleblowing)?
- Are accreditation records, certificates of conformance and analyzes reports independent?

6.2.3 Malicious contamination

Questions which the TACCP team could ask of both its own operations and that of its suppliers include:

- Are food safety audits rigorous and up-to-date?
- Are personnel security procedures in use?
- Is access to product restricted to those with a business need?
- Do storage containers have tamper-evident seals?
- Is the organization involved with controversial trade?
- Is the organization owned by nationals from conflict areas?
- Is there opportunity for access by sympathizers of single issue groups?
- Do any employees bear a grudge against the organization?
- Is staff boredom, discipline, recruitment a problem?
- Have business competitors been accused of espionage or sabotage?

6.3 Assessment of risk

Organizations need to understand the threats that they face, but should focus attention on the priority ones. For each identified threat the TACCP team considers and gives a score for the likelihood of each threat happening and for its impact (see Table 1).

<table>
<thead>
<tr>
<th>Likelihood of threat happening</th>
<th>Score</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high chance</td>
<td>5</td>
<td>Catastrophic</td>
</tr>
<tr>
<td>High chance</td>
<td>4</td>
<td>Major</td>
</tr>
<tr>
<td>Some chance</td>
<td>3</td>
<td>Significant</td>
</tr>
<tr>
<td>May happen</td>
<td>2</td>
<td>Some</td>
</tr>
<tr>
<td>Unlikely to happen</td>
<td>1</td>
<td>Minor</td>
</tr>
</tbody>
</table>

\(^{18}\) Further information on personnel security is available from: http://www.cpni.gov.uk/advice/Personnel-security/.

The likelihood of a threat happening can be judged by considering:

- whether an attacker would achieve their aims if successful;
- whether an attacker could have access to the product or process;
- whether an attacker would be deterred by protective measures;
- whether an attacker would prefer other targets; and
- whether an attack would be detected before it had any impact.

The impact might be assessed in financial terms or in terms of the seniority of staff needed to deal with it.

The risk score presented by each threat can be shown on a simple chart. An example risk scoring matrix is presented in Figure 3.
Figure 3 – Risk scoring matrix

<table>
<thead>
<tr>
<th>Impact</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Likelihood

<table>
<thead>
<tr>
<th>Very high risk</th>
<th>Threat A</th>
</tr>
</thead>
<tbody>
<tr>
<td>High risk</td>
<td>Threat B</td>
</tr>
<tr>
<td>Moderate risk</td>
<td>Threat C</td>
</tr>
<tr>
<td>Low risk</td>
<td>Threat D</td>
</tr>
<tr>
<td>Negligible risk</td>
<td>Threat E</td>
</tr>
</tbody>
</table>

NOTE This is an example risk scoring matrix, organizations may choose different criteria for the different risk categories.

6.4 TACCP reporting

Two fictional case studies showing how the TACCP process may be applied and adapted to best meet an individual company’s needs are given in Annex A. They are presented as formal records of the TACCP investigation and may be used to demonstrate that the business had taken all reasonable precautions should they be victims of an attack.
7 Critical controls

NOTE Tables 2, 3 and 4 are not intended to be exhaustive of all controls that may be considered relevant or proportionate to reduce a risk.

7.1 Controlling access
If a prospective attacker has no access to their target, then that attack cannot take place. It is not possible or desirable to prevent all access, but physical measures may limit access to certain individuals and those with a legitimate need. Some approaches to risk reduction that the TACCP team may feel are proportionate and relevant to their business are listed in Table 2.

