PAS 96:2017

Guide to protecting and defending food and drink from deliberate attack

Department for Environment Food & Rural Affairs

Food Standards Agency
food.gov.uk

bsi.

Publishing and copyright information

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

ISBN 978 0 580 98099 2

ICS 67.020

Publication history

First published March 2008

Second edition March 2010

Third edition October 2014

Fourth (current) edition November 2017

Contents

Foreword

This PAS was 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 16 November 2017.

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
- British Frozen Food Federation (BFFF)
- Campden BRI
- Crowe Clark Whitehill LLP
- Danone
- Department for Environment, Food & Rural Affairs (Defra)
- Food Standards Agency
- GIST Limited
- McDonald's Europe
- National Cyber Security Centre (NCSC)
- Sodexo Limited
- Tesco UK
- Tulip Limited
- University College London
- Willis Towers Watson

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 It will be withdrawn upon publication of its content in, or as, a British Standard.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.

Supersession

This PAS supersedes PAS 96:2014, which is withdrawn.

Information about this document

This is a full revision of the PAS 96:2014, and introduces the following principal changes:

- normative and informative references have been updated;
- subclause **3.7** Cyber-crime has been revised;
- subclause **6.2.4** added to cover vulnerabilities related to cyber-attacks;
- two new fictional case studies have been added as subclauses **A.5** and **A.6** to illustrate cyber security issues;
- Annex B updated;
- Annex D added covering 10 steps to cyber security;
- some editorial amendments have been undertaken.

Use of this document

As a guide, this PAS takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice and claims of compliance cannot be made to it.

Presentational conventions

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

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Contractual and legal considerations

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.[1)] 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 include deliberate contamination, electronic intrusion, and 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. These 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, business reputation, or 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 and safety 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 human resources, procurement, security and information technology.

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 then helps them devise 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 is to be used in a common-sense 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. While concerns for the safety and integrity of food and drink are paramount and much of the PAS is focussed on them, it needs to be stressed that its scope covers 'All Threats' and protection of all elements of food supply. This includes the viability of businesses within the supply chain.

It is intended to be of use to all organizations, but is of particular use to managers of small and medium sized food enterprises without 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

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

{SOURCE: NCSC Glossary [2]}

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

dishonest act or omission, relating to the production or supply of food, which is intended for personal gain or to cause loss to another party[2)]

NOTE 1 *Although there are many kinds of food fraud the two main types are:*

1) *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;*

[2)] The UK Food Standards Agency discusses food crime and food fraud at: https://www.food.gov.uk/enforcement/the-national-food-crime-unit/what-is-food-crime-and-food-fraud [3].

2) 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.*

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)

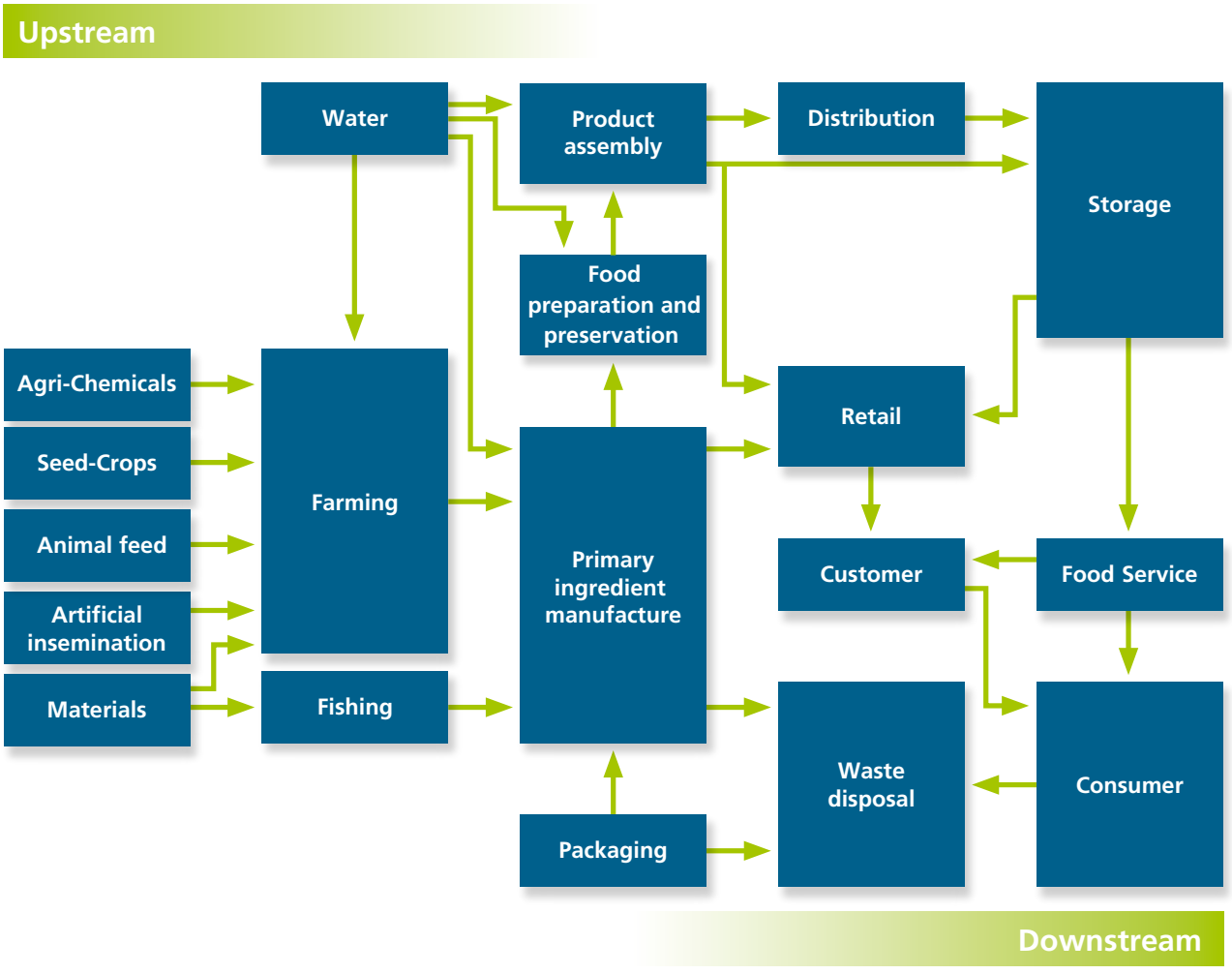
system which identifies, evaluates, and controls hazards which are significant for food safety

{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



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, people, 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 explains the nature of other threats, particularly the rapidly growing misuse of digital techniques.

3.2 Economically motivated adulteration (EMA)

NOTE *Details of many other cases are available from the US Pharmacopeial Convention's Food Fraud Database at http://www.foodfraud.org/ [4].*

Case 1

In 2016, customs officials in Nigeria confiscated 2.5 tonnes of rice which they suspected was made from plastic.[3)]

Case 2

Olive oil has been a frequent target for adulteration, often by other vegetable oils. In 2017 Italian authorities disrupted an organized crime ring which was exporting fake olive oil to the United States.[4)] Similarly, Brazilian officials reported that a very high proportion of olive oils tested did not meet the quality standards required by their labelling.[5)]

Case 3

Spanish police have accused a beef burger manufacturer of using minced pork and soya to increase the perceived meat content of their products for many years.[6)] It is not clear whether the burgers actually contained enough beef to satisfy any official regulation.

Case 4

In 2014 the Kenyan Dairy Board claimed that hawkers were putting lives at risk by adding preservatives (formalin and hydrogen peroxide) in a (probably futile) attempt to extend the shelf life of milk.[7)]

Case 5

Staff in a European meat packer felt, mistakenly, that they could avoid a product being condemned as carrying foot and mouth disease by covering it with disinfectant.

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 cases 4 and 5). 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.[8)]

[3)] Further information is available from: http://www.bbc.co.uk/news/world-africa-38391998 [5].

[4)] Further information is available from: https://www.oliveoiltimes.com/olive-oil-business/italy-arrests-33-accused-olive-oil-fraud/55364 [6].

[5)] Additional case study can be found: https://www.oliveoiltimes.com/olive-oil-business/brazil-reveals-widespread-olive-oil-fraud/56395 [7].

[6)] Further information is available from: https://www.euroweeklynews.com/3.0.15/news/on-euro-weekly-news/spain-news-in-english/144405-police-uncover-major-beef-food-fraud-in-spain [8].

[7)] Further information is available from: http://www.standardmedia.co.ke/article/2000107380/naivasha-hawkers-using-formalin-to-preserve-milk [9].

[8)] For further details on this adulteration case see the WHO and FAO publication, Toxicological aspects of melamine and cyanuric acid http://www.who.int/foodsafety/publications/melamine-cyanuric-acid/en/ [10].

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 adulterants[9] 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 verification, for example, financial audit could reveal:

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

3.3 Malicious contamination

Case 6

In 2005, a major British bakery reported that several customers had found glass fragments and sewing needles inside the wrapper of loaves.[10]

Case 7

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.[11]

Case 8

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 9

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 6) or widespread (see case 7) illness or death.

In case 7, 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 8 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 9) 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 7, (downstream in Figure 1) is more likely to cause harm to health than an attack on crops or primary ingredients.

3.4 Extortion

Case 10

In 1990, a former police officer was convicted of extortion after contaminating baby food with glass and demanding money from the multi-national manufacturer.[12]

Case 11

In 2008, a man was jailed in Britain after being convicted of threatening to bomb a major supermarket and contaminate its products.[13]

[9] For further information on adulterants see the U.S. Pharmacopeial Convention Food Fraud Database Version 2.0 at: http://www.foodfraud.org/#/food-fraud-database-version-20 [11].