Table 2 – Approaches to risk reduction

<table>
<thead>
<tr>
<th>Access to premises</th>
<th>Relevant? Proportionate?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to people on business only</td>
<td></td>
</tr>
<tr>
<td>Vehicle parking outside perimeter</td>
<td></td>
</tr>
<tr>
<td>Premises zoned to restrict access to those with a business need</td>
<td></td>
</tr>
<tr>
<td>Visible and comprehensive perimeter fencing</td>
<td></td>
</tr>
<tr>
<td>Perimeter alarm system</td>
<td></td>
</tr>
<tr>
<td>CCTV monitoring/recording of perimeter vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>Monitored access points</td>
<td></td>
</tr>
<tr>
<td>Approach roads traffic-calmed</td>
<td></td>
</tr>
<tr>
<td>Scheduled deliveries</td>
<td></td>
</tr>
<tr>
<td>Documentation checked before admittance</td>
<td></td>
</tr>
<tr>
<td>Missed deliveries investigated</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access to vehicles</th>
<th>Relevant? Proportionate?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to people</td>
<td></td>
</tr>
<tr>
<td>12 Chip &amp; PIN access control</td>
<td></td>
</tr>
<tr>
<td>13 Changing facilities, separate personal clothing from work wear</td>
<td></td>
</tr>
<tr>
<td>Screening of visitors</td>
<td></td>
</tr>
<tr>
<td>14 By appointment only</td>
<td></td>
</tr>
<tr>
<td>15 Proof of identity required</td>
<td></td>
</tr>
<tr>
<td>16 Accompanied throughout</td>
<td></td>
</tr>
<tr>
<td>17 Positive identification of staff and visitors</td>
<td></td>
</tr>
<tr>
<td>18 CCTV monitoring/recording of sensitive areas</td>
<td></td>
</tr>
<tr>
<td>Other aspects</td>
<td></td>
</tr>
<tr>
<td>19 Secure handling of mail</td>
<td></td>
</tr>
<tr>
<td>20 Restrictions on portable electronic and camera equipment</td>
<td></td>
</tr>
<tr>
<td>21 Limitations on access to mains services</td>
<td></td>
</tr>
<tr>
<td>22 BS ISO/IEC 27000 compliant cyber security</td>
<td></td>
</tr>
</tbody>
</table>
7.2 Tamper detection

Much raw material storage, some product storage, most distribution vehicles and all packaged foods can be tamper evident. Should an attacker gain access, tamper evidence gives some chance that the attack may be detected in time to avoid the impact.

Some approaches to aspects of tamper evidence that the TACCP team may feel are proportionate and relevant to their business are listed in Table 3.

Table 3 – Tamper evidence

<table>
<thead>
<tr>
<th>Detecting tampering</th>
<th>Relevant? Proportionate?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Numbered seals on bulk storage silos</td>
<td></td>
</tr>
<tr>
<td>2 Numbered seals on stores of labels and labelled packs</td>
<td></td>
</tr>
<tr>
<td>3 Effective seals on retail packs</td>
<td></td>
</tr>
<tr>
<td>4 Numbered seals on hazardous materials</td>
<td></td>
</tr>
<tr>
<td>5 Close stock control of key materials</td>
<td></td>
</tr>
<tr>
<td>6 Recording of seal numbers on delivery vehicles</td>
<td></td>
</tr>
<tr>
<td>7 Secure usernames and passwords for electronic access</td>
<td></td>
</tr>
<tr>
<td>8 Incursion reporting by cyber systems</td>
<td></td>
</tr>
</tbody>
</table>

7.3 Assuring personnel security

Personnel security guidance is used to mitigate the insider threat to the organization. Its principles can also be used by food businesses to judge whether key staff within the organizations that supply goods and services can be trusted to comply with specifications and procedures, and to work in the best interest of both the supplier and customer. Some approaches to assuring personnel security that the TACCP team may feel are proportionate and relevant to their business are listed in Table 4.

Table 4 – Personnel security

<table>
<thead>
<tr>
<th>Pre-employment checks</th>
<th>Relevant? Proportionate?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Proof of identity</td>
<td></td>
</tr>
<tr>
<td>2 Proof of qualifications</td>
<td></td>
</tr>
<tr>
<td>3 Verification of contractors</td>
<td></td>
</tr>
<tr>
<td>4 More sensitive roles identified with appropriate recruitment</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>On-going personnel security</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Staff in critical roles motivated and monitored</td>
</tr>
<tr>
<td>6 Whistleblowing arrangements</td>
</tr>
<tr>
<td>7 Temporary staff supervised</td>
</tr>
<tr>
<td>8 Individuals able to work alone</td>
</tr>
<tr>
<td>9 Favourable security culture¹⁸</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>End of contract arrangements</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Access and ID cards and keys recovered</td>
</tr>
<tr>
<td>11 Computer accounts closed or suspended</td>
</tr>
<tr>
<td>12 Termination interview assesses security implications</td>
</tr>
</tbody>
</table>

¹⁸ Further information on security culture is available from: http://www.cpni.gov.uk/advice/Personnel-security1/Security-culture/ [18].
8 Response to an incident

8.1 Management of a food protection crisis

Food protection and defence procedures aim to reduce the risk of an attack but cannot eliminate it, so emergency response and business continuity protocols are essential.

Food protection may sit within a business’ crisis management system (see BS 11200), and is likely to share its general objectives:

- to minimize physical and financial harm to consumers, customers, employees and others;
- to collaborate with investigatory and enforcement authorities;
- to gain public support for the organization;
- to minimize the cost, financial, reputational and personal, of the incident;
- to prevent re-occurrence; and
- to identify offenders.

Where contamination is implicit, quarantine and maybe withdrawal and recall of product might be expected.

In cases involving criminal action, police officers from serious crime units should be involved at the earliest opportunity to avoid any loss of evidence.

NOTE An important police contact in the U.K. may be the Anti-Kidnap and Extortion Unit of the National Crime Agency; others are also provided in Annex B.

Generally, the best time to learn how to manage a crisis is not in the crisis, so advanced planning and rehearsal of procedures is essential.

8.2 Contingency planning for recovery from attack

Business continuity management principles give good resilience to react to and recover from an attack. Advice on how best to develop and implement your organization’s recovery in response to a disruptive incident is provided in BS ISO 22313.
9 Review of food protection arrangements

It is vital that any changes which could affect the TACCP assessment, such as breaches and suspected breaches of security or authenticity, be immediately reported to the TACCP team leader who decides if a full review is needed.

The TACCP team should monitor official websites for updates in national threat assessments and for information on emerging risks, (see Annex B).

The local situation may be reviewed frequently and briefly against changes to conditions pertaining at the premises. A concise report of the review should have only limited circulation.

The TACCP team should regularly review food protection arrangements in line with other corporate policies.
Annex A (informative)
TACCP case studies

NOTE Both case studies are entirely fictitious and any resemblance to real organizations is coincidental.

A.1 General
This annex presents two case studies to illustrate how the TACCP process may be adapted, operated and reported by different organizations to reflect their business situation. They are written as formal records of the risk assessment exercise and do not attempt any background company context. Both companies have chosen to tabulate their findings.

Case study A is a national fast food chain, and case study B is a small enterprise with an owner/manager who handles all strategic and operational matters personally. In both cases the TACCP process has been deliberately changed from that described in Clause 5 to encourage users of this PAS to take an open-minded approach.

A.2 Case study A
Case study A presents an example report following the investigative work of the TACCP team at Burgers4U, a national fast food chain. The assumptions made are as follows:
• Burgers4U is a fictitious fast food chain with the unique selling proposition (USP) that it makes its own burgers. Nationally it is a major operator but it has no international business;
• the standard burger is considered to be typical of the range: standard, jumbo, veggie, cheese, and chilli;
• the Operations Director of Burgers4U leads the company’s Emergency Planning and Business Continuity Committee;
• the Head of Internal Audit holds delegated responsibility for security and fraud prevention;
• the TACCP team also received contributions from other managers on specialist topics; and
• this case study makes use of information in the Expert advisory group report: The lessons to be learned from the 2013 horsemeat incident [20].
TACCP case study A

Company: BURGERS4U
Location: All high street retail outlets
Product: Standard takeaway burger
TACCP team: Operations Director (Chairman)
Human Resources Manager
Procurement Manager
Technical Manager
Head of Internal Audit