[10] For further details on this case of malicious contamination see the Food Standards Agency archive at: http://webarchive.nationalarchives.gov.uk/20120206100416/http://food.gov.uk/news/newsarchive/2006/dec/kingsmill [12].

[11] For further information see the American Medical Association publication, A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars [13].

[12] For further details on this food tampering case see the Q Food publication at: http://www.qfood.eu/2014/03/1989-glass-in-baby-food/ [14].

[13] For further details on this extortion case see The Guardian article at: http://www.theguardian.com/uk/2008/jan/28/ukcrime [15].

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 10), is sensitive or where a company is seen as rich (see case 11).

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 12

One business consultancy uses the theft of the intellectual property of a fictitious innovative snack product as an example of commercial espionage.[14)]

Case 13

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.[15)]

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 13 suggests.

3.6 Counterfeiting

Case 14

In 2013, enforcement officers seized 9 000 bottles of fake Glen's Vodka from an illegal factory.[16)]

Case 15

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.[17)]

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 in the safety of the food.

[14)] For further information on this fictional case study is available from Murray Associates at: https://counterespionage.worldsecuresystems.com/tscm-the-missing-business-school-course.html [16].

[15)] For more information go to: http://www.grainews.ca/daily/chinese-woman-arrested-in-plot-to-steal-u-s-corn-technology [17].

[16)]) For further information on this example of counterfeiting see: http://thecounterfeitreport.com/product/322/ [18].

[17)] For further information on this case of counterfeiting see http://www.news.com.au/finance/offshore-raids-turn-up-fake-aussie-jacobs-creek-wines/story-e6frfm1i-1226029399148 [19].

3.7 Cyber crime

Case 16

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.[18)]

Modern information and communication technologies provide new and rapidly increasing opportunities for malpractice. In case 16 the fraudster uses social engineering to try to defraud both business and consumer. It is common for the attacker to try and exploit individual ignorance of the technologies involved. The fraud in this case is 'cyber-enabled', that is a familiar scam made easier by electronic communications. In total in England and Wales for the year to September 2016, the Office for National Statistics reported about 3.6 million frauds and nearly 2 million cases of computer misuse.[19)]

Case 17

In 2016, reports suggested that criminals had hacked Deliveroo accounts to order food on victims' cards.[20)]

Case 18

In 2015, Michigan-based Biggby Coffee reported a database breach with possible theft of customer information derived from loyalty card applications.[21)]

The fraud in both cases 17 and 18 could be carried out remotely over the Internet with little chance of detection and justice for the perpetrator.

Case 19

In 2016 the FBI and US Department of Agriculture alerted farmers to their increasing vulnerability to cyber-attack through their use of precision agriculture technology. [22)]

Such an attack could be cyber-enabled industrial espionage, or hacking - gaining unauthorized access to computer systems, perhaps with malicious intent.

Case 20

In 2016 a major supermarket discovered that scales at its self-service check outs had been corrupted to enable distributed denial of service (DDOS) attacks on public websites.

DDOS can be a real nuisance to companies, and lead to real losses when the company website is an important trading platform. The 'Internet of Things' (IoT) becomes more and more important; the Joint NCSC/NCA Threat Report[23)] exposes the vulnerability of (apparently innocuous) internet connected devices and their misuse by criminals.

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 the duped supplier and supposed purchaser to carry the cost and litigation.

[18)] For further information about this restaurant fraud see https://www.financialfraudaction.org.uk/news/2014/08/13/scam-alert-restaurants-and-diners-targeted-in-new-scam/ [20].

[19)] ONS Dataset: Crime in England and Wales: Experimental tables: Table E1: Fraud and computer misuse by loss (of money or property) – number and rate of incidents and number and percentage of victims from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables [21].

[20)] For further information see: https://business-reporter.co.uk/2016/11/23/cyber-criminals-use-hacked-deliveroo-accounts-order-food-victims-cards/ [22].

[21)] For further information see: http://www.canadianbusiness.com/business-news/michigan-based-biggby-coffee-reports-database-breach-possible-theft-of-customer-information [23].

[22)] Private Industry Notification PIN 160331-001 Smart Farming May increase Cyber Targeting Against US Food and Agriculture Sector see https://info.publicintelligence.net/FBI-SmartFarmHacking.pdf [24].

[23)] The Cyber Threat to UK Business at https://www.ncsc.gov.uk/news/ncsc-and-nca-threat-report-provides-depth-analysis-evolving-threat [25].

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. Cyber attacks across the world using 'ransomware' have demonstrated both how easily extortionists can now attack multiple victims and how difficult it is to bring them to justice.[24)] 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 decide to respond appropriately.

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.

[24)] For further information see The Cyber Threat to UK Business, pg 7 available from: https://www.ncsc.gov.uk/news/ncsc-and-nca-threat-report-provides-depth-analysis-evolving-threat [25].

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 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 Cyber criminals and other malicious digital actors

Cyber criminals aim 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 or even political, but may also be to demonstrate their expertise and ability to beat any protective system devised to stop them.

Traditionally, this type of attacker has information and communications technology expertise that can cause commercial harm. However, as warned in the Joint UK NCSC/NCA threat report [25], "The lines between those committing attacks continue to blur, with criminal groups imitating states …… and more advanced actors successfully using 'off the shelf' malware to launch attacks."[25)] This 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. The anonymity of the internet and the opportunity for remote intrusion into electronic systems makes cyber-crime increasingly attractive to professional criminals.

They may be deterred by close collaboration between food operations and national and international police authorities.

[25)] NCSC and NCA The Cyber Threat to UK Business available from: https://www.ncsc.gov.uk/news/ncsc-and-nca-threat-report-provides-depth-analysis-evolving-threat [25].

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 and the certainty of information on which the assessment is based;
- 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;
- prioritizing threats based on risk, and communicating such a prioritization across trading partners for shared risk acceptance;
- 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.

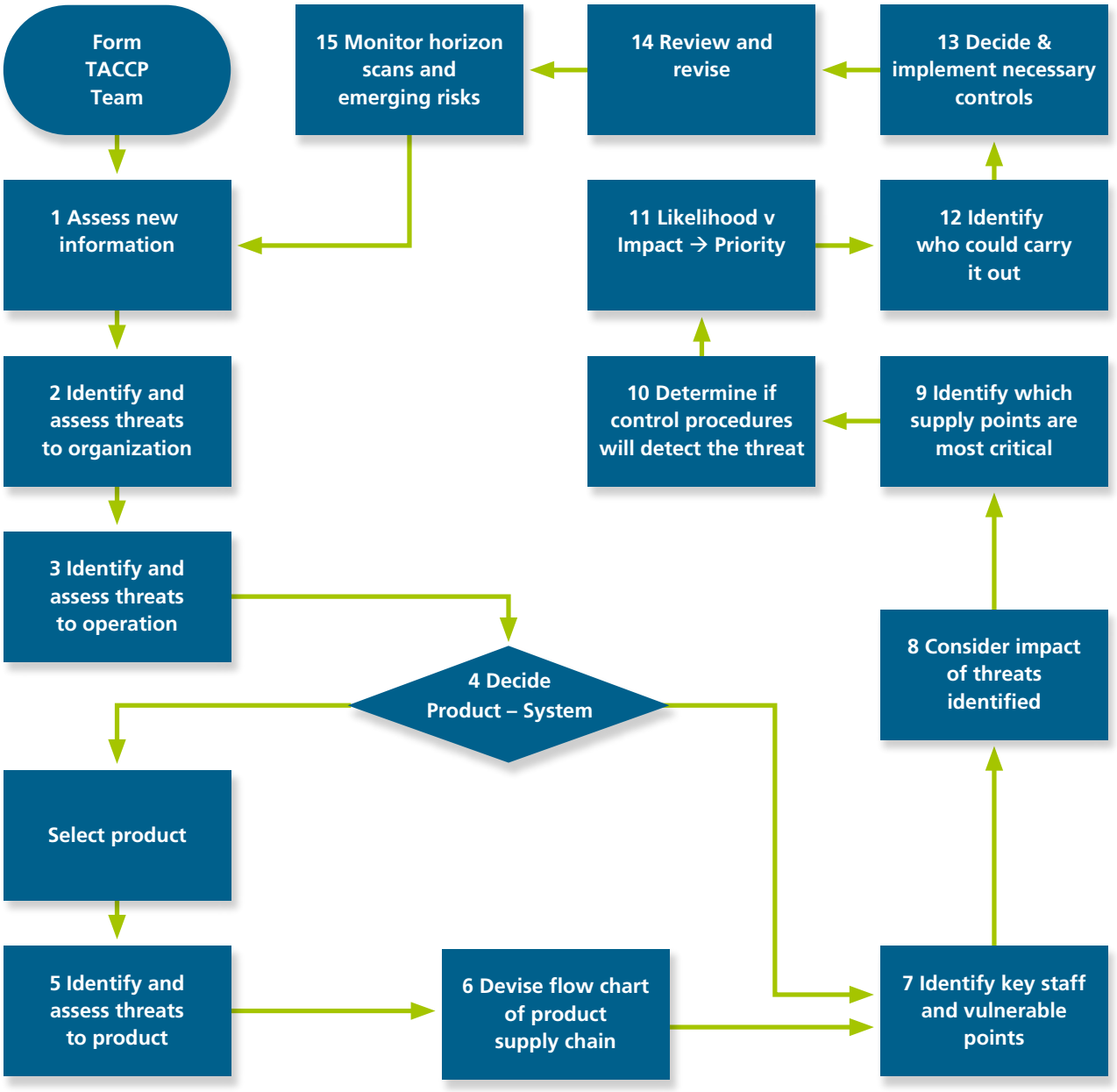
5.2 TACCP process

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 flowchart (see Figure 2) outlines the TACCP process and focuses on deliberate adulteration and contamination. Further information on each element of the TACCP process set out in Figure 2 is given in the corresponding numbered list [see **5.2**, 1) – **5.2**, 15)].

Figure 2 – Outline TACCP process



NOTE 1 *An alternative risk approach is CARVER + Shock which is outlined in Annex C.*

NOTE 2 *Figure 2 is meant to be an indicative illustration only.*

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 procurement;
- distribution and logistics;
- information technology;
- 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 its systems, especially electronic systems, 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) differentiate product threats from other threats:
   a) for non-product threats, go to Clause **11**;
   b) for product threats, select a product which is representative of a particular process;

   NOTE 4 *For example, a suitable product would be typical of a particular production line and could be one which is more vulnerable.*
5) identify individuals and/or groups that may want to target the specific product;
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) identify both the vulnerable points where an attacker might hope for success and the people who would have access from an examination of each step of the process;
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 Evaluating threats

The product, the premises and the organization and its information systems 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 evaluate 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?
- 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?
- Are low cost substitute materials available?
- Has pressure increased on suppliers' trading margins?

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

For the organization:

- Are we under foreign ownership by nations involved in international conflict?
- Do we have a celebrity or high profile chief executive or proprietor?
- Do we have a reputation for having significant links, customers, suppliers, etc. with unstable regions of the world?
- Are our brands regarded as controversial by some?
- Do we or our customers supply high profile customers or events?
- Is the organization involved with controversial trade?
- Have business competitors been accused of espionage or sabotage?

For the information systems:

- Does social media chatter suggest that we might be the target of digital intrusion?
- Are our Supervisory Control and Data Acquisition (SCADA) and other control systems also used by other organizations which could be prime targets?

Consideration of responses to these questions can give an understanding of the impact of a successful attack and the likelihood of it taking place. This informs a judgement on the proportionate level of protection required.

6.2 Identifying vulnerabilities

NOTE In this section EMA, malicious contamination and cyber attack 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 official advice on personnel security.[26)]

Questions which the TACCP team could ask include:

- 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 analyse their products?
- Which suppliers are not routinely audited?
- Are we supplied through remote, obscure chains?
- 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 analyses 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 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?

6.2.4 Cyber attack

Questions which the TACCP team may ask include:

- Has the Board adopted the NCSC's *10 Steps to cyber security* [27] and established appropriate procedures? (See Annex D)
- Are all IT/IS projects subject to an assessment of the risk of electronic intrusion?
- Are colleagues likely to be aware of and to report suspicious electronic communications (e.g. emails, SMS)?
- Is highly sensitive material held on separate, stand alone computer systems?
- Are passwords used securely, and in compliance with NCSC guidance?[27)]
- Are policies relating to the handling of electronic accounts when a member of staff joins, moves or leaves employment effective?
- Are any locality Wi-Fi links unencrypted or accessible by external users?
- Are manufacturing or other operational systems interconnected with information technology systems?
- Are internet enabled processes secure? For example, could process parameters be changed without proper authority? Could cloud based records be corrupted?
- Are data backup procedures effective?
- Are operators notified and aware of changes to production or other operational configuration, for example, to product formulations?
- Can production systems be remotely accessed?
- Are essential operations systems segregated from the company's corporate network and from the internet?
- Is externally sourced data (from email, internet or removable media) checked for malware before being imported?
- Does remote access to company systems require multi-factor authentication and is the extent of access limited?
- Do essential computerised systems have tested, offline backups?
- Are business continuity and disaster recovery plans for IT and production systems in place and effective?

[26)] Further information on personnel security can be found on CPNI's website at http://www.cpni.gov.uk/advice/Personnel-security1/ [26].

[27)] NCSC guidance is available from: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach [28].

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 1 – Risk assessment scoring

Likelihood of threat happening	Score	Impact
Very high chance	5	Catastrophic
High chance	4	Major
Some chance	3	Significant
May happen	2	Some
Unlikely to happen	1	Minor

NOTE 1 *This is an example scoring matrix, organizations may choose their own ranking scheme.*

NOTE 2 *Likelihood of a threat happening could be judged, for example, over a period of 5 years.*

NOTE 3 *Impact could consider death or injury, cost, damage to reputation and/or public and media perceptions of these consequences.*

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.

6.4 TACCP reporting

Four 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 has taken all reasonable precautions should they be victims of an attack.

Figure 3 – Risk scoring matrix

Impact						
	5				Threat A	
	4		Threat C			
	3					Threat B
	2	Threat E				
	1			Threat D		
		1	2	3	4	5
		Likelihood				

Very high risk	Threat A
High risk	Threat B
Moderate risk	Threat C
Low risk	Threat D
Negligible risk	Threat E

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

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

Access to premises		Relevant? Proportionate?
1	Access to people on business only	
2	Vehicle parking outside perimeter	
3	Premises zoned to restrict access to those with a business need	
4	Visible and comprehensive perimeter fencing	
5	Perimeter alarm system	
6	CCTV monitoring/recording of perimeter vulnerabilities	
Access to vehicles		**Relevant? Proportionate?**
7	Monitored access points	
8	Approach roads traffic-calmed	
9	Scheduled deliveries	
10	Documentation checked before admittance	
11	Missed deliveries investigated	
Access to people		**Relevant? Proportionate?**
12	Chip & PIN access control	
13	Changing facilities, separate personal clothing from work wear	
Access to electronic systems		**Relevant? Proportionate?**
14	Routine monitoring and implementation of NCSC guidance [28]	
15	Penetration testing by external professionals	
16	Routine training in cyber security principles (e.g. Cyber Essentials [29] or BS ISO 27000 series)	
Screening of visitors		**Relevant? Proportionate?**
17	By appointment only	
18	Proof of identity required	
19	Accompanied throughout	
20	Positive identification of staff and visitors	
21	CCTV monitoring/recording of sensitive areas	
Other aspects		**Relevant? Proportionate?**
22	Secure handling of mail	
23	Restrictions on portable electronic and camera equipment	
24	Limitations on access to mains services	

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

Detecting tampering		Relevant? Proportionate?
1	Numbered seals on bulk storage silos	
2	Numbered seals on stores of labels and labelled packs	
3	Effective seals on retail packs	
4	Numbered seals on hazardous materials	
5	Close stock control of key materials	
6	Recording of seal numbers on delivery vehicles	
7	Secure usernames and passwords for electronic access	
8	Reporting of unauthorized access by cyber systems	

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.

***NOTE** Further guidance on personnel and people security is available from: http://www.cpni.gov.uk/advice/Personnel-security1/ [26]. In particular, food businesses may make use of CPNI's publication, Holistic Management of Employee Risk (HoMER) [30].*

Table 4 – Personnel security

Pre-employment checks		Relevant? Proportionate?
1	Proof of identity	
2	Proof of qualifications	
3	Verification of contractors	
4	More sensitive roles identified with appropriate recruitment	
On-going personnel security		**Relevant? Proportionate?**
5	Staff in critical roles motivated and monitored	
6	Whistleblowing arrangements	
7	Temporary staff supervised	
8	Individuals able to work alone	
9	Favourable security culture[28)]	
End of contract arrangements		**Relevant? Proportionate?**
10	Access and ID cards and keys recovered	
11	Computer accounts closed or suspended	
12	Termination interview assesses security implications	

[28)] Further information on security culture is available from: CPNI at https://www.cpni.gov.uk/developing-security-culture [31].

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 (e.g. National Food Crime Unit in the UK);
- 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 *Some examples of police contacts are the National Crime Agency and the Anti-Kidnap and Extortion unit; 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 Management of a cyber-attack

Speed of response can greatly influence the damage caused by a cyber-attack so the maintenance of colleague awareness can be crucial. The complexity and variety of attacks can be so great that selection of a specialist contractor (in advance of the incident) may benefit many organizations.

Thoughts about cyber incident response are available from CREST (Council of Registered Ethical Security Testers) [32]. Support may also be available from membership of Cyber Security Information Sharing Partnership (CiSP) [33].

8.3 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

Any changes which could affect the TACCP assessment, such as breaches and suspected breaches of security or authenticity, should immediately be 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.

NOTE *The TACCP report and any review documents are commercially sensitive and confidential. Trusted senior managers with a 'need to know' and enforcement officials require access. Organizations may consider publication of a generic overview for internal use and/or to present to external auditors. Such an overview avoids detail which could be of value to an attacker. External auditors are to respect the sensitive nature of the TACCP process.*

Annex A (informative) TACCP case studies

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

A.1 General

This annex presents four 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.

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.

Case study C and case study D are intended to highlight cyber security issues faced by innovative food businesses. Case study C is a food initiative by an established internet, but not food, operator. Case study D is a professional food business aiming to exploit digital opportunities.

In all 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 [34].