Table A.1 – Threat information

<table>
<thead>
<tr>
<th>No</th>
<th>Threats to company from:</th>
<th>Possible method of operation</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Animal rights activists</td>
<td>Vandalism or sabotage</td>
<td>Little evidence of current activity</td>
</tr>
<tr>
<td>B</td>
<td>Hacktivists</td>
<td>Distributed denial of service (DDOS) attack on website</td>
<td>Developing company profile may provoke attack</td>
</tr>
<tr>
<td>C</td>
<td>Company buyers</td>
<td>Fraud; collusion with suppliers</td>
<td>Established team working autonomously</td>
</tr>
<tr>
<td>D</td>
<td>Criminals</td>
<td>Counterfeiting; misappropriation of packaging</td>
<td>Increasing risk as brand strengthens</td>
</tr>
<tr>
<td>E</td>
<td>Supporters of local businesses</td>
<td>Adverse publicity; ‘Guilt by association’ with fast food</td>
<td>Some locations report high levels of press interest</td>
</tr>
<tr>
<td>F</td>
<td>Overworked company staff, disenchanted</td>
<td>Petty contamination; possible serious malicious contamination</td>
<td>Some staff shortage where there is little post-18 education; and in locations with an extremist reputation</td>
</tr>
<tr>
<td></td>
<td>company staff, disenchanted could lead</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>to alliance with extremists (e.g.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>terrorists)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>Single issue groups</td>
<td>Deliberate infestation of premises</td>
<td>Some recent precedent</td>
</tr>
<tr>
<td>H</td>
<td>Front line staff</td>
<td>Theft; collusion with customers</td>
<td>Rigorous audit in place; Outlet managers trustworthy (personnel security checks)</td>
</tr>
<tr>
<td>I</td>
<td>Suppliers of meat</td>
<td>EMA – non-animal protein, or non-beef meats, replacing meat</td>
<td>Beef is specified and expected, even though not claimed in publicity</td>
</tr>
<tr>
<td>J</td>
<td>Front line staff</td>
<td>Deliberate undercooking of patty</td>
<td>Rotas minimize chance of collusion</td>
</tr>
<tr>
<td>K</td>
<td>Front line staff</td>
<td>Selling burger too long after wrapping</td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>Ideologically motivated group</td>
<td>Malicious contamination of component</td>
<td>Official threat level unchanged</td>
</tr>
</tbody>
</table>

**NOTE** Press reports of concerns about food authenticity are pertinent.
Figure A.1 – Threat identification

Start

01 Select bakery

02 Mains water

03 Store water, adjust temperature

04 Source flour + minor ingredients

05 Mix, divide, prove, bake buns

06 Cool, freeze, pack buns

07 Palletize

08 Cold storage

09 Deliver to Burgers4U

10 Select abattoir/cutting plant

11 Source meat

12 Butchery

13 Deliver to Burgers4U

14 Chill storage

15 Weigh seasonings etc

16 Weight meat for mince

17 Mince patty batches

18 Form pattys

19 Freeze pattys

20 Pack to cases

21 Palletize

22 Cold storage

23 Source packaging

24 Source consumables

25 Source pickle + garnish

26 Deliver to Burgers4U

27 Ambient storage

27 Ambient storage

28 Deliver to restaurant

29 Pick orders

30 Deliver to restaurant

31 Cold storage

32 Move to kitchen

33 Prepare burger

34 Wrap burger

35 Hot storage

36 Receive order

37 Supply order

38 Receive cash

39 Dispose of waste

End
### Table A.2 – Threat identification

<table>
<thead>
<tr>
<th>Step no</th>
<th>Process step</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Access</th>
<th>Mitigation</th>
<th>Adulterant; Contamination</th>
<th>Impact of process</th>
<th>QA/QC</th>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>01A</td>
<td>Select bakery</td>
<td>Various</td>
<td>Casual staff</td>
<td>Production staff</td>
<td>Contracts require personnel security protocols</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>01B</td>
<td>Select bakery</td>
<td>Fraud</td>
<td>Collusion</td>
<td>Buyers</td>
<td>Little</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>02</td>
<td>Mains water</td>
<td>Malicious contamination</td>
<td>Bulk storage reservoirs</td>
<td>Services engineers</td>
<td>Effective control of access</td>
<td>Soluble toxins</td>
<td>May inhibit yeast; may affect dough handling</td>
<td>May fail sensory tests</td>
<td>—</td>
<td>1 1</td>
</tr>
<tr>
<td>03</td>
<td>Store water; adjust temperature</td>
<td>As above</td>
<td>Batch storage reservoirs</td>
<td>As above</td>
<td>As above</td>
<td>As above</td>
<td>As above</td>
<td>—</td>
<td>1 1</td>
<td></td>
</tr>
<tr>
<td>04</td>
<td>Source flour + minor ingredients</td>
<td>Fraudulent substitution</td>
<td>Little cost advantage to fraudster</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>— —</td>
<td></td>
</tr>
<tr>
<td>05</td>
<td>Mix, divide, prove, bake buns</td>
<td>Malicious contamination</td>
<td>Batch mixing operation</td>
<td>Skilled mixer operative</td>
<td>Trained experienced staff</td>
<td>Powdered toxin</td>
<td>May inhibit yeast; may affect dough handling</td>
<td>May fail sensory tests</td>
<td>—</td>
<td>1 1</td>
</tr>
</tbody>
</table>
### Table A.2 – Threat identification (continued)