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

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

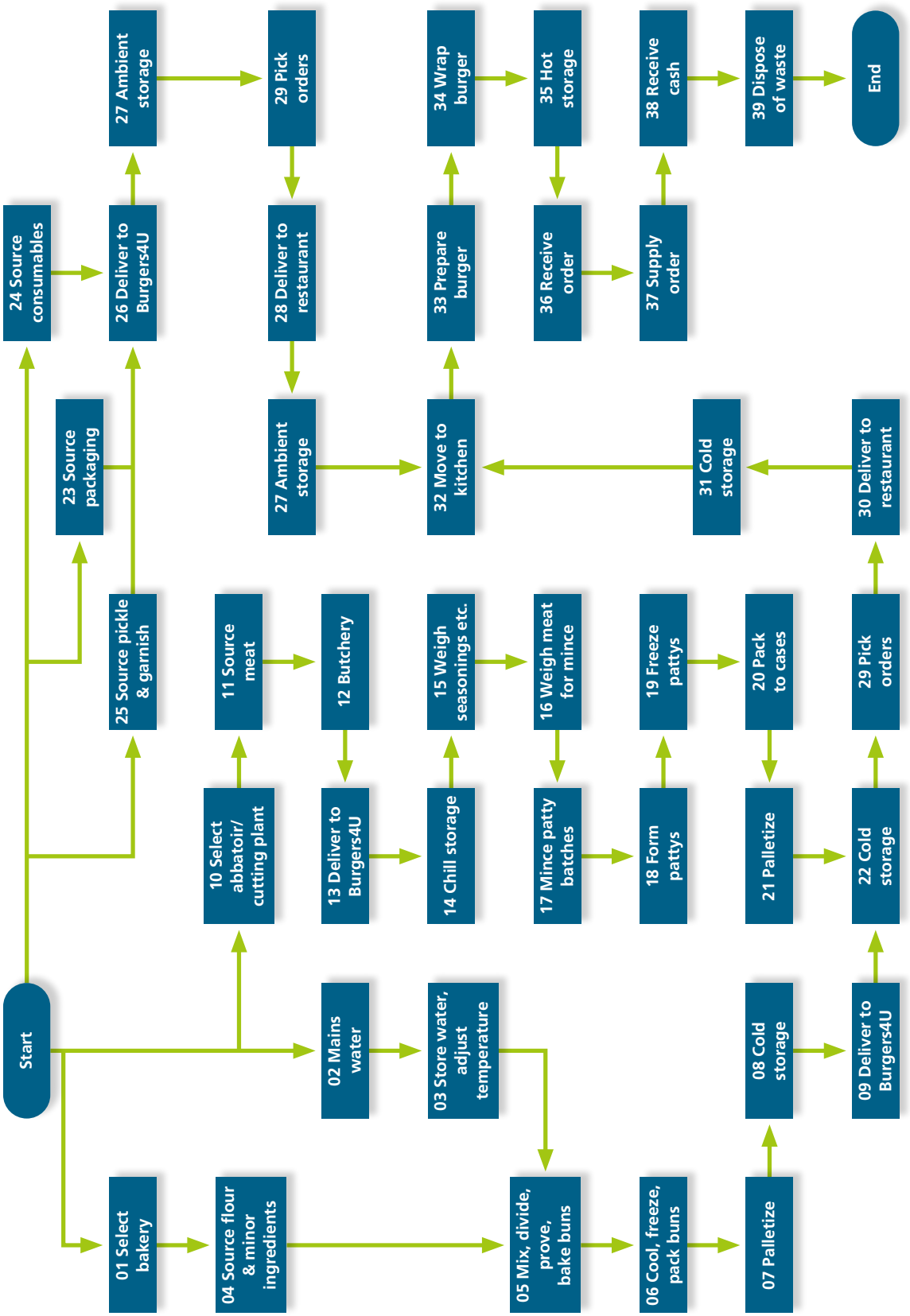


Figure A.1 – Threat identification

Table A.2 – Threat identification

Step no	Process step	Threat	Vulnerability	Access	Mitigation	Adulterant; Contamination	Impact of process	QA/QC	Likelihood	Impact
01A	Select bakery	Various	Casual staff	Production staff	Contracts require personnel security protocols	—	—	—	—	—
01B	Select bakery	Fraud	Collusion	Buyers	Little	—	—	—	2	3
02	Mains water	Malicious contamination	Bulk storage reservoirs	Services engineers	Effective control of access	Soluble toxins	May inhibit yeast; may affect dough handling	May fail sensory tests	1	1
03	Store water; adjust temperature	As above	Batch storage reservoirs	As above	As above	As above	As above	As above	1	1
04	Source flour + minor ingredients	Fraudulent substitution	Little cost advantage to fraudster	—	—	—	—	—	—	—
05	Mix, divide, prove, bake buns	Malicious contamination	Batch mixing operation	Skilled mixer operative	Trained experienced staff	Powdered toxin	May inhibit yeast; may affect dough handling	May fail sensory tests	1	1
06	Cool, freeze, pack buns	—	—	—	—	—	—	—	—	—
07	Palletize	—	—	—	—	—	—	—	—	—
08	Cold storage	—	—	—	—	—	—	—	—	—
09	Deliver to Burgers4U	—	—	—	—	—	—	—	—	—

Table A.2 – Threat identification *(continued)*

Step no	Process step	Threat	Vulnerability	Access	Mitigation	Adulterant; Contamination	Impact of process	QA/QC	Likelihood	Impact
10A	Select abattoir / cutting plant	Fraud	Collusion	Buyers	Little	—	—	—	3	5
10B	Select abattoir / cutting plant	Fraudulent substitution	Poor segregation of species	Delivery drivers; process staff	Unique animal identification recorded	Meat from cheaper sources	Negligible	Random tests may detect unless collusion	2	3
11	Source meat	Fraudulent substitution	Poor segregation of species	Process management and staff		Meat from cheaper sources	Negligible	Random tests may detect unless collusion	4	3
12	Butchery	Fraudulent substitution	Poor segregation of species	Process management & staff		Meat from cheaper sources	Negligible	Random tests may detect unless collusion	2	3
13	Deliver to Burgers4U	Hijacking of consignment	Supplier responsibility	—	—	—	—	—	—	—
14	Chill storage	—	—	—	—	—	—	—	—	—
15	Weigh seasonings etc	Malicious contamination	Manual operation	Process management & staff	Rigorous hygiene standards	Powdered toxins	Negligible	May fail sensory tests	1	3
16	Weigh meat for mince	As above	As above	As above	As above	As above	As above	As above	As above	As above
17	Mince patty batches	As above	As above	As above	As above	As above	As above	As above	As above	As above

Table A.2 – Threat identification *(continued)*

Step no	Process step	Threat	Vulnerability	Access	Mitigation	Adulterant; Contamination	Impact of process	QA/QC	Likelihood	Impact
18	Form pattys	As above	As above	As above	As above	As above	As above	As above	As above	As above
19	Freeze pattys	—	—	—	—	—	—	—	—	—
20	Pack to cases	—	—	—	—	—	—	—	—	—
21	Palletize	—	—	—	—	—	—	—	—	—
22	Cold storage	—	—	—	—	—	—	—	—	—
23	Source packaging	Misappropriation; Counterfeiting	Supplier warehouse security	Agency delivery drivers	Little	—	—	—	2	4
24	Source consumables	—	—	—	—	—	—	—	—	—
25	Source pickle + garnish	Ingredient substitution	—	—	Established brands; reliable contracts	—	—	—	—	—
26	Deliver to Burgers4U	—	—	—	—	—	—	—	—	—
27	Ambient storage	—	—	—	—	—	—	—	—	—
28	Deliver to restaurant	—	—	—	—	—	—	—	—	—
29	Pick orders	—	—	—	—	—	—	—	—	—
30	Deliver to restaurant	—	—	—	—	—	—	—	—	—
31	Cold storage	—	—	—	—	—	—	—	—	—
32	Move to kitchen	Malicious substitution	Out of hours; unsupervised	Night store-staff	Tamper evident cases	‘Spiked’ pattys	Little	None	1	3

Table A.2 – Threat identification *(continued)*

Step no	Process step	Threat	Vulnerability	Access	Mitigation	Adulterant; Contamination	Impact of process	QA/QC	Likelihood	Impact
33	Prepare burger	Deliberate undercooking	Lone worker	Restaurant staff	Rigorous food safety manufacture	—	—	None	1	2
34	Wrap burger	—	—	—	—	—	—	—	—	—
35	Hot storage	—	—	—	—	—	—	—	—	—
36	Receive order	—	—	—	—	—	—	—	—	—
37	Supply order	Selling too long after wrapping	Restaurant manager under wastage pressure	—	Personnel security procedures	—	—	—	2	2
38	Receive cash	Theft	Restaurant staff	Counter staff	Automated cash tills; rigorous audit	—	—	—	4	1
39	Dispose of waste	Misappropriation; Counterfeiting	Unlocked external bins	Public	Daily removal	—	—	—	1	2

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

Table A.3 – Threat assessment

Threat	Description	Vulnerable step	Likelihood	Impact	Protective action
A	Vandalism or sabotage	All locations	1	2	Maintain vigilance
B	DDOS attack on website	Marketing	3	3	Ensure cyber security good practice
C:01B	Fraud; collusion with suppliers	Select bakery	2	3	Job rotation <5 years
C:10A		Select abattoir/cutting plant	3	5	Internal audit

Table A.3 – Threat assessment *(continued)*

Threat	Description	Vulnerable step	Likelihood	Impact	Protective action
D:23	Counterfeiting; misappropriation of packaging	Source packaging	2	4	Formal notice to supplier; new supplier if no improvement in security after 6 months
D:39		Dispose of waste	1	2	No further action
E	Adverse publicity: 'Guilt by association' with 'fast food'	Corporate	2	1	Review PR strategy
F:32	Petty contamination; Possible serious malicious contamination	Move to kitchen	1	3	Part used cases to be security sealed by manager
G	Deliberate infestation of premises	Restaurants	1	2	Maintain vigilance
H:38	Theft: collusion with customers	Receive cash	4	1	No further action
I:10B	EMA – non-animal protein, or non-beef meats, replacing meat	Select abattoir/cutting plant	2	3	Stronger management of vendor: technical audit, regular sampling/ad hoc testing, facilitate whistleblowing
I:11		Source meat	4	3	
I:12		Butchery	2	3	
J:33	Deliberate undercooking of patty	Prepare burger	1	2	No further action
K:37	Selling burgers too long after wrapping	Supply order	2	2	No further action
L:02	Malicious contamination of component	Mains water	1	1	No further action
L:03		Store water; adjust temperature	1	1	
L:05		Mix, divide, prove, bake buns	1	1	
L:15		Weigh seasonings etc.	1	3	Key staff to meet personnel security standards

Figure A.2 – Threat prioritization

	Impact						
		5			C:10A		
		4		D:23			
		3	F:32 L:15	C:01B I:10B I:12	B	I:11	
		2	A D:39 G J:33	K:37			
		1		E		H:38	
Excludes (1,1) threats			1	2	3	4	5
			Likelihood				

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 Burgers4U 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. Advice and tenders for cyber response services may be sought (e.g. from CREST approved suppliers). 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 Bridgeshire Cheese Company. It was prepared, alone in the absence of other executive colleagues, 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 an example threat assessment report. Figure A.3 represents a vulnerability assessment flowchart.

Table A.4 – Threat assessment report 20170602

Threat no	From	Threat	Vulnerability [A]	Mitigation	Consequence	Impact	Likelihood	Protective action
1	Suppliers	Non-organic supply	'Top-up' milk; Bought-in calves; semen [B]	All goods from accredited suppliers	Loss of organic status	5	2	Require certificate of conformance for all ad hoc purchases
2	Neighbours over-reacting to 'effluent nuisance'	Widespread livestock disease	Rights of way through farm	Biosecurity meets best practice	Loss of herd and/or insurance cover	3	2	Install reservoir to avoid effluent discharge when wind from the SW
3	BCC staff	Malicious contamination	Manual operations, unsupervised (process largely self-controlling)	All staff are family members or long term trusted partners; All batches are taste tested	Localized illness possible	2	1	No further action
4	Adjacent farms	Trials of GM crops	Perimeter pasture land	Accreditation organization campaign	Loss of organic status	4	3	Cooperative action with trade association to lobby elected officials
5	Opportunist criminals	Theft of product	Distribution, vehicle often unmanned and unlocked	Little	Value of goods; Loss of reputation for reliability	2	3	Replace with more modern vehicle at earliest opportunity
6	Cyber criminals	Remote attack on Cloud controlled production process	Tampering with the 'Off the Peg' SCADA system to reduce pasteurization time/temperature	Supplier is re-assuring	Hazardous product from under-processing	5	1	Maintain separate QC analysis Take NCSC advice

[A] See Figure A.3 for the full vulnerability process assessment.
[B] Other goods are routinely sourced from long-standing accredited companies.

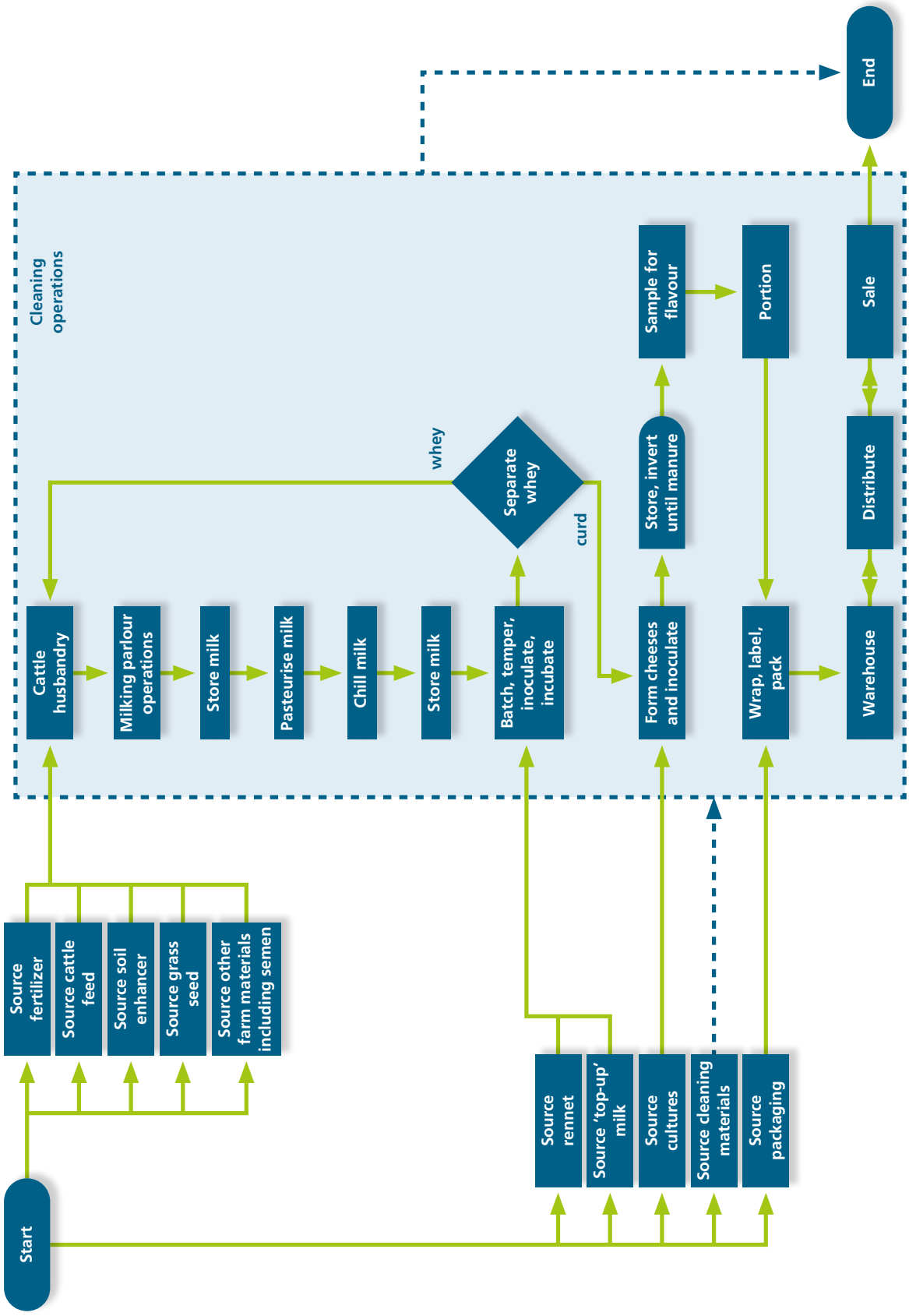


Figure A.3 – Vulnerability assessment

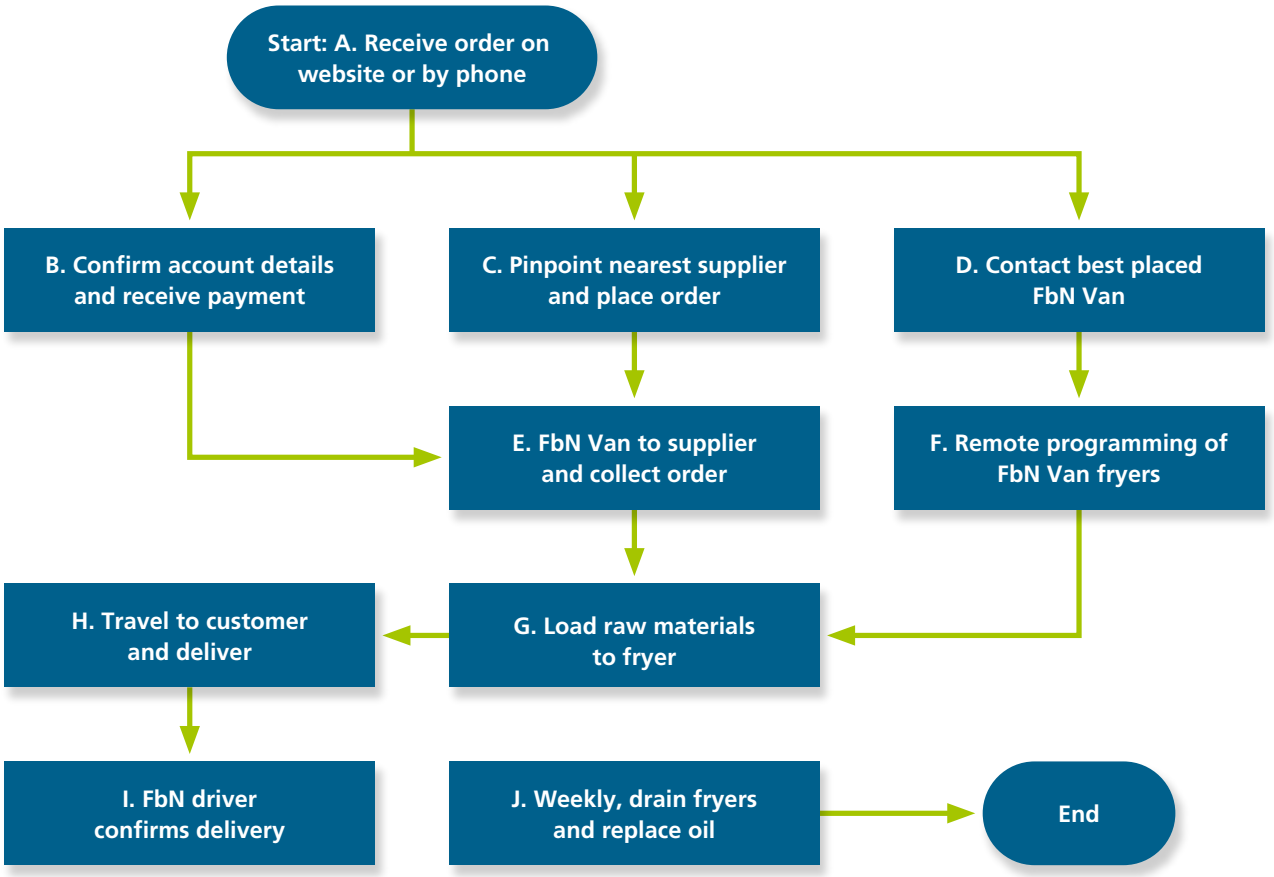
A.5 Case study C

FryByNite is a new venture, the national hot food delivery service of a major internet-based general trading company. The company is a world leader in its software and logistics management field, but is new into food business operations. It recognizes its weakness in food and has a consultant food specialist on contract for the duration of the launch and consolidation phases of FryByNite.