<table>
<thead>
<tr>
<th>Step no</th>
<th>Process step</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Access</th>
<th>Mitigation</th>
<th>Adulterant; Contamination</th>
<th>Impact of process</th>
<th>QA/QC</th>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>06</td>
<td>Cool, freeze, pack buns</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>07</td>
<td>Palletize</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>08</td>
<td>Cold storage</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>09</td>
<td>Deliver to Burgers4U</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>10A</td>
<td>Select abattoir / cutting plant</td>
<td>Fraud</td>
<td>Collusion</td>
<td>Buyers</td>
<td>Little</td>
<td>—</td>
<td>—</td>
<td>3</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>10B</td>
<td>Select abattoir / cutting plant</td>
<td>Fraudulent substitution</td>
<td>Poor segregation of species</td>
<td>Delivery drivers; process staff</td>
<td>Unique animal identification recorded</td>
<td>Meat from cheaper sources</td>
<td>Negligible</td>
<td>Random tests may detect unless collusion</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>Source meat</td>
<td>Fraudulent substitution</td>
<td>Poor segregation of species</td>
<td>Process management and staff</td>
<td>Meat from cheaper sources</td>
<td>Negligible</td>
<td>Random tests may detect unless collusion</td>
<td>4</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Butchery</td>
<td>Fraudulent substitution</td>
<td>Poor segregation of species</td>
<td>Process management &amp; staff</td>
<td>Meat from cheaper sources</td>
<td>Negligible</td>
<td>Random tests may detect unless collusion</td>
<td>2</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Deliver to Burgers4U</td>
<td>Hijacking of consignment</td>
<td>Supplier responsibility</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>14</td>
<td>Chill storage</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Step no</td>
<td>Process step</td>
<td>Threat</td>
<td>Vulnerability</td>
<td>Access</td>
<td>Mitigation</td>
<td>Adulterant; Contamination</td>
<td>Impact of process</td>
<td>QA/QC</td>
<td>Likelihood</td>
<td>Impact</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------</td>
<td>-----------------------------</td>
<td>---------------------</td>
<td>---------------------------------</td>
<td>--------------------------------------</td>
<td>----------------------------</td>
<td>--------------------</td>
<td>-------</td>
<td>------------</td>
<td>--------</td>
</tr>
<tr>
<td>15</td>
<td>Weigh seasonings etc</td>
<td>Malicious contamination</td>
<td>Manual operation</td>
<td>Process management &amp; staff</td>
<td>Rigorous hygiene standards</td>
<td>Powdered toxins</td>
<td>Negligible</td>
<td></td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>16</td>
<td>Weigh meat for mince</td>
<td>As above</td>
<td>As above</td>
<td>As above</td>
<td>As above</td>
<td></td>
<td>As above</td>
<td></td>
<td>As above</td>
<td>As above</td>
</tr>
<tr>
<td>17</td>
<td>Mince patty batches</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Form pattys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Freeze pattys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Pack to cases</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Palletize</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Cold storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Source packaging</td>
<td>Misappropriation; Counterfeiting</td>
<td>Supplier warehouse security; Agency delivery drivers</td>
<td>Little</td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Source consumables</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Source pickle + garnish</td>
<td>Ingredient substitution</td>
<td></td>
<td></td>
<td>Established brands; reliable contracts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Deliver to Burgers4U</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table A.2 – Threat identification (continued)