FryByNite aims to deliver freshly cooked hot food to customers' doorsteps within 30 minutes of receiving a web or telephone order. The standard product is fish and chips, with each delivery vehicle carrying programmable deep fat fryers. Raw product is ordered over the internet from a network of contracted fast food outlets. These prepare the food and load it into the frying baskets used by the delivery vehicle. A global positioning system (GPS) estimates the time to customers' premises and initiates the frying process. When ready, the frying baskets withdraw automatically and the food is packaged and kept hot so that the customer receives hot freshly cooked food in better condition than if they had visited the outlet themselves. (See Figure A.4)

Example product: Fried fish and chips for home delivery (as typical of the menu)

Figure A.4 – FryByNite workflow



TACCP Team: Director of Human Resources (Chairman)
Director of Information Systems
Consultant food technologist
Head of security

Threat information

NOTE *As a new 'brand' FryByNite is covered by holding company risk management and contingency planning procedures. The TACCP therefore addresses operational aspects of the new venture.*

Table A.5 – Threat information

No	Threat actors	Threats to company from:	Possible method of operation	Comments
1	Hacktivists	Failure of web based ordering system	DDOS attack	Protected by company-wide systems and expertise
2	Nation states	Loss of GPS-based navigation	Over-commitment and/or inadequate maintenance by satellite operators.	No control over threat actors but strong contractual protection with operators
3	Extortionists	Exfiltration of sensitive data	Phishing emails to staff	Ransomware readily available
4	Insiders	Theft of IP	Unauthorised access to administrative privileges	
		Threats to product:		
5	Aggrieved suppliers	Food poisoning	Inadequate handling of product	
6	Competitors	Food poisoning	Failure of van cooking regime	From power failure, or subversion of process controls
7	Aggrieved staff	Food poisoning	Malicious contamination	Personnel security screening in place
		Threats to operations:		
8	Criminals	Attack on vehicle/driver	Mugging for cash	Signs: "No cash held in this vehicle" in place
9	Vandals	Petty damage to vehicle	Random unplanned opportunism	Riskier areas noted on satnav system
10	Fraudsters	Loss of income	Use of stolen personal data to create false account	

Table A.6 – Threat assessment

Step	Threat	Threat No.	Vulnerability	Mitigation	Adulterant/ Contaminant	Comment	Likelihood	Impact
A	DDOS (**1**)	A1	High – public site	Corporate systems give early warning	—	Nuisance; loss of sales; annoyed customers	4	2
A	Inter-bank failure (**2**)	A2	Electronic funds transfer system is a prime cyber target, but well protected	Maintaining close links with system operators	—	Small chance of major loss	2	4
B	Fraudulent account (**10**)	B1	Fictitious delivery point	Check new accounts on set-up	—	Time waster	1	1
C	Supplier not available	C1	Databases out of date	Close partnership with suppliers	—		1	1
C	Product contamination (**5**) (**6**) (**7**)	C2	Batter may be target	Suppliers vetted for HACCP operation	Toxic chemicals; spore-forming bacteria	Supplier does not know customer identity, unless collaboration	1	4
C	Product substitution (**5**)	C3	Opportunistic food fraud	As C2	Exchange of species	Reputation and regulation	3	2
D	GPS failure	D1	Poor signal	Liaison with telecoms providers	—	Contingency plans in place	1	1
F	Corruption of control system with malware (**1**) (**4**)	F1	New technology: snags likely	Trials show resilience	—	Fire or undercooked food possible	3	5
G	Undercooking	G1	Oversized fillets	Size limits	—	Product inedible	1	1

Table A.6 – Threat assessment *(continued)*

Step	Threat	Threat No.	Vulnerability	Mitigation	Adulterant/ Contaminant	Comment	Likelihood	Impact
G	Product contamination (**4**)	G2	Unsupervised manual operation	Personnel screening	Toxic chemicals; spore-forming bacteria		2	4
H	Delays on route	H1	Unexpected traffic or roadworks	Automatic updates of satnav	—	Compensation if food inedible	3	1
H	Assault on staff (**8**)	H2	Some difficult customers and areas.	Staff training in conflict avoidance	—	A key concern in some areas	2	5
H	Damage to vehicle (**9**)	H3	Vehicle unsupervised during delivery	Riskier areas noted on satnav system	—	Largely nuisance	1	2
J	Inappropriate disposal of waste oil (**7**)	J1	Staff under pressure seeking shortcuts	Replacement 'new for old'	—	Reputation damage	1	2
J	Use of wrong oil	J2	Staff under pressure seeking shortcuts or covering mistakes	Replacement 'new for old'	Other edible oils Mineral oils Toxic organic chemicals	Issues: labelling; allergy; integrity; toxicity; fire safety	1	4

Figure A.5 – Threat prioritization

Likelihood						
	5					
	4		A1			
	3	H1	C3			F1
	2				A2 G2	H2
	1	B1 C1 D1 G1	J1 H3		C2 J2	
		1	2	3	4	5
	Impact					

Table A.7 – Threat register

Threat	Rating (L,I)	Description	Further defensive action	Responsibility	Comment
F1	(3,5)	Corruption of process control system for fryers	Daily review through roll-out and consolidation phases. Build contact with software provider.	Director of InfoTech	Target (2,3) within one year.
A1	(4,2)	DDOS - website	Build NCSC contact. Track social media chatter.	Director of InfoTech	On-going. Threat rating unlikely to change.
H2	(2,5)	Assault on staff	Evaluate use of body cameras	Director of InfoTech	With Director of Human Resources
C3	(3,2)	Fraudulent product substitution	Introduce low level overt product sampling	Consultant food technologist	Target (1,2)
A2	(2,4)	Inter-bank funds transfer failure	Continue current protocols.	Director of InfoTech	Insurance cover adequate.
G2	(2,4)	Malicious product contamination	Introduce ongoing personnel security routines.	Director of Human Resources	Target (1,4)
H1	(3,1)	Delays on route	Continue current protocols.		Under proportionate control.
J1	(1,2)	Inappropriate disposal of waste oil	Review and promote 'new for old' model.	Director of Human Resources	Target (1,1) within one year.
H3	(1,2)	Damage to vehicle	Continue current protocols.		Under proportionate control.

Table A.7 – Threat register *(continued)*

Threat	Rating (L,I)	Description	Further defensive action	Responsibility	Comment
C2	(1,4)	Malicious product contamination	Include handling of non-food chemicals in supplier accreditation.	Consultant food technologist	Threat rating unlikely to change.
J2	(1,4)	Use of wrong oil	Build technology into induction training.	Director of Human Resources	Threat rating unlikely to change.
B1	(1,1)	Fraudulent customer account	No further action required.	-	Under proportionate control.
C1	(1,1)	Supplier not available	Review training of database admin.	Director of Human Resources	-
D1	(1,1)	GPS failure	No further action required.	-	Under proportionate control.
G1	(1,1)	Undercooked product	No further action required.	-	Under proportionate control.

Commentary

1. As a new development the TACCP Team plans to meet monthly to review developments.
2. In all the Team has identified 15 threats of which seven require substantive protective action.
3. Remote control of the frying operation creates the opportunity for new threats (F1) which would receive senior attention and organizational priority.
4. Precautions, i.e. appropriate training, from launch of the initiative have kept the likelihood of assault on staff low, but further work is needed.
5. The parent company's senior managers continue its policy of avoiding a high profile public image which helps reduce the chance of FbN being a target.

A.6 Case study D

F. Armer & Daughters Ltd is an established agricultural company with an enviable reputation for 'good practice'. The business has evolved and grown from its origins as a mixed family farm supplying its local population with seasonal produce through to its present broad horticultural tariff. The core business is 'fresh as fresh can be' supply of vegetables for retail sale. Some fruit and specialist cereals complement vegetable production. There is increasing interest in supply to food service operations.

The business is managed on a day-to-day basis by the granddaughters of the farm's founder, the father of the F. Armer who named the company and remains its Chairman. It employs a small team to run the highly mechanised cleaning and packing factory but relies heavily on agricultural contractors for farming work, using temporary staff to cover peak periods. It is committed to external verification of its processes and procedures and receives exemplary reports from accreditation bodies and multiple customers alike. These procedures include an effective approach to risk management.

The company has now undertaken a massive move into automation and remote control of both farming and pack-house operations. It is committed to the use of unmanned aerial vehicle (UAV) surveillance of crops to better manage irrigation, application of pesticides, fertilizers and other treatments, and harvesting. It intends to fully integrate chilling, cleaning, trimming and packing of produce. It aims to significantly reduce further the time from field to despatch.

As part of this initiative and as it rolls out, the Directors have contracted a consulting information security specialist to conduct a TACCP exercise related specifically to the new information systems. Risk management of the conventional business is well established. The intention is that they have proportionate controls in place.

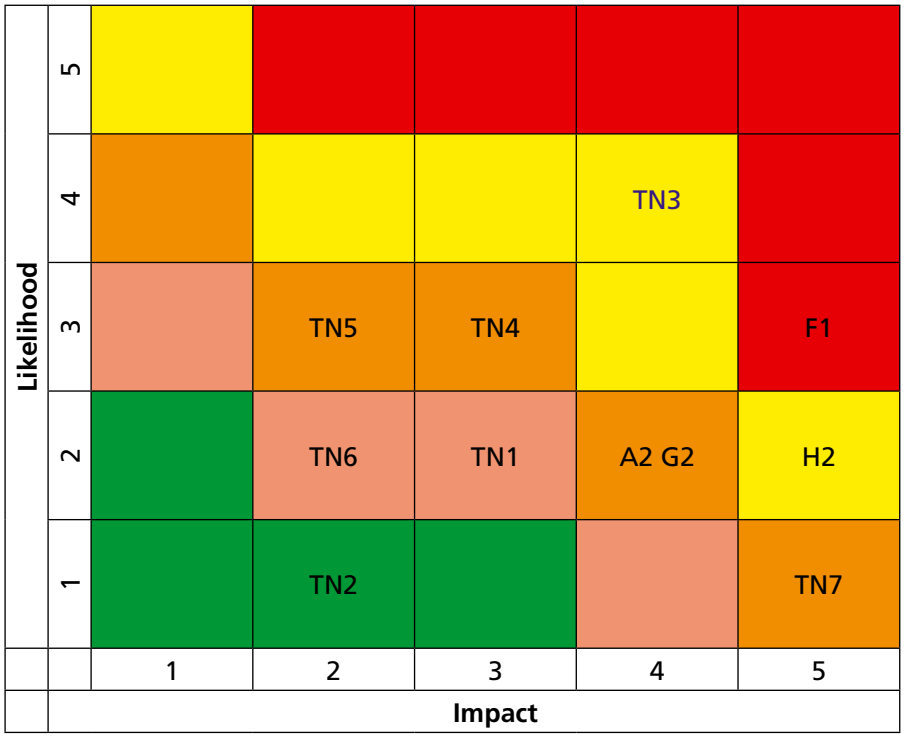
Table A.8 – Possible sources of malicious activity affecting F. Armer & Daughters Ltd

Greatest threat from:	Moderate threat from:	Lowest threat from:
Hacktivists	Alienated former employees seeking vengeance	Competitors
Sabotage of IT support infrastructure	Terrorists seeking publicity	Environmental campaigners
Extortionists		Contractors
Criminals stealing innovative IP		

Table A.9 – Threat assessment

Threat No.	System	Threat	Vulnerability	Mitigation	Comment	Likelihood	Impact
TN1	Electronic ordering from customers	Failure of telephone lines (weather, accident, sabotage, incompetence)	Operation can be slow but has not failed in 5 years	Strong personal arrangements with buyers so mobile call is an expedient		2	3
TN2	Electronic ordering from customers	Data corruption during transfer	Intervention by unauthorised parties	Big variances from planned volumes will prompt confirmation		2	2
TN3	Raising processing orders for pack-house	Malfunction of data transfer	Disruption to the cleaning/ packing operation leading to major waste, product shortages and downtime	Secure, tamper-evident housing for equipment	Manual entry will delay the packing operation to an unacceptable degree	4	4
TN4	Raising vehicle loading and delivery papers	Data corruption	Major cost penalties from rejected consignments		Contracted hauliers unlikely to note discrepancies	2	3
TN5	UAV monitoring of crops	Cameras and sensors fail to spot emerging problems	Remote control of device can be taken over by malicious actors	Routine software updates installed	Both harm caused and theft of the device could be incentives for malpractice	3	2
TN6	Computer farm record system	Takeover for ransom by criminals	Remote access by Directors over the Internet provides opportunity for criminals	Independent back-up daily would reduce losses	Key to operational practice and external accreditation	2	2
TN7	Industrial control systems	Sabotage of electronic controls	High cost highly sophisticated instruments cannot be duplicated, so non-operation = non-production	Updating and maintenance is rigorous	Contracted service engineer on call 24/7	1	5

Figure A.6 – Threat prioritization



Commentary

1. The company has fully embraced 'totally integrated manufacture' as its path to efficiency and customer service but is not yet fully aware of the vulnerabilities which are implied. The consulting information security specialist has been further contracted to complete the threat assessment and recommend proportionate controls.

2. So far as is practicable, duplicate systems are to be operated until completion of the assessment.

3. Support and advice from ncsc.gov.uk is used to raise awareness among key contractors and trusted staff.

4. Review to take place in one month.

Annex B (informative)
Sources of information and intelligence about emerging risks to food supply

B.1 General

The World Health Organisation (through INFOSAN) and the Food and Agriculture Organisation (through EMPRES and GIEWS) of the United Nations coordinate global efforts to identify new risks and enact control measures to minimize their impact.

They disseminate information to national food organizations like the Food Standards Agency in the United Kingdom. These national food organizations can then make it available to food businesses, typically through trade associations, but it really is a 2-way process.

NOTE *Subscription services which provide helpful information also include:*

- *HorizonScan which monitors global food integrity issues, see: https://horizon-scan.fera.co.uk/ ;*
- *Food Fraud Database from the US Pharmacopeial Convention, see: https://www.foodfraud.org/;*
- *US-CERT - United States Computer Readiness Team see https://www.us-cert.gov/.*

B.2 Information and intelligence levels

Figure B.1 illustrates the global dissemination and exchange of information and intelligence about emerging risks to food which may be used to update TACCP assessments. Five levels may be used to describe different levels of information sharing, 1 being the lowest and 5 being the highest:

Level 1 — Food organization;

Level 2 — Local;

Level 3 — National;

Level 4 — European;

Level 5 — International.

Figure B.1 – Global dissemination of information and intelligence about emerging risks to food which may be used to update TACCP assessments

NOTE *Further information on these international sources can be found at the following: INFOSAN http://www.who.int/foodsafety/areas_work/infosan/en/ [35], EMPRES http://www.fao.org/foodchain/empres-prevention-and-early-warning/en/ [36] and GIEWS http://www.fao.org/giews/english/index.htm [37].*

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:

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 [38].

C.2 EU 5-point action plan

In response to the horse meat fraud in 2013, the European Commission set in place the following 5 point plan [39].

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 [40], follows on from FDF's guide 'Sustainable Sourcing: Five steps towards managing supply chain risk' [32] 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.

Annex D (informative)
10 Steps to cyber security: A board level responsibility[29)]

NOTE This annex was developed from source material provided by the National Cyber Security Centre (NCSC).

D.1 Key questions for CEOs and boards

D.1.1 Protection of key information assets is critical

1) How confident are we that our company's most important information is being properly managed and is safe from cyber threats?
2) Are we clear that the Board are likely to be key targets?
3) Do we have a full and accurate picture of:
   - the impact on our company's reputation, share price or existence if sensitive internal or customer information held by the company were to be lost or stolen?
   - the impact on the business if our online services were disrupted for a short or sustained period?

D.1.2 Exploring who might compromise our information and why

1) Do we receive regular intelligence from the Chief Information Officer/Head of Security on who may be targeting our company, their methods and their motivations?
2) Do we encourage our technical staff to enter into information-sharing exchanges with other companies in our sector and/or across the economy in order to benchmark, learn from others and help identify emerging threats?

D.1.3 Pro-active management of the cyber risk at Board level is critical

1) The cyber security risk impacts share value, mergers, pricing, reputation, culture, staff, information, process control, brand, technology, and finance. Are we confident that:
   - we have identified our key information assets and thoroughly assessed their vulnerability to attack?
   - responsibility for the cyber risk has been allocated appropriately? Is it on the risk register?
   - we have a written information security policy in place, which is championed by us and supported through regular staff training? Are we confident the entire workforce understands and follows it?

[29)] For further information on cyber security see: https://www.ncsc.gov.uk/guidance/10-steps-board-level-responsibility [42].

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*

BS ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*

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

[1] CODEX ALIMENTARIUS. *CODEX CAC/RCP 1-1969: General principles of food hygiene.* Rome: CODEX Alimentarius, 2003.

[2] NATIONAL CYBER SECURITY CENTRE. Glossary. Available from: https://www.ncsc.gov.uk/glossary [viewed July 2017].

[3] FOOD STANDARDS AGENCY. Available from: https://www.food.gov.uk/enforcement/the-national-food-crime-unit/what-is-food-crime-and-food-fraud [viewed July 2017].

[4] US Pharmacopeial Convention's Food Fraud Database. Available from: http://www.foodfraud.org/ [viewed July 2017].

[5] BBC. '*Plastic rice' seized in Nigeria*. BBC, 2016. Available from: http://www.bbc.co.uk/news/world-africa-38391998 [viewed July 2017].

[6] OLIVE OIL TIMES. *Italy arrests 33 accused of olive oil fraud.* Olive Oil Times, 2017. Available from: https://www.oliveoiltimes.com/olive-oil-business/italy-arrests-33-accused-olive-oil-fraud/55364 [viewed July 2017].

[7] OLIVE OIL TIMES. *Brazil reveals widespread olive oil fraud.* Olive Oil Times, 2017. Available from: https://www.oliveoiltimes.com/olive-oil-business/brazil-reveals-widespread-olive-oil-fraud/56395 [viewed July 2017].

[8] EURO WEEKLY NEWS. *Police uncover major beef food fraud in Spain*. Euro Weekly News, 2017. Available from: https://www.euroweeklynews.com/3.0.15/news/on-euro-weekly-news/spain-news-in-english/144405-

police-uncover-major-beef-food-fraud-in-spain [viewed July 2017].

[9] ANTONY GITONGA. *Naivasha Hawkers using formalin to preserve milk.* Standard Media. Available from: http://www.standardmedia.co.ke/article/2000107380/naivasha-hawkers-using-formalin-to-preserve-milk [viewed July 2017].

[10] WORLD HEALTH ORGANIZATION and FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS. *Toxicological aspects of melamine and cyanuric acid: Report of a WHO expert meeting in collaboration with FAO*. WHO and FAO, 2009. Available from: http://www.who.int/foodsafety/fs_management/Exec_Summary_melamine.pdf, [viewed July 2017].

[11] U.S. PHARMACOPEIAL CONVENTION. *Food fraud database version 2.0.* Available by subscription from: http://www.foodfraud.org/#/food-fraud-database-version-20 , [viewed July 2017].