<table>
<thead>
<tr>
<th>Step no</th>
<th>Process step</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Access</th>
<th>Mitigation</th>
<th>Adulterant; Contamination</th>
<th>Impact of process</th>
<th>QA/QC</th>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>Ambient storage</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>28</td>
<td>Deliver to restaurant</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>29</td>
<td>Pick orders</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>30</td>
<td>Deliver to restaurant</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>31</td>
<td>Cold storage</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>32</td>
<td>Move to kitchen</td>
<td>Malicious substitution</td>
<td>Out of hours; unsupervised</td>
<td>Night store-staff</td>
<td>Tamper evident cases</td>
<td>‘Spiked’ pattys</td>
<td>Little</td>
<td>None</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>33</td>
<td>Prepare burger</td>
<td>Deliberate undercooking</td>
<td>Lone worker</td>
<td>Restaurant staff</td>
<td>Rigorous food safety manufacture</td>
<td>—</td>
<td>—</td>
<td>None</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>34</td>
<td>Wrap burger</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>35</td>
<td>Hot storage</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>36</td>
<td>Receive order</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>37</td>
<td>Supply order</td>
<td>Selling too long after wrapping</td>
<td>Restaurant manager under wastage pressure</td>
<td>—</td>
<td>Personnel security procedures</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
### Table A.2 – Threat identification (continued)

<table>
<thead>
<tr>
<th>Step no</th>
<th>Process step</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Access</th>
<th>Mitigation</th>
<th>Adulterant; Contamination</th>
<th>Impact of process</th>
<th>QA/QC</th>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>Receive cash</td>
<td>Theft</td>
<td>Restaurant staff</td>
<td>Counter staff</td>
<td>Automated cash tills; rigorous audit</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>39</td>
<td>Dispose of waste</td>
<td>Misappropriation; Counterfeiting</td>
<td>Unlocked external bins</td>
<td>Public</td>
<td>Daily removal</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

**NOTE** The symbol ‘—’ indicates ‘not applicable’ or ‘not significant’.

### Table A.3 – Threat assessment

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
<th>Vulnerable step</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Protective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Vandalism or sabotage</td>
<td>All locations</td>
<td>1</td>
<td>2</td>
<td>Maintain vigilance</td>
</tr>
<tr>
<td>B</td>
<td>DDOS attack on website</td>
<td>Marketing</td>
<td>3</td>
<td>3</td>
<td>Ensure cyber security good practice</td>
</tr>
<tr>
<td>C:01B</td>
<td>Fraud; collusion with suppliers</td>
<td>Select bakery</td>
<td>2</td>
<td>3</td>
<td>Job rotation &lt;5 years;</td>
</tr>
<tr>
<td>C:10A</td>
<td></td>
<td>Select abattoir/cutting plant</td>
<td>3</td>
<td>5</td>
<td>Internal audit</td>
</tr>
<tr>
<td>D:23</td>
<td>Counterfeiting; misappropriation of packaging</td>
<td>Source packaging</td>
<td>2</td>
<td>4</td>
<td>Formal notice to supplier; new supplier if no improvement in security after 6 months</td>
</tr>
<tr>
<td>D:39</td>
<td></td>
<td>Dispose of waste</td>
<td>1</td>
<td>2</td>
<td>No further action</td>
</tr>
<tr>
<td>E</td>
<td>Adverse publicity: ‘Guilt by association’ with ‘fast food’</td>
<td>Corporate</td>
<td>2</td>
<td>1</td>
<td>Review PR strategy</td>
</tr>
<tr>
<td>F:32</td>
<td>Petty contamination; Possible serious malicious contamination</td>
<td>Move to kitchen</td>
<td>1</td>
<td>3</td>
<td>Part used cases to be security sealed by manager</td>
</tr>
<tr>
<td>G</td>
<td>Deliberate infestation of premises</td>
<td>Restaurants</td>
<td>1</td>
<td>2</td>
<td>Maintain vigilance</td>
</tr>
<tr>
<td>H:38</td>
<td>Theft: collusion with customers</td>
<td>Receive cash</td>
<td>4</td>
<td>1</td>
<td>No further action</td>
</tr>
</tbody>
</table>
### Table A.3 – Threat assessment (continued)