[12] FOOD STANDARDS AGENCY. *Update on malicious tampering with Kingsmill bread.* Food Standards Agency, 2006. Available from: http://webarchive.nationalarchives.gov.uk/20120206100416/http://food.gov.uk/news/newsarchive/2006/dec/kingsmill [viewed July 2017].

[13] TOROK, THOMAS J. MD, TAUXE, ROBERT V. MD, MPH, WISE, ROBERT P. MD, MPH; LIVENGOOD, JOHN R MD, SOKOLOW, ROBERT, MAUVAIS, STEVEN, BIRKNESS, KRISTEN A,SKEELS, MICHAEL R PhD, MPH, HORAN, JOHN M MD MPH, FOSTER, LAURENCE R, MD, MPH. *A large community outbreak of Salmonellosis caused by intentional contamination of restaurant salad bars.* American Medical Association, 1997. Available from: http://www.cdc.gov/phlp/docs/forensic_epidemiology/Additional%20Materials/Articles/Torok%20et%20al.pdf [viewed July 2017].

[14] Q FOOD. *Food Tampering: [1989] Glass in baby food*. Germany. Available from: http://www.qfood.eu/2014/03/1989-glass-in-baby-food/ [viewed July 2017].

[15] ORR, JAMES. *Blackmailer jailed over Tesco bomb threats*. The Guardian, 2008. Available from: http://www.theguardian.com/uk/2008/jan/28/ukcrime [viewed July 2017].

[16] MURRAY, KEVIN D. *Electronic eavesdropping & Industrial espionage*. New York: Murray Associates. Available from: https://counterespionage.worldsecuresystems.com/tscm-the-missing-business-school-course.html [viewed July 2017].

[17] GILLAM, CAREY. *Chinese woman arrested in plot to steal U.S corn technology*. Kansas City: Grainews. Available from: http://www.grainews.ca/daily/chinese-woman-arrested-in-plot-to-steal-u-s-corn-technology [viewed July 2017].

[18] THE COUNTERFEIT REPORT. *How to identify counterfeit Glen's vodkas*. Alexandria, 2014. Available from: http://thecounterfeitreport.com/product/322/ [viewed July 2017].

[19] NEWSCORE. *Offshore raids turn up fake Aussie Jacob's Creek wines*. Australia, 2011. Available from: http://www.news.com.au/finance/offshore-raids-turn-up-fake-aussie-jacobs-creek-wines/story-e6frfm1i-1226029399148 [viewed July 2017].

[20] FINANCIAL FRAUD ACTION UK. *Restaurants and diners targeted in new scam.* London. Available from: http://www.financialfraudaction.org.uk/cms/assets/1/scam%20alert%20-%20restaurants%20web%20link%20doc.pdf [viewed July 2017].

[21] NATIONAL FRAUD AUTHORITY. *Annual fraud indicator.* National Fraud Authority, 2013. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf [viewed July 2017].

[22] SMITH, MATT. *Cyber criminals use hacked Deliveroo accounts to order food on victims' cards*. DAILY TELEGRAPH, 2016. Available from: https://business-reporter.co.uk/2016/11/23/cyber-criminals-use-hacked-deliveroo-accounts-order-food-victims-cards/ [July 2017].

[23] ASSOCIATED PRESS. *Michigan-based Biggby Coffee reports database breach, possible theft of customer information*. CANADIAN BUSINESS, 2015. Available from: http://www.canadianbusiness.com/business-news/michigan-based-biggby-coffee-reports-database-breach-possible-theft-of-customer-information [viewed July 2017].

[24] FEDERAL BUREAU OF INVESTIGATION CYBER DIVISION. *PIN Number 160331-001 Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector 3*1. March 2016. Available from: https://info.publicintelligence.net/FBI-SmartFarmHacking.pdf [viewed July 2017].

[25] NATIONAL CYBER SECURITY CENTRE and NATIONAL CRIME AGENCY. *The Cyber Threat to UK Business*. Available from: https://www.ncsc.gov.uk/news/ncsc-and-nca-threat-report-provides-depth-analysis-evolving-threat [viewed July 2017].

[26] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. *Personnel security*. London: CPNI. Available from: http://www.cpni.gov.uk/advice/Personnel-security1/ [viewed July 2017].

[27] NATIONAL CYBER SECURITY CENTRE. *10 Steps to Cyber Security*. NCSC, 2016. Available from: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security [viewed July 2017].

[28] NATIONAL CYBER SECURITY CENTRE. *Password Guidance: Simplifying your approach*. Available from: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach [viewed July 2017].

[29] HM GOVERNMENT. *Cyber Essentials – Protect your business against cyber threats*. Available from: https://www.cyberaware.gov.uk/cyberessentials/ [viewed July 2017].

[30] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. *Holistic management of employment risk (HoMER).* London: CPNI, 2012. Available from: http://www.cpni.gov.uk/advice/Personnel-security1/homer/ [viewed July 2017].

[31] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. Developing a Security Culture London: CPNI https://www.cpni.gov.uk/developing-security-culture [viewed July 2017].

[32] CREST. Available from: http://www.crest-approved.org/ [viewed July 2017].

[33] Cyber Security Information Sharing Partnership (CiSP) Available from https://www.ncsc.gov.uk/cisp [viewed August 2017].

[34] SCOTTISH GOVERNMENT and FOOD STANDARDS AGENCY. *Expert advisory group report the lessons to be learned from the 2013 horsemeat incident.* 2013. Available from: http://www.scotland.gov.uk/Resource/0043/00437268.pdf [viewed July 2017].

[35] WORLD HEALTH ORGANIZATION. *International Food Safety Authorities Network (INFOSAN)*. Available from: http://www.who.int/foodsafety/areas_work/infosan/en/ [viewed July 2017].

[36] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS. *Emergency prevention system (EMPRES)*. Available from: http://www.fao.org/foodchain/empres-prevention-and-early-warning/en/ [viewed July 2017].

[37] GLOBAL INFORMATION AND EARLY WARNING SYSTEM (GIEWS). Available from: http://www.fao.org/giews/english/index.htm [viewed July 2017].

[38] FOOD AND DRUG ADMINISTRATION. *Carver + Shock Primer – An overview of the Carver plus Shock method for food sector vulnerability assessments.* FDA, 2009. Available from: http://www.fda.gov/downloads/Food/FoodDefense/FoodDefensePrograms/UCM376929.pdf [viewed July 2017].

[39] FOOD AND DRINK FEDERATION. *Food authenticity: Five steps to help protect your business from food fraud*. London: FDF, 2013. Available from: https://www.fdf.org.uk/food-authenticity.aspx [viewed July 2017].

[40] FOOD AND DRINK FEDERATION. *Sustainable sourcing: Five steps towards managing supply chain risk*. London: London: FDF, 2014. Available from: http://www.fdf.org.uk/sustainable-sourcing.aspx [viewed July 2017].

[41] NATIONAL CYBER SECURITY CENTRE.*10 Steps: A board level responsibility.* Available from: https://www.ncsc.gov.uk/guidance/10-steps-board-level-responsibility [viewed July 2017].

[42] NATIONAL CYBER SECURITY CENTRE. *10 Steps: A Board Level Responsibility*. NCSC, 2016. Available from: https://www.ncsc.gov.uk/guidance/10-steps-board-level-responsibility [viewed July 2017].

Further reading

BRC Global Standard for Food Safety. British Retail Consortium.

BRITISH RETAIL CONSORTIUM (BRC). *Cyber Security Toolkit: A Guide for Retailers*. Available from: https://brc.org.uk/media/120731/brc-cyber-security-toolkit_final.pdf [viewed July 2017].

CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. *Products and services*. Available from: http://www.cpni.gov.uk/advice/ [viewed July 2017].

EUROPEAN COMMISSION. http://ec.europa.eu/dgs/health_consumer/dyna/consumervoice/create_cv.cfm?cv_id=891

FOOD STANDARDS AGENCY. *Principles for preventing and responding to food incident*. FSA, 2007. Available from: http://multimedia.food.gov.uk/multimedia/pdfs/taskforcefactsheet23mar07.pdf [viewed July 2017].

INSTITUTE OF FOOD SCIENCE AND TECHNOLOGY. *Good manufacturing practice: A guide to its responsible management*. Wiley-Blackwell, 2013.

MI5 THE SECURITY SERVICE. *Current threat level in the UK.* Available from: www.mi5.gov.uk [viewed July 2017].

NATIONAL CYBER SECURITY CENTRE. *Guidance*. Available from: https://www.ncsc.gov.uk/guidance [viewed July 2017].

WORLD HEALTH ORGANIZATION. *Terrorist threats to food. Guidelines for establishing and strengthening prevention and response systems.* Food Safety Issues (WHO), 2008.

INTERPOL. *Operation Opson*. Available from: http://www.interpol.int/Crime-areas/Trafficking-in-illicit-goods-and-counterfeiting/Operations/Operations/Operation-Opson [viewed July 2017].

EUROPAL and INTERPOL. *Operation Opson III 2013: Targeting counterfeit and substandard foodstuff.* Available from: http://www.ipo.gov.uk/ipenforce-opson.pdf [viewed July 2017].

CIO from IDG (International Data Group - Global) 5 steps to respond to a security breach. Available from: https://www.cio.com.au/article/580908/5-steps-respond-security-breach/ [viewed August 2017].

CampdenBRI Guideline 72 TACCP (Threat Assessment and Critical Control Point) - A practical guide.

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

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.

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

Information regarding online access to British Standards and PASs via British Standards Online can be found at **http://shop.bsigroup.com/bsol**

Further information about British Standards is available on the BSI website at **www.bsigroup.com/standards**

Copyright

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

BSI, 389 Chiswick High Road
London W4 4AL
United Kingdom
www.bsigroup.com

ISBN 978-0-580-98099-2