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
<th>Vulnerable step</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Protective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>I:10B</td>
<td>EMA – non-animal protein, or non-beef meats, replacing meat</td>
<td>Select abattoir/cutting plant</td>
<td>2</td>
<td>3</td>
<td>Stronger management of vendor: technical audit, regular sampling/ad hoc testing, facilitate whistleblowing.</td>
</tr>
<tr>
<td>I:11</td>
<td></td>
<td>Source meat</td>
<td>4</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>I:12</td>
<td></td>
<td>Butchery</td>
<td>2</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>J:33</td>
<td>Deliberate undercooking of patty</td>
<td>Prepare burger</td>
<td>1</td>
<td>2</td>
<td>No further action</td>
</tr>
<tr>
<td>K:37</td>
<td>Selling burgers too long after wrapping</td>
<td>Supply order</td>
<td>2</td>
<td>2</td>
<td>No further action</td>
</tr>
<tr>
<td>L:02</td>
<td>Malicious contamination of component</td>
<td>Mains water</td>
<td>1</td>
<td>1</td>
<td>No further action</td>
</tr>
<tr>
<td>L:03</td>
<td></td>
<td>Store water; adjust temperature</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>L:05</td>
<td></td>
<td>Mix, divide, prove, bake buns</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>L:15</td>
<td></td>
<td>Weigh seasonings etc</td>
<td>1</td>
<td>3</td>
<td>Key staff to meet personnel security standards</td>
</tr>
</tbody>
</table>
## A.3 Conclusions

TACCP gave a threat register of 19 threats, of which 9 are under satisfactory control.

Fraud in the selection of abattoir/cutting plant is the greatest threat to Burgers4U. On-going cost penalties and significant reputational damage could result. Closely linked are the threats of species or non-meat protein substitution. Within the TACCP team, the Technical Manager is charged with the implementation of protective action with the objective of reducing the threat to (2,3) within 12 months. This action is likely to also mitigate other sourcing threats.

As a brand with an increasing reputation for quality and integrity, the threat of counterfeited goods increases. The traditional supplier of printed packaging material does not recognize this and has inadequate physical security procedures in place. As an otherwise reliable partner, the Procurement Manager is tasked with challenging the supplier to remedy the situation or to find an alternative. This threat should be assessed as (1,3) or better within 6 months.

The Burger4U website is not a primary selling instrument but does play a significant marketing role. The Head of Internal Audit is assigned to liaise with the Business Systems Department to ensure proper resourcing of cyber security procedures generally and against denial of service attacks in particular. No reduction in the assessment (3,3) is anticipated.

The Technical Manager is to monitor official and industry sources of information and intelligence on emerging risks and decide with the TACCP team chairman whether to reconvene the group in advance of its scheduled 6 monthly routine meeting.

### A.4 Case study B

Case study B presents an example threat assessment report of the proprietor of Bridgeshire Cheese Company, prepared by A Bridgeshire the Managing Partner, and summarizes their individual assessment of the threats it faces. Bridgeshire Cheese Company is a fictitious small family-farm owned and operated organic cheese producer selling to speciality retailers and food service businesses.

Table A.4 represents the company’s threat assessment report based on the vulnerability assessment flowchart (see Figure A.3).
<table>
<thead>
<tr>
<th>Threat no</th>
<th>From</th>
<th>Threat</th>
<th>Vulnerability a)</th>
<th>Mitigation</th>
<th>Consequence</th>
<th>Impact</th>
<th>Likelihood</th>
<th>Protective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Suppliers</td>
<td>Non-organic supply</td>
<td>‘Top-up’ milk; Bought-in calves; semen b)</td>
<td>All goods from accredited suppliers</td>
<td>Loss of organic status</td>
<td>5</td>
<td>2</td>
<td>Require certificate of conformance for all ad hoc purchases</td>
</tr>
<tr>
<td>2</td>
<td>Neighbours</td>
<td>Widespread livestock disease</td>
<td>Rights of way through farm</td>
<td>Biosecurity meets best practice</td>
<td>Loss of herd and/or insurance cover</td>
<td>3</td>
<td>2</td>
<td>Install reservoir to avoid effluent discharge when wind from the SW</td>
</tr>
<tr>
<td>3</td>
<td>BCC staff</td>
<td>Malicious contamination</td>
<td>Manual operations, unsupervised (process largely self-controlling)</td>
<td>All staff are family members or long term trusted partners; All batches are taste tested</td>
<td>Localized illness possible</td>
<td>2</td>
<td>1</td>
<td>No further action</td>
</tr>
<tr>
<td>4</td>
<td>Adjacent farms</td>
<td>Trials of GM crops</td>
<td>Perimeter pasture land</td>
<td>Accreditation organization campaign</td>
<td>Loss of organic status</td>
<td>4</td>
<td>3</td>
<td>Cooperative action with trade association to lobby elected officials</td>
</tr>
<tr>
<td>5</td>
<td>Opportunist</td>
<td>Theft of product</td>
<td>Distribution, vehicle often unmanned and unlocked</td>
<td>Little</td>
<td>Value of goods; Loss of reputation for reliability</td>
<td>2</td>
<td>3</td>
<td>Replace with more modern vehicle at earliest opportunity</td>
</tr>
</tbody>
</table>

A) See Figure A.3 for the full vulnerability process assessment.
B) Other goods are routinely sourced from long-standing accredited companies.
Figure A.3 – Vulnerability assessment
Annex B (informative)
Sources of information and intelligence about emerging risks to food supply

B.1 Figure B.1 illustrates local and global systems which may be used to update TACCP assessments.

Figure B.1 – Global dissemination of information and intelligence about emerging risks to food

Annex C (informative)
Complementary approaches to food and drink protection

C.1 CARVER+Shock

CARVER+Shock is an offensive prioritization tool that has been adapted for use in the American food sector. Like TACCP, CARVER+Shock involves an organization playing 'Red Team', where the team members put themselves in the place of the prospective attacker and ask:

a) If I wanted to cause harm, or make more money, or gain publicity, or take advantage of the situation in some other way:
   • What would I do?
   • Where would I do it?
   • When would I do it?

In effect they use the military targeting tool to judge weaknesses by assessing their:

- Criticality
- Accessibility
- Recognizability
- Vulnerability
- Effect
- Recoverability

More information on CARVER+Shock is available from Carver + Shock Primer [24].

C.2 EU 5-point action plan

The EU 5-point Action Plan to address the shortcomings identified in Europe's food supply chain [25] is to be implemented by 2014.

1) Develop synergies between enforcement authorities, ensure rapid exchange of information on intentional violations of food chain rules, promote the involvement of Europol in investigations.

2) Ensure that rules on horse passports are enforced correctly, that passports are delivered only by competent authorities and that national databases are created.

3) Require that financial penalties for intentional violations of food chain rules be established at sufficiently dissuasive levels, and that control plans in the Member States include unannounced controls.

4) Adopt rules on mandatory origin labelling of meat (sheep, goat, pig, poultry, horse, rabbit, etc.) and deliver a report in autumn 2013 on the possible extension of mandatory origin labelling to all types of meat used as ingredient in foods.

5) Present and assess the results of the controls currently carried out in the EU countries.

C.3 UK Food and Drink Federation

The UK Food and Drink Federation’s (FDF) Guide on ‘Food authenticity: Five steps to help protect your business from food fraud [26], follows on from FDF’s guide ‘Sustainable Sourcing: Five steps towards managing supply chain risk’ [27] and provides information on:

1) mapping your supply chain;
2) identifying impacts, risks and opportunities;
3) assessing and prioritizing your findings;
4) creating a plan of action; and
5) implementing, tracking, reviewing and communicating.
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.

Risk management
BIP 2153, Managing risk the ISO 31000 way
BS 31100, Risk management – Code of practice and guidance for the implementation of BS ISO 31000
BS EN 31010, Risk management – Risk assessment techniques
BS ISO 31000, Risk management – Principles and guidelines
PD ISO/TR 31004, Risk management – Guidance for the implementation of ISO 31000

Crisis management
BS 11200, Crisis management – Guidance and good practice

Business continuity management
BS ISO 22301, Business continuity management systems – Requirements and guidance
BS ISO 22313, Societal security – Business continuity management systems – Guidance

Supply chain security
BS ISO 28000, Specification for security management systems for the supply chain
BS ISO 28002, Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use
PD CEN/TR 16412, Supply chain security (SCS) – Good practice guide for small and medium sized operators

Information security
BS ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary

Other standards
BS 10501, Guide to implementing procurement fraud controls
BS EN ISO 22000, Food safety management systems – Requirements for any organization in the food chain

Other publications and websites


Further reading

BRC Global Standard for Food Safety. British Retail Consortium.


British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

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

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similarly for PASs, please notify BSI Customer Services.

Tel: +44 (0)845 086 9001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)845 086 9001
Email: plus@bsigroup.com

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)845 086 9001
Email: membership@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website www.bsigroup.com/shop. In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)845 086 9001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. This does not preclude the free use, in the course of implementing the standard, of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained. Details and advice can be obtained from the Copyright & Licensing Department.

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com